

# The Basics of Digital Privacy

# The Basics of Digital Privacy

Simple Tools to Protect Your  
Personal Information and Your  
Identity Online

**Denny Cherry**

Technical editor  
**Thomas LaRock**



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEW YORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

**SYNGRESS®**

**Acquiring Editor:** *Chris Katsaropoulos*  
**Editorial Project Manager:** *Benjamin Rearick*  
**Project Manager:** *Priya Kumaraguruparan*  
**Designer:** *Matthew Limbert*

Syngress is an imprint of Elsevier  
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2014 Elsevier Inc. All rights reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

#### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described here in. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

#### Library of Congress Cataloging-in-Publication Data

Application Submitted

#### British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

ISBN: 978-0-12-800011-3

Printed and bound in the United States of America

14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

		<b>Working together to grow libraries in developing countries</b>
<a href="http://www.elsevier.com">www.elsevier.com</a> • <a href="http://www.bookaid.org">www.bookaid.org</a>		

For information on all Syngress publications, visit our website at [store.elsevier.com/syngress](http://store.elsevier.com/syngress)

# Dedication

This book is dedicated to my lovely wife Kris, who is gracious enough to allow me to spend every waking moment working on this and to spend countless nights, weekends, and entire weeks traveling in support of the Microsoft SQL Server community and my day job, which I enjoy to a level that probably isn't normal.



# Acknowledgments

I'd like to thank everyone who was involved in putting this book together (if I forgot you on this list, sorry). This includes my editors Ben, Chris, and Heather, and my friend and technical editor Thomas LaRock, all of whom helped me out greatly in the development process.

# Author Biography

Denny Cherry is the owner and principal consultant for Denny Cherry & Associates Consulting and has over a decade of experience working with platforms such as Microsoft SQL Server, Hyper-V, vSphere, and Enterprise Storage solutions. Denny's areas of technical expertise include system architecture, performance tuning, security, replication, and troubleshooting. He currently holds several of the Microsoft Certifications related to SQL Server for versions 2000 through 2008 including the Microsoft Certified Master as well as being a Microsoft MVP for several years. Denny has written several books and dozens of technical articles on SQL Server management and how SQL Server integrates with various other technologies.

# Introduction

This book looks at the problems associated with data privacy and specifically how we keep our data private from others who shouldn't be accessing the data.

In the first chapter, [Chapter 1](#), we look at how much information you should be storing online and the risks of storing that information online.

In [Chapter 2](#), we review the guidelines for selecting usernames and passwords as well as options for two-factor authentications.

In [Chapter 3](#), we look at the home computer network. The home computer network has many weak points such as the router, the Wi-Fi network, and the devices on the home network.

[Chapter 4](#) looks at the weaknesses within the home computer as well as how to encrypt all the sensitive data that is stored on your computer.

[Chapter 5](#) talks about how to limit the information you post online.

[Chapter 6](#) reviews the various ways that people and governments are able to watch what you do online.

The final chapter, [Chapter 7](#), looks at the specific laws and programs that have been discovered around the spring and summer of 2013 that various governments are able to use to monitor what people around the world do.

# Storing Your Personal Information Online

# 1

---

## INFORMATION IN THIS CHAPTER

- How much information you should share with companies
- Risks of sharing too much information online
- Knowing how companies protect your information
- Cookies and websites

This chapter talks about the risks of storing information online and how we can mitigate some of those risks.

---

## STORING YOUR PERSONAL INFORMATION ONLINE

In the modern world, we all end up storing information online, even if we don't know that we are. Every company that you do business with stores information about their customers, including you, in a computer on their network. Every website that you visit on the Internet be it from your desktop computer, laptop computer, cell phone, library computer, and Internet café is storing information about you in some form or another. That computer or system of computers in some cases runs a database that allows the customer service, sales, marketing, etc., staff to find customer information, run reports on purchase history, etc. Even when you do business with companies in person and not via the Internet, you will have information stored about your purchases within their systems.

The perfect example of this is the customer loyalty cards that are given out by grocery stores. These cards are very useful for us the customers because it gives us access to discounts that we wouldn't normally have access to without having to cut coupons and remember to bring them in. The information that the store gathers via these loyalty programs tells them everything about their customers, their shopping habits, and so on.

---

## NOTE

### What companies can do with this information

One of the most famous problems that has become visible to the general public happened with the large retailer. Target started sending coupons based on personal shopping habits that they tracked via their loyalty program. One specific customer, who lived with her father, began receiving coupons for prenatal vitamins and baby supplies. The father was quite upset that

Target was sending his daughter, who was under the age of 18, these coupons so he went to the local Target store and complained to the store manager. The daughter then had to explain to her father that she was indeed pregnant.

The way that Target had been able to figure this out was by analyzing her store purchases on her loyalty program card called data analytics.

You can read more about this use of data at <http://basicsofdigitalprivacy.com/go/target>

---

Understanding just how much information companies track about their customers, both their online customers and their offline customers, is critical to understanding how you as the customer can protect yourself against data and identity theft. Understanding how the companies collect and use the information about you the customer allows you to make informed decisions about what information to give companies and when. In a lot of situations, you can just give the company false information to get through the process without giving them a way to track you. A perfect example is when asked for your phone number at checkout, give them all zeros, or when asked for your zip code, give them the zip code of the store instead of your home.

The problem with it comes to protecting our own privacy is that we as people by our nature want to be friendly and accommodating. Companies are able to take advantage of this by asking for information that we are usually all too willing to give away, even if we shouldn't be. Companies may not always make it very obvious that they are collecting this sort of information. Often, they will get you to give the company this information as part of the security questions that are used to later verify that you are you when you forget your password. However, many of the questions that companies use can be easily enough found by simply looking at social networking sites (which we will be talking about in this chapter and [Chapter 5](#)).

## How much information you share with companies

The companies that we do business with on a daily basis are collecting massive amounts of information about us on a regular basis. As of the writing of this book in the summer of 2013, there are no laws or regulations about how much information a company can collect about their customers.

The reason that companies collect all this information about their customers is for a couple of different reasons. The first, and the most common, is so that they can better target advertising so that there is a better chance of selling their customers additional products at a later date. This reason makes total sense when you think about it: companies make their money by selling us products. If they can figure out what products we want to buy before we know that we want to buy them, they have a better chance of selling us the products than their competitor does.

For example, if Best Buy is able to figure out that I need to buy a new Blu-ray DVD player before Target is able to figure out that I need to buy a new Blu-ray DVD player, and Best Buy is able to get me an ad for their new Blu-ray player that is available in the stores, then odds are that I will end up purchasing the Blu-ray DVD player from Best Buy and not from Target.

The second reason that companies collect information about their customers is much less likeable and enjoyable for their customers. This is when companies collect and store information about their customers so that the information that is collected can be sold to other companies so that the other companies can advertise to us. The easiest example of this practice is Facebook. With Facebook, we willingly give all our information over without any thought about it. Facebook then uses that information to more easily enable advertisers to display us ads on the Facebook website. In this case, we are no longer the customer, we become the product that is being sold.

### **Risks of sharing too much information online**

When companies collect and store large amounts of information about us, that information becomes more at risk of being stolen by other people. The biggest threat to consumers when it comes to identity theft is that the information needed to steal someone's credit card information or their entire identity can be found in the computers of companies that those consumers do business.

#### ***Giving attackers the information that they need***

As we share more and more information online about our lives on social networks like Facebook and Twitter, it becomes easier and easier for identity thieves to find out the information that they need to break into our accounts and take over our identities; we will be talking more about social networks in [Chapter 5](#).

When we set up accounts with companies such as our banks, we set up a username and a password. When we do this, we keep these items secret so that no one else knows what these items are. However, there is a weakness with this system that becomes painfully easy to exploit and that is the fact that all of these accounts are set up to go with a specific e-mail address. That e-mail address is your e-mail address and is used to send you information about the bank and your electronic statements and to allow you to gain access to your account in the event that you forget what your password is. By their nature, e-mail addresses are not secret and are known by all our friends and family and may even be published on the Internet so that customers, old friends, and so on can contact us. The e-mail address that is posted online can also be used by attackers as the first step in gaining access to our bank accounts.

Once an attacker has figured out what your e-mail address is, finding out the website where your e-mail can be accessed usually isn't all that hard. For example, if you have an e-mail address that ends in @earthlink.net, your e-mail can be accessed via the website [webmail.earthlink.net](http://webmail.earthlink.net). If your e-mail address ends in @gmail.com, then your e-mail can be accessed via the website [www.gmail.com](http://www.gmail.com). Figuring out the website to access even rare domains is usually very straight forward.

On most public website sites, there is going to be a link that can be used to allow the customer to figure out or reset the password in the event that the password has been lost. Usually, this is done by asking a series of questions that only the owner of the account would know the answer to. When the Internet was first being used and this sort of challenge and response question concept was put together, this worked

very well as no one was posting personal information online. However, as time has moved forward and social networking has continued to grow in popularity, the idea of challenge and response questions hasn't really changed. Now, instead of the information to answer these questions being something that only the account owner would know, it's a real possibility that the answers to these questions has been shared online on social networking sites.

---

## NOTE

### **Challenge questions should be challenging**

Recently, I was setting up a new bank account at one of the major banks in the United States. As a part of the process, they help you set up your username and password for the online banking system. While going through the process, the challenge and response questions were shown so that I could pick the questions that I wanted to use for my online access to the bank.

Every one of the questions that was shown was information that most people would share on Facebook, Twitter, or any other social network without thinking twice about it. Some of the questions that were on the list included questions like what city you met your spouse in.

---

### ***Telling thieves when to break into your house***

While social networks are great for telling our friends and relatives what is going on in our lives, our friends and family aren't the only people that can view the information that we post on social networking sites. Most social networking sites are wide open by default meaning that anyone who looks at the site can find the information that you post on the site (we will talk more about how to set up security on social networking sites in [Chapter 5](#)).

As we post more and more information on social networking sites, we become more and more used to posting everything that we are doing online. However, when it comes to traveling, for business or pleasure, we need to be very careful how much information we post online. Likewise, we need to be very careful about posting our actual home address online. If we have posted where we actually live, and we also post when we are on vacation out of town, we have just told any potential burglars in our home area where our house is and the fact that it'll be empty. If we post online that we are going to Hawaii for vacation as an example, a potential burglar can assume that the house will be empty for at least 4-5 days if not for a full week.

---

## NOTE

### **Me and my social networking**

Personally, I love using Foursquare when I'm traveling on business trips or on vacation. It lets my friends know where I'm at, and if I go back to a city later, it tells me where I've been so that I know if I want to go back or if it is somewhere that I can skip.

When at home, however, I reduce my use of services like Foursquare as I don't want just anyone knowing my home address and when I'm at home and when I'm not. So while I may check into restaurants when I'm at home, I never check into my actual home or my local supermarket, etc.

---

There are a several location services that have become popular online. The first is Foursquare and the second is Facebook's location service. When using either one of these services, it is important to not check in at your actual home as this gives away the exact location of your home, your family, and all your stuff. While finding someone's home address isn't all that hard if you know where to look online, the goal of masking yourself on social networking just a little bit is to make it a little harder to find out information like where you live and when you aren't there. If you are a big fan of using these location services, picking a location in the general area of your home is generally safe enough for most people; however, for those people who work in a high security field, they should avoid these sorts of services. This includes people who work in law enforcement, for security companies, banks, and doctors, basically anyone who works with the public or a segment of the public and doesn't really want to have people.

### **Knowing how companies protect your information**

A big problem when it comes to giving information to companies online is knowing how the company is going to protect the information that you give them. Many companies will post information on their website that will give you basic information about what the company will be doing with your information and how they will protect it. While some basic information may be provided, there won't be any details such what information is being encrypted or how employees are trained to ensure that personal data aren't printed and lost that way. The reason that such information isn't available to the general public is that it gives attackers more information about the company and what sorts of gaps the company has in their data protection policies.

With websites like Facebook and Twitter, these companies while holding lots of personal information, aren't really holding lots of your confidential information. However, other companies such as insurance companies, doctors' offices, credit card companies, payroll services, or even your employers' human resources and payroll departments all hold massive amounts of information about you, much of which you don't want anyone else to find out about, while some of which is protected information according to many countries' data protection laws, including the United States.

In the United States, all medical data are protected by a federal law called HIPPA or the Health Information Patient Protection Act. This law that was passed and signed into law 1996 requires that all companies that handle medical information (insurance companies, doctors' offices, medical billing companies, etc.) take precautions to ensure that the medical data that they store either on paper or in a computer system are protected so that only the people who should have access to the information actually have access to them. While this all sounds great in principal, the reality is that it is very easy for the employees at these healthcare companies to lose confidential data in the course of their normal job activities.

For example, a medical auditor could be reviewing medical records at a medical insurance company to ensure that doctors aren't overbilling the insurance company. While the auditor is reviewing these records, they may end up printing up a copy of



the data to make reviewing the information easier. Once that audit is complete, the auditor is supposed to shred the printouts. However, they could end up lost in the person's desk or dropped on the floor. While lost in the auditor's desk isn't the worst thing, if the papers were dropped on the floor, the cleaning person who comes through at night emptying the trash may throw the papers on the floor away without knowing what they are or that they are supposed to be shredded. This means that there are now medical data on printouts sitting in the trash without being shredded that could be pulled from the trash by anyone who is walking past the trash dumpsters and who knows what they are looking for or who finds the papers when they make their way to the city dump.

Even if in our example, the auditor doesn't print the information, but instead, they access the information from their company laptop that they then put in their trunk as they head home for the day. On the way home, the auditor heads to the supermarket to pick up dinner for the family. While in the supermarket, the employee's car, with the laptop still in the trunk, is now stolen by a car thief. The car thief now has the employee's laptop as well. The hard drive within the laptop can be easily enough installed in another computer so that the information from the laptop can be downloaded and sifted through. There are data encryption options available that would prevent the data on the hard drive from being read, which are talked about in detail in [Chapter 4](#). If the company policy says that the laptop hard drive is encrypted and that it is actually encrypted using a high security encryption process, then the information can't be viewed by the car thief. But if the company has no requirement to encrypt the data of the laptop's hard drive, then it won't be protected. In any case, the company won't be posting on their website the kinds of protection that they have in place to protect their customers' information.

The main reason that companies don't broadcast this information isn't to keep their customers in the dark, but to help protect the customers' information. If the company doesn't tell people how the data are protected, then attackers don't know how the data are protected, which means that the attacker doesn't know how the data are protected, which means that getting access to the data takes longer and is harder. One of the goals of data security is to make breaking through the security so hard and take so long that it isn't worth the time and the trouble to attempt to break through the data security. While it probably seems like I'm disagreeing with myself in this section, I kind of am. This is one of those times where companies and their customers don't have the same interests in mind. The companies want to keep their practices secret, while the customers want to know how their data are being protected.

## Cookies and websites

Most websites in the modern times of the Internet use cookies to store information about the user and how they use the website on the user's computer. These cookies can store a variety of information within them, with the user of the website having little if any control over what information is stored within the cookie. Cookies are created per website meaning that different websites cannot read each other's cookies.

As an example, if you were to go to [www.google.com](http://www.google.com) and [www.yahoo.com](http://www.yahoo.com), both of these websites would create their own cookies on your computer. This cookie will contain some basic information about you, not necessarily your name or your e-mail address, but there will be at the minimum a specific identifier that is unique to your computer so that these sites can track your interactions with their respective properties. However, Google's website has not access to Yahoo's cookie, and likewise, Yahoo has no access to Google's cookie.

That being said, there are risks to cookies when it comes to online privacy. The first one being that these cookies allow the website to track you as you move around on their website. At first, this doesn't sound all that bad, but when it comes to the major Internet companies like Google, their website isn't confined to just their website. This is because Google controls the largest advertising network on the Internet called Google AdWords. This advertising platform is used by the majority of websites to display all manner of advertisements on all manner of websites. As you move from website to website, not only the websites that contain the advertisements will display advertisements on the website that you are viewing but also the advertising system will also track that you visited that website. Then, when you browse other websites using this tracking data, the advertising system would then display advertisements that are similar in nature to the sites that you have visited.

---

## REAL-LIFE EXPERIENCE

### Watching the ads become more relevant

In my line of work as an IT consultant, I end up doing more than my fair share of traveling. Every time I travel, I use the same few companies, United Airlines to book the flights, Hilton Hotels to stay at, and Avis to get my rental car. During my normal day, I see all manner of advertisements online. As soon as I book my flights, I begin seeing advertisements for United Airlines on all the other websites that I visit. Once I book my hotel, I'll begin to see ads for either Hilton or one of their competitors such as Hyatt or Marriott. Once I book my rental car through Avis, I suddenly begin seeing advertisements for Avis's competitors such as Hertz and Enterprise.

The way that the Google advertising system knows that I've just been looking at the United Airlines website and that it should show me advertisements for United Airlines is because the Google advertising website, which is used to display the ads on the [www.united.com](http://www.united.com) website, has tracked the fact that I was just browsing the United Airlines website. It knows that I'm me on both the United Airlines website and the other websites that are using the Google advertising system because of the cookie that exists on my computer that was placed there by the Google advertising system.

You may be asking yourself why I would see advertisements from the United Airlines after viewing the United Airlines website, but when viewing the Hilton Hotels website, I see ads from other hotel chains. The reason for this is because United has bought all the ads that are triggered by being shown after viewing their website, where Hilton hasn't done this. This tells the Google advertising system that after I view the United Airlines site, I shouldn't see any other advertisements for other companies in the same category as United Airlines, in this case airlines. Hilton and Avis haven't set up this same agreement with Google, which is a quite expensive advertising purchase to make but worth it according to United Airlines.

---

Many people consider this tracking across the Internet to be quite intrusive as it gives one company, specifically a company that you may not be doing business with, access to basically your entire browsing history that they can data mine and use this to serve up advertisements that are reliant to you the user. And frankly, I have to agree with those people. Many people wonder how this sort of Internet tracking is legal. The most basic reason why this sort of thing is allowable is because every website that you visit is going to have some sort of End User License Agreement (EULA) that specifies the terms that you must agree to in order to use the website. Buried somewhere in that user agreement, which it is assumed that you have agreed to by using the website, is something that will give the website and its partner websites, which would include the advertising systems, the right to track you via cookies.

There are a few ways to solve this.

### ***InPrivate Browsing***

The first is to enable a feature in most web browsers called “InPrivate Browsing.” In Internet Explorer, this can be enabled by opening Internet Explorer, then clicking on the Tools menu icon (the gear in the upper right-hand corner of modern versions of Internet Explorer), then clicking on the menu that says “Safety,” and then selecting “InPrivate Browsing.” This will open a new Internet Explorer window and this new window will be running in private browsing mode. Any websites that you view when working within the InPrivate Browsing window will not be saving any cookies, temporary Internet files (also known as cache), browsing history, etc.

---

### **NOTE**

#### **Porn mode?**

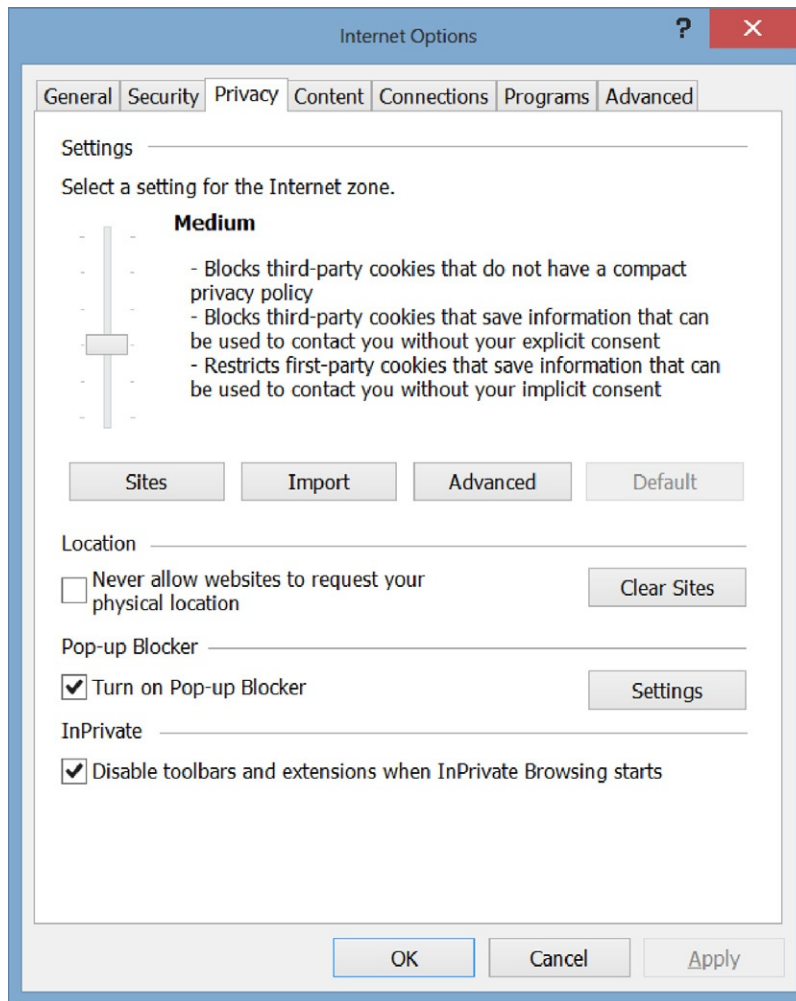
When “InPrivate Browsing” was first introduced, it quickly earned the nickname “Porn Mode” or “PrOn Mode.” The reason for this is that many people don’t want their spouses to know that they are browsing adult content. It was assumed that this would be what the bulk of people who were using “InPrivate Browsing” would be using it for, as for the bulk of people not tracking their adult browsing history is the most important thing that they don’t want other people seeing.

The reality is that “InPrivate Browsing” is much more valuable than this as it can be used to protect Internet users from the prying eyes of companies who want to do nothing more than sell advertisements on behalf of other companies so that you’ll click on the ads.

---

### ***Turning cookies off in Internet Explorer***

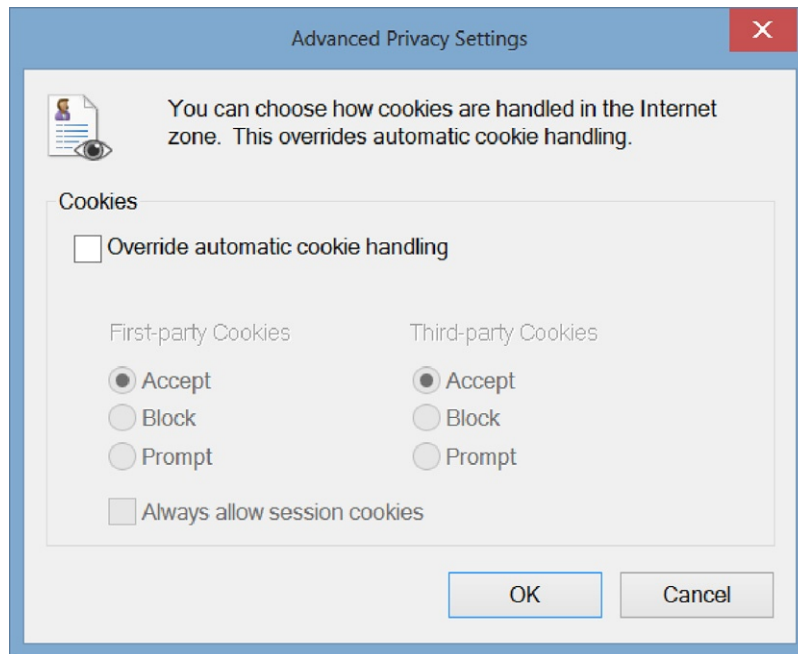
The second method that can be used to prevent cookie tracking by the advertising company is to disable cookies within the web browser. This is a very easy thing to do. In newer versions of Internet Explorer, click on the gear icon in the upper right-hand corner of the Internet Explorer application. In older versions, click on the Tools drop-down menu. In either case, click on the “Internet Options” menu item. On the Privacy tab at the top of the window, there are settings for configuring the cookie usage as shown in [Figure 1.1](#).

**FIGURE 1.1**

Internet Explorer's privacy settings.

Clicking the Advanced button will allow you to override the default handing of cookies. Checking the checkbox allows the configuring of first-party cookies and third-party cookies as shown in [Figure 1.2](#).

From this screen, you can configure Internet Explorer to Accept, Reject, or Prompt for cookies. The default for Internet Explorer is to accept all cookies. By rejecting cookies, the website would attempt to create the cookies, but the web browser would simply ignore the request to create and save the data to the cookie.

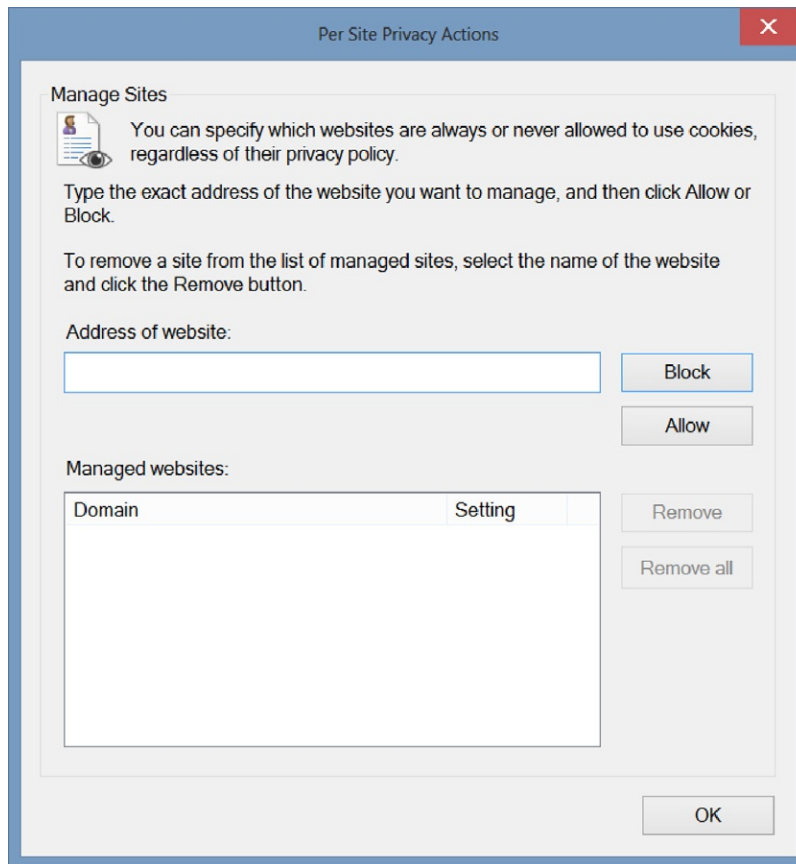
**FIGURE 1.2**

Advanced cookie configuration.

By setting the settings to prompt, this would prompt you each time the web browser requested to create, update, or read a cookie. While this will slow down the web using experience by prompting over and over to use the cookie, it will give you the ability to control exactly which cookies are used and which ones aren't. This can be important as you may wish to store login information for a website and only deny the website the ability to store the advertising cookies.

If there are specific websites that you wish to prevent from ever saving a cookie on the system, this can be done through the Privacy tab of the Internet Options window as well. On the top half of the screen, there is a section labeled "Settings," and within that section, there is a button labeled "Sites." Clicking on that button will bring up a screen similar to that shown in [Figure 1.3](#).

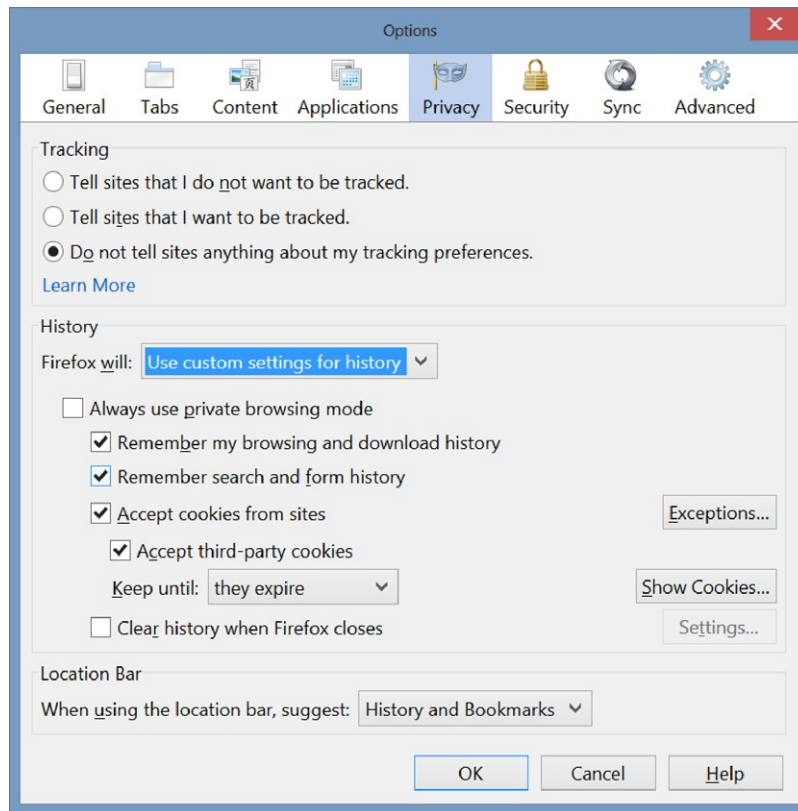
By adding a site to the screen shown in [Figure 1.3](#), the specific site can be prevented from using cookies at all on the site. For example, to block Google's AdWords system, enter the URL [www.googleadservices.com](http://www.googleadservices.com) and then click the block button. Clicking OK all the way out will enable this setting so that the next time you view an advertisement that has been served by the Google advertising system, the Google advertising system will not be able to track the data.

**FIGURE 1.3**

Per Site Privacy Actions screen.

### ***Turning cookies off in Firefox***

Internet Explorer isn't the only web browser that allows for turning off cookies, and this can also be done in Mozilla's Firefox web browser as well. In Firefox, to turn off cookies, click on the Tools drop-down menu at the top of the Firefox application. If you don't see any of the drop-down menus, click on the key labeled "Alt," which should make the menus at the top appear. After clicking on the Tools drop-down menu, select from the "Options" menu option. On the Options window that appears, select the "Privacy" page as shown in [Figure 1.4](#). On the "Privacy" page within the "History" section within the "Firefox will" drop-down menu, change the setting from "Remember History," which is the default to "Use custom settings for history" as shown in the middle of [Figure 1.4](#).

**FIGURE 1.4**

Firefox cookie settings.

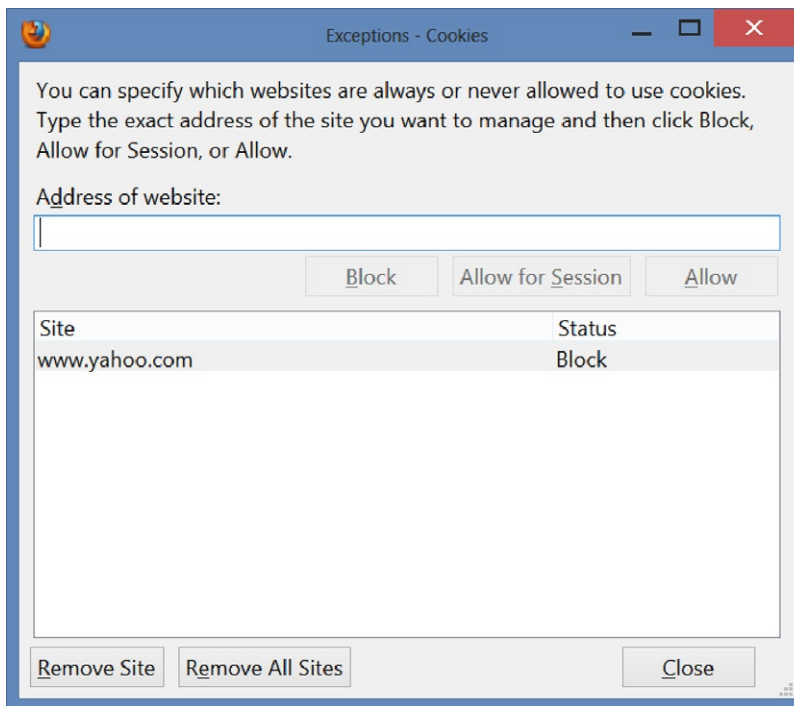
To completely disable all cookies, uncheck the check box next to “Accept cookies from sites.” You can optionally leave cookies enabled but disable cookies, which are created by what are called third parties. Third-party cookies are cookies that are created by one website and are used by another website. An example is the Stack Exchange family of websites such as [games.stackexchange.com](http://games.stackexchange.com) and [programming.stackexchange.com](http://programming.stackexchange.com), among other websites within the family. Along with the Stack Exchange websites, there are other sites within the network of websites called Server Fault ([www.serverfault.com](http://www.serverfault.com)), Stack Overflow ([www.stackoverflow.com](http://www.stackoverflow.com)), and User “Something” ([www.userflow.com](http://www.userflow.com)). Because the main pages of the website names “stackexchange,” “serverfault,” and “stackoverflow” are all different, they are considered to be different sites; however, they are configured to share a username and password for all the sites, and when you sign into one website, [www.serverfault.com](http://www.serverfault.com), for example, and then view the [www.stackoverflow.com](http://www.stackoverflow.com) website, the second site will know automatically that you are logged in and who you are.

**NOTE****How much of a risk are third-party cookies?**

The risk that comes with third-party cookies all depends on what sites you use that use third-party cookies and the sites that you use that attempt to read those third-party cookies. If you don't use any sites that use third-party cookies, then there is no risk as by default when websites create cookies they are only available for use by that specific website. In order for a cookie that was created by one website to be accessible by another website, the website that creates the cookie must specify that the cookie be created as accessible by other websites.

If you wish to configure specific websites to not support cookies within Firefox, this can be easily enough done via the “Privacy” tab shown in Figure 1.4. When the “Privacy” tab is open, clicking the “Exceptions” button will allow you to configure that specific websites will be configured to either allow or block the use of cookies as shown in Figure 1.5.

Within the Exceptions page, simply enter the address of the website as shown such as [www.yahoo.com](http://www.yahoo.com) and click either the “Block,” “Allow for Session,” or

**FIGURE 1.5**

Specific cookie exceptions in Firefox.



“Allow” buttons. Using the “Block” button will prevent Firefox from ever accepting a cookie from the specified website. Using the “Allow” button will always allow the website to create and use its cookies. Using the “Allow for Session” button will allow the website to use cookies but only while the web browser is open. When Firefox is closed and reopened, the website will no longer be able to use cookies.

Within the Options window on the “Privacy” tab you can configure how long Firefox should keep the cookies. By default, the cookies will be kept until they expire, typically for 2 weeks or longer depending on how the website has been configured. The other options for how long to keep the cookies are “I close Firefox” and “ask me every time.” By selecting “I close Firefox,” the cookies will be kept until the Firefox web browser is closed, at which time, all the cookie files will be deleted. By selecting the “ask me every time,” the user will be prompted to select how long the cookie should be saved for each time that a new cookie is created.

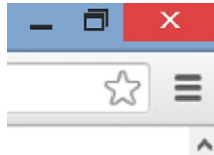
### ***Turning cookies off in Chrome***

Much like the other major web browsers, the Chrome web browser made by Google, Inc., can be configured with various cookie settings. In order to change the cookie settings within Google Chrome, click on the menu button at the upper right of the Chrome web browser as shown in [Figure 1.6](#).

Once the menu has opened setting the “Settings” option from the context menu. Scroll to the bottom of the page that is shown and click the “Show advanced settings...” link that is typically shown in blue. When the additional menu options appear within the “Privacy” section, click the “Content settings...” button. Within the Cookies section, shown in [Figure 1.7](#).

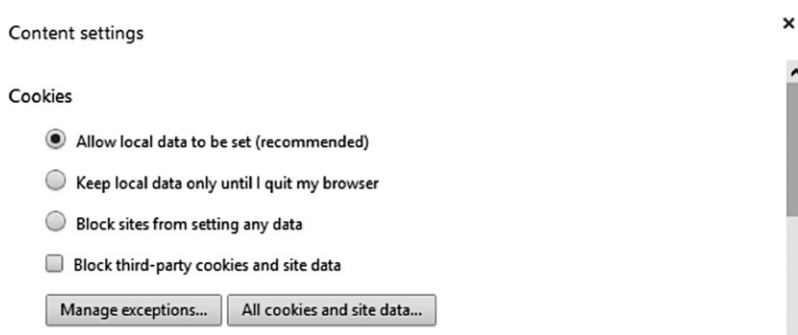
Google Chrome allows for much the same set of settings as Mozilla’s Firefox browser. By default, Google Chrome uses the setting “Allow local data to be set.” This setting allows the Chrome web browser to save cookies to the computer. The setting “Keep local data only until I quit my browser” allows the application to save the cookie but only until Chrome is closed. Once Chrome is closed, it will automatically delete all of the cookies.

The setting “Block sites from setting any data” will prevent Chrome from using any cookies. The check box “Block third-party cookies and site data” will allow sites to use cookies but not third-party cookies.



**FIGURE 1.6**

The menu button within Google Chrome.

**FIGURE 1.7**

Cookie settings within Google Chrome.

**FIGURE 1.8**

Chrome's cookie setting.

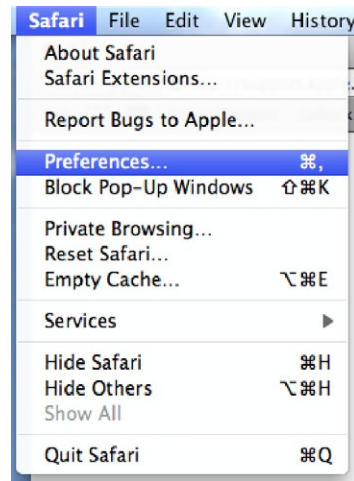
By clicking the Manage Exceptions button, the option to configure exceptions to these rules is set. This screen is shown in [Figure 1.8](#). To add an exception, enter in the site that you wish to set the exception for, and select the kind of exception from the “Behavior” drop-down. When you are done entering the needed exceptions, click the “Done” button to save the settings.

### ***Turning off cookies in Safari***

Turning off the cookies in Safari on the Mac operating systems is just as easy as using the Windows web browser, which were discussed previously in this chapter. To make the change, simply open the Safari web browser. Then, click the Safari

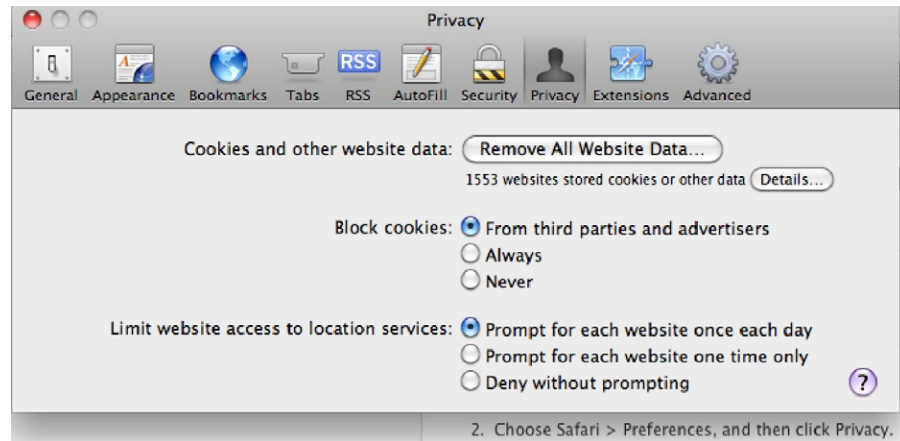
drop-down menu at the top of the screen and click on Preferences from the drop-down menu as shown in [Figure 1.9](#).

When the Settings window opens, select the Privacy button at the top of the window that will open a window similar to the one shown in [Figure 1.10](#).



**FIGURE 1.9**

Safari drop-down menu.



**FIGURE 1.10**

Safari privacy settings.

From the privacy settings page shown in [Figure 1.10](#), you have the option to block all cookies from third-party websites by selecting the “From third parties and advertisers” option. You can prevent all cookies from being used by selecting to “Always” block cookies, or you can allow the use of cookies by all websites by selecting the “Never” option.

## SUMMARY

Protecting your information and your privacy, which really go hand in hand, starts with knowing how much information you should be giving to companies on the Internet. The more information you give to these companies, the more information that will be available for these companies to sell or trade to other companies. As you give away information to companies, you lose control of the information, leaving it up to a company that doesn’t have your best interest at heart to decide what to do with information about you.

When it comes to browsing the web, understanding the technology that drives the web, specifically within the web browsers that we use to browse, the Internet, and the cookies that are used to track us is key in keeping your personal information, personal. Only allowing companies that you trust to use cookies can make your web browsing experience a little less seamless at times, but the trade-off is well worth it in regard to data privacy.

# Username and Passwords for Websites

# 2

---

## INFORMATION IN THIS CHAPTER

- Picking a username
- Picking a password
  - “Strong” passwords
- Unique passwords
  - Remembering all your passwords
- Two-factor authentication
- The more important, the longer they should be

This chapter talks about how to select usernames and passwords that are easy to remember while being hard for someone else to figure out so that people can’t easily get into your accounts.

---

## PICKING A USERNAME

When getting signed up for a website, you are asked for a variety of information such as your name, address, phone number, e-mail address, and, most importantly, a username and password. Selecting the username and password is very important. This is especially true of the username as often you can’t change the username once you have signed up for the service.

When picking a username, it is important to select a username that is easy to remember but isn’t going to be all that easy for someone to guess. If the username is displayed, on a chat forum website, for example, then this obviously becomes much less important as the username will probably be displayed on the website for all the users to see. At the very least, when selecting usernames for use on Internet websites, you want to have two different usernames, one for casual use websites like Twitter, Facebook, and any other sites that you use and a second username for use on sites that would include your banking websites and any other sort of financial institution’s websites. The reason for this is that while many websites out there take a lot of care in ensuring that their customers’ information isn’t going to be compromised, it isn’t worth the risk of using the same username for multiple websites. There have been several data breaches that have happened over the years. One in particular

affected people across the widest range of social factors because the data breach happened to users of the website [eHarmony.com](http://eHarmony.com). You can read more about this data breach at <http://basicsofdigitalprivacy.com/go/eharmony>. When part of the user list for eHarmony was leaked, this was a wake-up call to a lot of people about how they should be setting up usernames and passwords for websites as anyone who was using the same username and password for their eHarmony account and for their banking information had just had someone else have access to their banking username and password.

Many people like to use their e-mail address for their banking website or credit card company website. Doing this is very convenient as it is very easy to remember your own e-mail address. However, if the attacker is able to figure out your e-mail address, which really isn't all that hard most of the time, you've now given the attacker one of the two pieces of information required to get into your bank account. Because of this, it is recommended that you use a username that is not an e-mail address for all banking and financial websites. This way, if someone was going to attempt to break into your online banking profile, they wouldn't have access to your username just by knowing what your e-mail address is. If you have multiple e-mail accounts using one for social networking and friends to contact you on and a second e-mail address that is used only for banking information, then using the e-mail address that you only use for banking information should be a fairly safe practice, but only if that e-mail address is never given out to anyone other than the bank.

---

## NOTE

### Usernames in the real world

It is all well and good to tell people to pick a username that is hard for others to figure out. In reality, this usually doesn't work out all that well. Many websites that have any sort of chat board or social networking aspect to them will publically display the username on the website. For websites that have a chat feature or a social networking component and that show the username on the site, make sure that you select a username that is different from the username that you use on sites such as banking websites and other websites that handle your financial data.

---

When selecting the username, make sure that you don't include any sort of descriptive information in the username. Specific things to avoid include where you live or were born, your birthdate, or any information beyond your name that could be used to identify you other than your name. Beyond these simple rules, your username can be just about anything that you want. The reason that we don't want to include any sort of additional personal information in the username is that this personal information will probably be used as the answers to the security questions that you would need to answer if you forgot your password. While putting something like the year of your birth into the username, `marks1972`, for example, will probably make it more likely that the username is available, you've just told a potential attacker what one of the answers to the security question is. A perfect example of figuring this information from someone else is shown during a video that was

recorded during the Defcon conference in 2010. You can watch this video at <http://basicsofdigitalprivacy.com/go/StolenComputer>. This video does have some language that one might find offensive, be warned. The presentation starts about 3 minutes into the video, and the part where the presenter talks about using the usernames to figure out the birthdate of the person who stole his computer starts about 13 minutes into the video.

---

## NOTE

### Where “mrdenny” came from

- I often get asked how I came up with the handle and username “mrdenny.” The story is actually shockingly boring. When I begin working for the Internet Service Provider (ISP) EarthLink Network in Pasadena, CA, we had to select e-mail addresses for our personal accounts, which we got as part of working there. The e-mail address [denny@earthlink.net](mailto:denny@earthlink.net) had already been taken by another person, which really surprised me, and at the time we couldn't reuse e-mail addresses, even if we worked there.
  - The instructor in the training was named Don Taylor and when we started he chose mrdontay as his e-mail address. So I decided that was a good idea and went with [mrdenny@earthlink.net](mailto:mrdenny@earthlink.net) figuring that I could always change it later. Well it turned out that I ended up liking the username and it ended up sticking with me. Sadly I don't own that first e-mail address anymore from EarthLink Network (now known as EarthLink, Inc.) but the handle mrdenny has stuck around for the last 15 years or so. Because I've been using it for so long, people know that they can find me on Twitter, Facebook, and lots of other sites using the username.
  - While you may not have a similar story for selecting your username, having a handle that's easily recognizable as you makes it easier for people to figure out if it's you or not.
  - Of course, I only use the username “mrdenny” for my public persona; for things like banking, I use a completely different username, which I'm the only one who knows.
- 

---

## PICKING A PASSWORD

Picking a password requires much more care than picking your username. Passwords should be strong and unique for each website. Passwords that are strong have very specific characteristics. There are four groups of characters on the standard keyboard: lowercase letters, uppercase letters, numbers, and special characters (typically found on the number keys when you hold the shift key down). For passwords to be considered strong, they need to contain at least three of those four types of characters. If you use all four of types of characters, that is even better. In addition to using at least three of the character types, the password should be at least eight characters long. The reason that we want to have passwords to be long is to increase the complexity of the password. The more complex the password is, the harder it will be for someone to brute-force attack the password. This is talked about more in the following section. The end result of a password that is very long is that it takes someone so long to attempt to guess the password by using a brute-force method that they simply give up and move on to another person to attempt to attack.

### How passwords are figured out

There are a variety of ways for an attacker to figure out what the password for an account is. The first way is the one that is specifically related to having a long and strong password and is the only method of attack that you, the account owner, can help prevent. This attack method is called a brute-force attack. In this kind of attack, the person who is trying to figure out the password basically tries every password possible starting with just a single character up to a password as long as is needed. This is done with scripts and applications that are specifically designed to try the same username with different passwords over and over very quickly. These applications can try usernames and passwords basically as quickly as the website or the application can try the username and password. Websites that are properly built will have protection for a brute-force attack built into the website. This protection will be to only allow a specific number of failed log-in attempts before the user's account is locked so that no further attempts can be tried. You may have run into this sort of protection on the website when attempting to log into the website and you can't remember the password. After a few tries (the specific number of tries is completely up to the website developer), the account is locked and you have to either call their customer support department or go through the forgot password process in order to get the account unlocked.

The longer the password is, the longer it will take for the password to be figured out. Just a few years ago, it could take months or years to figure out a password. While just a few years later, a password can be figured out in just days and for just a few dollars. The reason that this is the case is because of the power of cloud computing. Back in the olden days of technology, also known as the mid-1990s, if someone wanted to break into an account, the person trying would typically only have one or two computers at their disposal. In today's world of cloud computing, hundreds or thousands of computers can be rented from various cloud computing providers for just a few dollars, and all of these computers can be used all at once to try all the various options of passwords all at once. The economics of the cost to brute force a password are changing very rapidly. However, a great article was put together in October of 2009 by a company called Electronic Alchemy and can be read at <http://basicsofdigitalprivacy.com/go/passwordcosts>.

Other attack methods involve the attacker breaking into the website through other methods that aren't anything that we, the end users of the applications, can do anything about. In these attack methods, the attacker downloads the usernames and the encrypted passwords from the website's database. The attacker then attempts to break the encryption on the passwords. Unfortunately, there is nothing that you as the end user can do to prevent this sort of attack. You as the user of the website need to trust that the website is encrypting the passwords with a strong level of encryption so that if the passwords are attacked, it takes as long as possible to get through the encryption. This leads directly into our next section.



## Unique passwords

Every website and application that is used should have a different password setup for it. This makes figuring out which password is used for each application difficult, but it makes the passwords much more secure. The reason that we want to use different passwords for each website is so that if one password is compromised, the attacker doesn't get access to every website that you use.

When setting up unique passwords, do not include the name of the website as the unique part of the password. Doing so is basically the same as not putting any sort of unique value into the password field as the attacker will easily enough know what the unique value is in your other passwords. For example, if the part of the password that doesn't change was "password" using this format we could put the website name after the password. So if the website that the account was being set up for was [www.bestbuy.com](http://www.bestbuy.com), having the password of "passwordbestbuy" would tell the attacker that your password for [www.target.com](http://www.target.com) would be "passwordtarget" and the password for [www.ebay.com](http://www.ebay.com) would be "passwordebay," and so on.

### *Creating unique passwords*

There are a variety of applications that can be used to help you create passwords that should be totally unique for each website. None of these applications are really any better or worse than others. The important thing is that an application is used as they will create passwords that are very random. Different password-generating applications do this in different ways.

---

## NOTE

### **Very random is not truly random**

If you are a mathematician or other scientist, you are probably looking at the output from your favorite password generator and about to send me an e-mail that they aren't truly random. Yes, I'm aware that password generators aren't actual random as they use random number generators within the software in order to create the password. While they aren't truly random, they are close enough to truly random for the general public to understand that they are random.

While the software does use a predictable algorithm to create the random password, this is ok. In order for someone to be able to recreate the password, using the password generation software would require that they use the same software and the same exact computer and the password will need to be generated at the exact same moment in time. The reason for these requirements is that each piece of software that generates passwords will have its own algorithm that is used to create the password. These pieces of software use the internal device IDs from the computer that they are installed on as well as constantly changing values, such as the date and time, as parts of the algorithm that is used to create the password. This allows for many passwords to be created in a short period of time while having them all be totally random from each other.

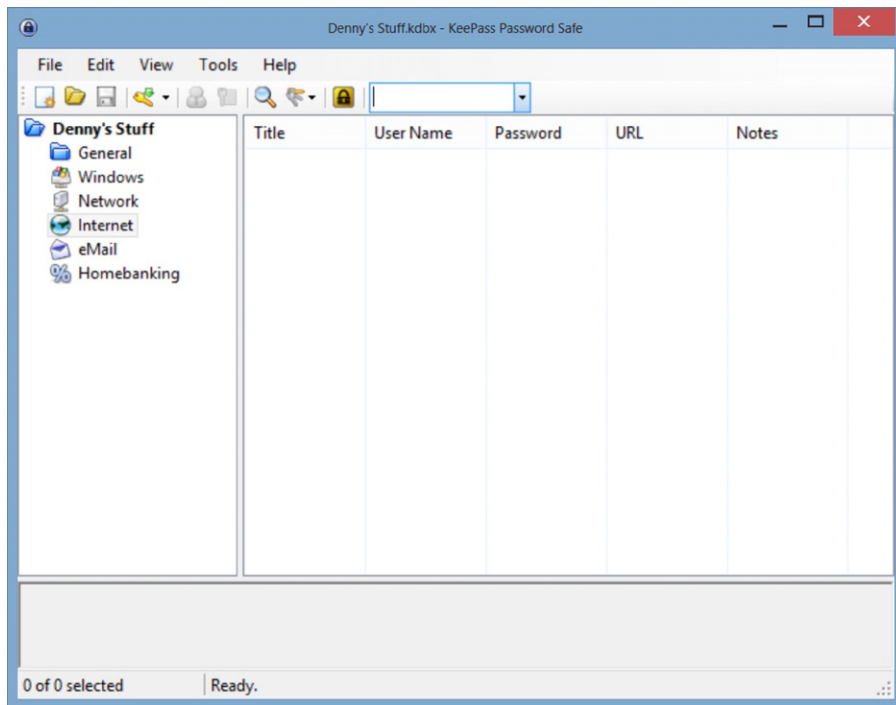
---

One of the password-generating applications is called KeePass. KeePass does a few things for you as the user. The first thing that this application does is create new

passwords that are very long and very strong. This allows you to have a truly random and very long password for each unique website that you use. The second thing that the application does is store the passwords in an encrypted database that makes it so that you don't need to memorize all of these long and strong passwords that are basically impossible to memorize. The passwords within KeePass are stored with usernames as well as the website that the username and password are for, making it very easy for you to copy and paste the information from the KeePass application into the web browser when you need to log into the website.

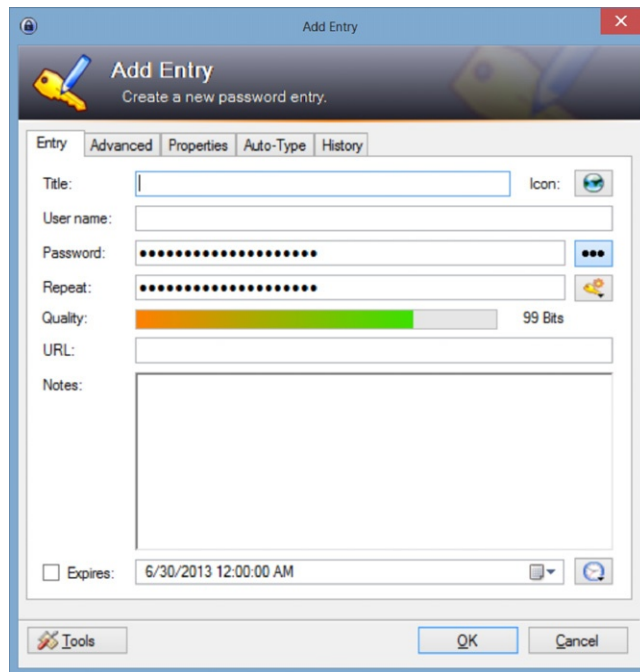
Using KeePass to create these unique passwords and store them is quite easy. After downloading the KeePass application from [www.KeePass.org](http://www.KeePass.org) and installing the application, open the application and you should see a screen similar to the one shown in [Figure 2.1](#).

Select the menu item on the left where you want to save usernames and passwords; typically this would be under the Internet option. Right click on the white area on the right-hand side of the screen and select "Add Entry" from the context menu that appears. This will open a window similar to that shown in [Figure 2.2](#).

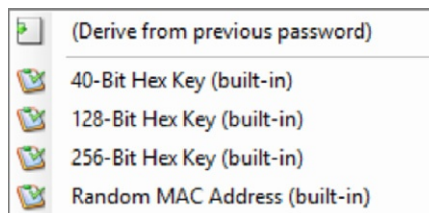


**FIGURE 2.1**

KeePass home screen.

**FIGURE 2.2**

Add Entry screen within KeePass.

**FIGURE 2.3**

Profile Generation Drop-down Menu.

In the title field, enter a title of the entry; typically this would be the URL for the website, for example, [www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com). In the username field, enter the username for the website that you will be using. The password field and the repeat field are already filled out. Clicking the button with three dots on it will show the generated password. If a more secure password is desired, click the button below the button with three dots, then select “Generate Using Profile,” and then select either the 128-bit profile or the 256-bit profile as shown in [Figure 2.3](#).

In the URL field, enter the URL for the website. Clicking the OK button saves the setting into the KeeSave application's database.

---

**NOTE**

When setting up KeePass or any other password database like KeePass, there is one password that is very important to always remember, that is, the password to the KeePass database. Without this password, you will lose access to all the passwords that were saved within the application. The password that is used for the KeePass application should be a secure password and should not be written down anywhere that anyone can find it. Putting a copy of it in a safe deposit box at the bank would be an acceptable place to store a copy of it; however, you wouldn't want to keep a copy of it within your home unless you have a wall safe or some other very secure place where it can be stored.

Somewhere that some people like to store the written down version of their KeePass password is in the freezer. Now don't just stick the piece of paper in the freezer; that won't do you much good as the moisture within the freezer will destroy the paper pretty quickly. Instead, you'll want to put the paper into a ziplock bag or better yet a suction bag where you can remove all the air from the bag. Then put the bag with the paper inside it at the very back of the freezer or under all the stuff in the freezer. To make the password more secure, you can get a small cookie tray that is just a little bigger than the paper. Freeze a small amount of water in the bottom of the tray. When it is mostly frozen, put the bag with the paper in the tray, then cover the bag with more water, and put it back in the freezer. The next day you'll have the bag with the paper in it suspended in ice. Remove it from the tray and put the block of ice in the back of the freezer or under everything. This gives you access to the password, but you'll have to wait a while before you can get to it without damaging the piece of paper.

---

Modern web browsers can all store usernames and passwords in a secure manner so that you don't have to type in the username or password or to copy and paste from the password application. The passwords are stored within the web browser setting as encrypted values so the risk of the values being stolen from the web browser settings is very low. That being said, most web browsers make it very easy, sometimes too easy, to view the passwords on the screen. Usually, you just need to go into the settings screen for the various web browsers and there will be a button somewhere where you can view the passwords that are saved. This protects your passwords from being downloaded by someone, but not from someone who sits in front of your computer and has access to view the screen.

**Passphrases**

A great option when picking a new password is to instead use a passphrase. A passphrase is a normal English (or other language) phrase that you use as your password. An example of a great passphrase to use could be a quote from the Beatles song "A Hard Day's Night" such as "Itsb3enaharddaysn!ght" which takes the phrase "It's been a hard day's night" from the song, removes the spaces, and changes a couple of characters from letters to numbers and characters. Normally, passwords which are considered to be strong are very hard to remember because they are long and have numbers and characters placed throughout the password. Normal passwords are often hard to remember while passphrases which are based on songs, TV shows, movies, famous quotes, etc., are very easy to remember.

---

## TWO-FACTOR AUTHENTICATION

Another fantastic way to ensuring a unique password for websites is to use a system called two-factor authentication. With two-factor authentication, there are two pieces of information that are required. The first is a code that you as the user know and the website stores in their system. The second piece of information is a randomly generated number that is generated by either a key fob, an application on your phone, an application on your computer, or a text message sent to your cell phone. Both pieces of information are put into the website's password field when logging into the website.

Two-factor authentication is nice because the passwords can only be used once, and the random values are only valid for a short period of time. For example, if using a key fob, the key fob generates a new value every 60 seconds and if the password isn't used within the 60-second window, the password becomes invalid and not able to be used.

As of the time of the writing of this book, in the summer of 2013, there were a wide variety of companies who have made two-factor authentication systems. However, most if not all of these applications are specific to just one or two companies with few companies making their two-factor authentication systems available to other websites or applications. This means that when using two-factor authentication via your phone, you may end up having to have several applications installed on your phone.

### Using fob-based systems

Fob-based two-factor authentication systems are probably the oldest example and the easiest to use. The fob, shown in [Figure 2.4](#), doesn't require any user interaction to use other than to enter the information into the website or application when prompted.

These fob-based systems require that you have two pieces of information when using the fob. You need to have the actual device that has the changing number on it as shown in [Figure 2.4](#), but you also need to know a static value that doesn't change. When logging in with the fob, you take the static value that you know, for example, 1234, and then put the value from the fob after it. Using the value from [Figure 2.4](#), this would mean that the password that would be used to log into the website or application would be "1234497364."



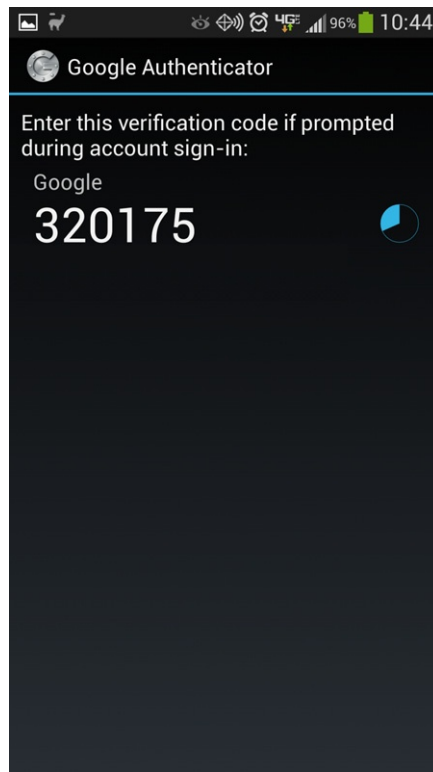
**FIGURE 2.4**

Picture of a fob used for two-factor authentication.

### Using software-based two-factor authentication systems

Software-based two-factor authentication systems, shown in [Figure 2.5](#), work in a very similar method to the fob. The big difference between using the fob-based method and using a software application-based method is that instead of needing a fob for each website that you wish to use, you simply use a single application (or two applications if some websites use Apple's system and others use Google's system). This also prevents you from having to carry and track these additional physical fobs instead of putting the two-factor authentication within a device that you are already going to carry with you at all times anyway. Whenever you are using two-factor authentication on your cell phone, be sure to secure your cell phone with the most secure method available on the phone. If you don't and the phone is lost or stolen, then whoever has the phone also has all of your two-factor authentication codes as well.

In order to use either Apple or Google's system when prompted, simply bring up the application on your mobile device and select the site that you wish to use. Then, enter the number as prompted.



**FIGURE 2.5**

Showing Google's two-factor authentication program.

## Using a text-messaging-based system

Using a text-messaging-based system is just about as easy as using the other systems that have been discussed in this chapter. When using a text-messaging-based system when beginning the log-in process, the website requests a username and a password. Upon entering the correct username and password, the cell phone that is tied to the account is sent a text message that includes a pin code, which can only be used once to log in. The webpage then prompts you to enter this pin number into the website. Typically, when using these pin-based systems, a wrong pin number can only be used three to five times at which point a new pin number is needed. This prevents someone from simply trying all the possible pin numbers to find the correct one.

These text-message-based systems are considered to be pretty secure. One of the reasons for this security is due to the fact that with text messaging, the text message is only delivered once. Even if someone took a SIM card from one cell phone and inserted it into another cell phone, the old text messages wouldn't be downloaded again. Even if someone was able to gain access to the older codes that had been texted to someone, those codes shouldn't be valid codes anymore. While it is up to the company that sends the text message to determine how long the codes are valid for, it is usually a short window of time usually just a few minutes or up to an hour.

---

### NOTE

#### **Not all two-factor authentication is created equal**

While one hopes that all the companies that are using two-factor authentication are doing it correctly, this sadly isn't the case. One prime example is on the Bank of America website. When Bank of America first introduced their two-factor authentication, they did a very, very poor job implementing it. The Bank of America two-factor system is only used to protect the wire transfers and bill pay sections of the website. So far, this sounds like it is set up correctly. While the main part of the password is only protected by the user's password (which isn't great but it'll do), you have to use the two-factor authentication in order to actually get money out of the account.

The problem with Bank of America's implementation is that to add a cell phone as a two-factor device all, you have to do is log onto the Bank of America website and add the phone to the account. While I'm sure this was done to make it more convenient for their customers, it shows a lack of understanding on the part of the bank on how these systems should work.

The problem with this implementation is that the two-factor authentication is only protected by the primary authentication method, in this case the user's password. For this system to be done truly properly, adding a phone device would require going into one of Bank of America's branches and presenting them with proper identification to prove that you are the owner of the account and that the phone number that you wish to use does in fact belong to you.

With the system as it is (as of the writing of this book in the summer of 2013), anyone who has the password for the account has the ability to add a phone to the account; then using that phone, transfer all the money to another account or to an account at another branch.

---

These text-message-based two-factor authentication systems work fairly well for most people and are typically very secure as the odds of someone who is attempting to break into your account having physical access to your cell phone is minimal. However, these systems are not perfect. The biggest problem with them is that they typically require that you are physically located in your home country. While this

isn't an issue for many people, for those that travel internationally on business, this prevents those customers from having access to the account while they are outside the country. The reason for this is that most international travelers do not use International Roaming on their cell phones when in other countries. The first reason is the cost as cell phone companies charge incredibly high rates when traveling in other countries. The second is that in a lot of cases, the needed cell phone network simply isn't available in other countries. The perfect example for this is the CDMA network that Verizon's cell phones use. As of the writing of this book in the summer of 2013, there was little to no CDMA network in Europe, so if a traveler needed to receive a text message via their cell phone and they were a Verizon customer with their normal cell phone in Europe, there would be no way to receive the text message.

---

## NOTE

### Installing Windows 8 and two-factor authentication

I recently had a chance to install the new (as of the writing of this book in the summer of 2013) beta version of the Windows 8.1 operating system on a new computer that I had purchased. Before installing Windows 8.1 on this computer, I had been using the Windows 8 operating system on all of my computers and all of my computers were using the Microsoft account (formally called a Windows Live account) to log into all my computers. As part of using your Microsoft account, you configure a cell phone number so that you can approve adding new computers to your Microsoft account for authentication.

As part of the installation process for Windows 8.1, I was prompted for my Microsoft account information just like before, but during the installation process right after specifying my Microsoft account information, I was prompted on the computer screen to enter a confirmation code. Before I could finish reading the instructions on the screen that told me that Microsoft would be sending me a text message, my phone had already beeped telling me that a new text message had been received. I entered the text message and moved on with the installation.

This was frankly one of the easiest two-factor authentication processes that I had seen in quite a while.

---

---

## THE MORE IMPORTANT THE LONGER THEY SHOULD BE

The usernames and passwords for some websites have become more important than others in recent years. This isn't because of the information that the website contains but instead because the website grants you access to other websites. This is done through a system called OAUTH (pronounced o-auth) where a website allows its username and password system to be used by other websites. This is good for the website that allows its username and password system to be used via OAUTH because it makes the OAUTH website more important in the global Internet system. This is also good for the websites that are using the OAUTH service on the other website because the website that is using the OAUTH service doesn't need to store their own username and password.

Due to the fact that the website that has the OAUTH service can be used to sign into many other websites, the password that is used for these websites should be the



strongest password possible. There are many different websites out there that can serve as OAUTH providers. This includes websites like [openid.com](http://openid.com), [myopenid.com](http://myopenid.com), [Verisign.com](http://Verisign.com), and other sites like [google.com](http://google.com) and [facebook.com](http://facebook.com). It doesn't matter which of these sites is used to sign into the various other websites, but whichever one (or ones) is used, the password that is used should always be the strongest possible password. Using the techniques like the ones talked about in the "Picking A Password" section earlier in this chapter will help you to ensure that you have a strong password that is secure and will prevent others from gaining access to all the other websites that you use.

## SUMMARY

Having strong and unique passwords is key to protecting yourself in today's world on the Internet. While we like to think of the Internet as a nice peaceful place where everyone can get along, the reality is that the Internet is more like the Wild West than a peaceful place. There are lots of people out there who want to take your money and your identity and use it for their own purposes, which usually aren't going to turn out well for you. Protecting yourself proactively is the only way to ensure that you aren't taken advantage of online.

# Your Home Network

# 3

---

## INFORMATION IN THIS CHAPTER

- Securing your router
- Securing your Wi-Fi network
  - Wi-Fi encryption options
  - Hiding your wireless network
  - MAC address filtering
- Letting others onto your Wi-Fi network
- Other devices on the network

In this chapter, we will be discussing proper ways to secure your home network so that people aren't able to get onto your wireless network without your express permission.

---

## SECURING YOUR HOME NETWORK

A shockingly easy way for people to access your home computer is via your home network. An improperly configured home network would allow any attacker on the public Internet to contact your home computer and attempt to install a virus or key logger on it. Another potential point of vulnerability for many home networks is the Wi-Fi network. An incorrectly configured Wi-Fi could, while appearing to be secure, actually be completely insecure. Using someone's incorrectly secured Wi-Fi to gain access to their files and information does require that they are close to your home, typically within just a few hundred feet. This doesn't however give any level of protection because people often do "war driving" where they simply drive around a neighborhood looking for unsecure Wi-Fi networks that they can use. Once gaining access to an unsecured Wi-Fi network, the person could be attempting to break into the owner's computer remotely, or they could use the Wi-Fi connection to perform some sort of illegal act such as viewing or downloading child pornography, hacking into a company or government computer network, stealing music or software, or any number of other activities.

---

**NOTE****You may be legally responsible for what others do on your computer network**

The law on this varies from country to country, state to state, and in some cases city to city. In some jurisdictions, judges are ruling that the owner of the Wi-Fi is responsible for properly securing the Wi-Fi and ensuring that everyone who is using that Wi-Fi is doing only legal operations. This means that if you haven't taken the proper steps to properly secure your home network and someone uses your home network to steal music, you could be held financially liable when the music industry association (RIAA in the United States) attempts to sue the music pirate.

The same goes for if someone was to connect to your Wi-Fi network and download child pornography. You could then be charged as an accessory after the fact for the main crime of child pornography. This would carry a heavy fine and possible jail time, and depending on the judge and the sentencing requirements, the Wi-Fi network owner could end up being required to register as a sex offender for in the end having Wi-Fi at home and not setting it up correctly.

While the odds of this happening are slim, it is certainly possible, and that should be enough to scare anyone into correctly setting up their Wi-Fi to prevent people they don't know from getting on the Wi-Fi at their home or office.

---

**Securing your router**

When you have high-speed Internet access such as cable Internet or a DSL service, you will have some sort of router. The router may be a device that was purchased by you or it could have been provided by your Internet service provider. Routers come in a variety of shapes and sizes, a variety of which are shown in [Figure 3.1](#).

If the router is not properly secured, it could leave the home network vulnerable to attack from an outside attacker via the Internet. The first thing to ensure that the home network is protected is by having a home router. Most (but not all) home Internet service will provide two devices that are used to connect the home computers to the Internet. Cable Internet services will typically provide a cable modem and a router, while DSL services will typically provide a DSL modem and a router. Some of these services such as the AT&T U-verse service will provide you only with a single device that serves as both the DSL modem and the router in a single device.

**FIGURE 3.1**

A sampling of home routers.

---

There are a couple of different software components within the home router that help secure the home network from the potential hackers who are on the Internet. These two main components are the use of a technology called network address translation (NAT) and the network firewall.

---

## NOTE

### **What are the odds that someone will attack my home network?**

A question that gets asked a lot when talking about home network security, specifically with regard to securing the home network from Internet attackers, is what are the odds that someone is going to try to attack my home network from the Internet? The answer is a pretty basic one, 100%. Attackers are constantly looking for open computers and networks to attack. Several studies have been done over the years where brand new computers are placed on the Internet and left there to see how long it took for people to begin attacking the computer, and then how long it would take to compromise the computer by getting viruses installed on it. Within one hour's time, not only had the attacks started but the computer also had several viruses installed on it that were all competing for resources. One of my favorites can be read about at <http://basicsofdigitalprivacy.com/go/honeypot>.

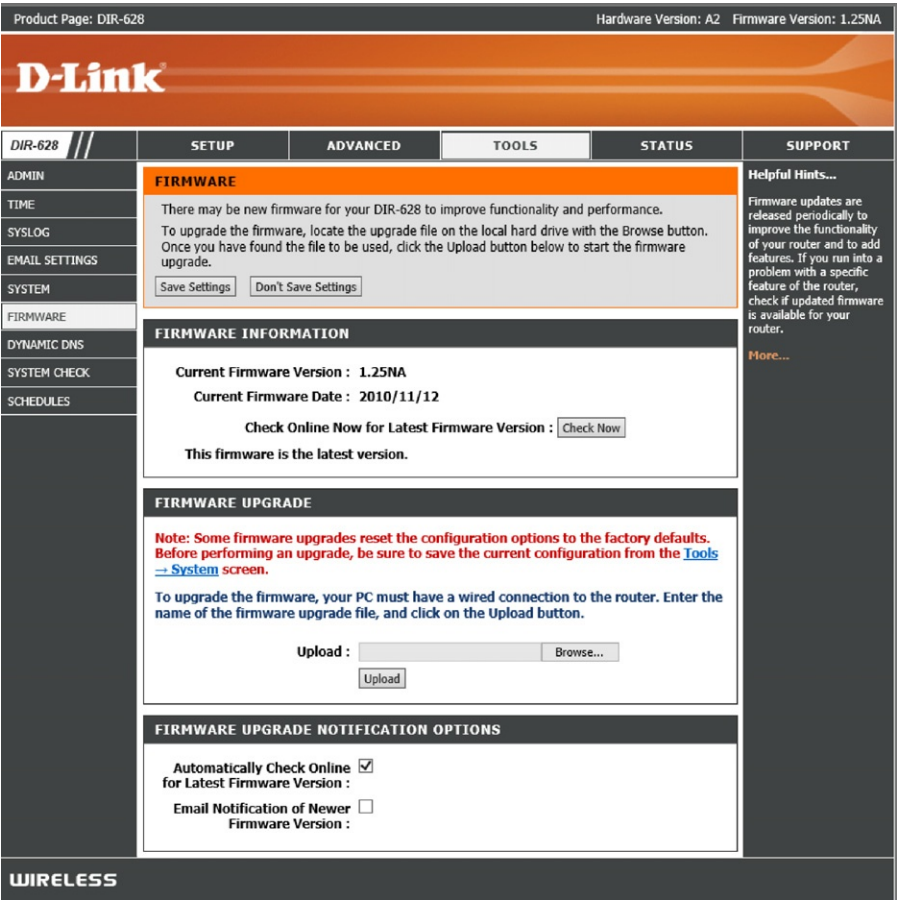
---

How each of these routers is configured will vary depending on the router and the version of the software that is installed. Many of these routers ship with older software than is currently available for these routers. Updating the software on the router requires logging onto the router itself using a web browser. There will be instructions, which came with the router, that tell you how to connect to the router and what the default username and password are if you haven't changed it. If you don't have that documentation handy, a quick Internet search for "{your router model} documentation" where {your router model} is the actual model number found on the back or bottom of your router will usually find the documentation. Once you are logged onto the router, you'll need to find the firmware page. This will usually have some sort of way to check if the firmware is up-to-date, or at least it will have a link to the manufacturer's website so you can manually check that the firmware is up-to-date. You can see the firmware page for a D-Link router in [Figure 3.2](#) and the router update page for a NetGear router can be found in [Figure 3.3](#).

Not all routers can be updated manually. An example of this is the router that the AT&T U-verse service ships to you. The reason that this router can't be updated manually is because AT&T pushes new firmware to the router automatically when there are updates available so the router is always current. They can do this because the router is provided as a part of the service and it is partially managed by AT&T as a part of the U-verse service. Some providers offer this level of services but many do not. You'll need to check with your service provider to see if they handle this for you.

### ***Network address translation***

NAT is used for a couple of different reasons within home routers. The first reason is due to the fact that Internet service providers typically only issue one public IP address to home network customers. IP addresses are the way that computers talk to each other over the Internet. Every computer or device on the Internet needs to



**FIGURE 3.2**  
D-Link firmware update page.

have an IP address, and with the Internet service provider only providing a single IP address, a way is needed to give multiple computers and other devices within the home network access to the Internet by sharing that one IP address.

**NOTE**  
**How NAT works?**

At a high level, NAT works by doing a one to many mapping between the public IP address that the Internet service provider gives us to use and the private IP address that our home network uses. The NAT service, which runs within the router, handles this conversion and mapping without any changes or special configuration on the computers.

**FIGURE 3.3**

NetGear router update page.

Because of the mapping that NAT does, which is typically turned on by default, it makes it very hard for potential attackers on the public Internet to access the computers within the home network. This is because network address translation is a one-way process where computers and devices on the home network can talk to the Internet, but a computer or device on the public Internet, a website, for example, cannot connect to a computer on the home network. This feature alone helps protect the home network from an attacker who is trying to access the home computers and the home network.

### **Network firewalls**

Network firewalls are used to ensure that no one is able to connect to the home router. The router will have a variety of management services running on it such as the web-site that is used to configure the router among other services. Because the router is connected to the public Internet, we don't want anyone being able to connect to the router and make any changes on it from the public Internet. Because of that, the router should be configured with the firewall on the router preventing any sort of network access to the router itself, which will typically be configured by the manufacturer of the router before the router is sold. Without having the firewall in place, an attacker could attempt to break into the router, and if they were successful, they would then be able to reconfigure the router to allow themselves access to one or more of the computers or devices on the home network.

## Securing your Wi-Fi network

Incorrectly configured Wi-Fi networks are an extremely easy way for attackers to gain access to personal information, which is being transmitted over the Wi-Fi network, even when the Wi-Fi network is configured to use some of the available forms of encryption. This is because the older encryption standard, called WEP or Wired Equivalent Privacy, is considered to be extremely insecure. There are several flaws in the design and implementation of the WEP encryption system, so any network that is configured to use WEP should be considered to be just as insecure as a Wi-Fi network that doesn't have any data encryption configured at all. In fact, in 2004, the IEEE standards committee, which is the committee that decides what versions of what protocols make it into the final Wi-Fi specifications, had declared that WEP was to be removed from the Wi-Fi specification.

---

### NOTE

#### **This all sounds very technical**

Much of that last paragraph may sound very technical to you if you don't work in the information technology field or a related field, and that's OK. While I really have no desire to go into the history of WEP within this book nor do I really want to dive into all the technical problems with WEP, if you want to read up a little more about WEP, I would recommend starting with the Wikipedia page for WEP, which you can find at <http://basicsofdigitalprivacy.com/go/wep>.

---

After WEP was introduced, but before it was declared as not worth using, a second set of encryption protocols was introduced into the Wi-Fi specification. This new encryption specification is called WPA or Wi-Fi Protected Access and comes in two different versions, WPA and WPA2. WPA was first ratified in 2003, while WPA2 was first ratified in 2004, so they should be available in every modern Wi-Fi router created since then and all modern operating systems. Even older operating systems such as older versions of the Microsoft Windows operating system, which were created before 2003 and 2004, have had patches created that should be installed so that WPA and WPA2 are available on these older computers. Given the option between WPA and WPA2, WPA2 should be the version that is used as it is more secure than the older WPA specification.

Setting up these settings requires configuring the Wi-Fi access point or router with the specified setting. Many of the newer home routers come preconfigured using the WPA2 setting, while older routers did support these secure settings and came with the security settings disabled by default.

### ***AT&T U-Verse router***

Securing your Wi-Fi router requires connecting to the router's webpage. As stated earlier in this chapter, you'll find the information on connecting to your router in your router's documentation. For the AT&T U-verse router as an example, this is changed on the Settings page, then the LAN tab, and then the Wireless subtab.

On this page, there are several settings that can be adjusted shown in [Figure 3.4](#) and specified later:

- The wireless can be enabled or disabled.
- The wireless network name (SSID) can be set manually or the default can be used.
- Authentication and encryption settings can be set.
- The encryption key, which can be either the default one that is on the sticker on the back of the router or your own wireless password.

The screenshot shows the 'Settings' tab of the router's web interface. The 'LAN' sub-tab is selected, and the 'Wireless' section is active. A warning icon and message are at the top: 'Warning: Modifying the settings on this page can impact the ability of devices to access your wireless network.'

**Wireless Interface**

- Wireless Interface:** Enabled (Default: Enabled)
- Wi-Fi Protected Setup:** Status: idle
- Disabled:** Disabled (Default: Disabled)
- Enter WPS PIN:** [Text Field] (Buttons: Use PIN, Push-Button)
- Push WPS Button Remotely:** [Push-Button]

**Network**

- Network Name (SSID):** MyHomeWifi (Default: 2WIRE236)
- SSID Broadcast:** Enabled (Default: Enabled)
- Wireless Channel:** Auto (Default: Auto)
- Current Wireless Channel:** 1
- Check Wireless Channel Availability:** Rescan

**Security**

- Wireless Security:** Enabled (Default: Enabled)
- Authentication Type:** WPA-PSK (TKIP) and WPA2-PSK (AES) (Default: WPA-PSK (TKIP) and WPA2-PSK (AES))
- Wireless Key:**
  - ☐ Use default Wireless Network Key printed on the System Label
  - ☒ Use custom Wireless Network Key [Text Field]

**FIGURE 3.4**

AT&T U-verse-provided router's wireless network configuration.



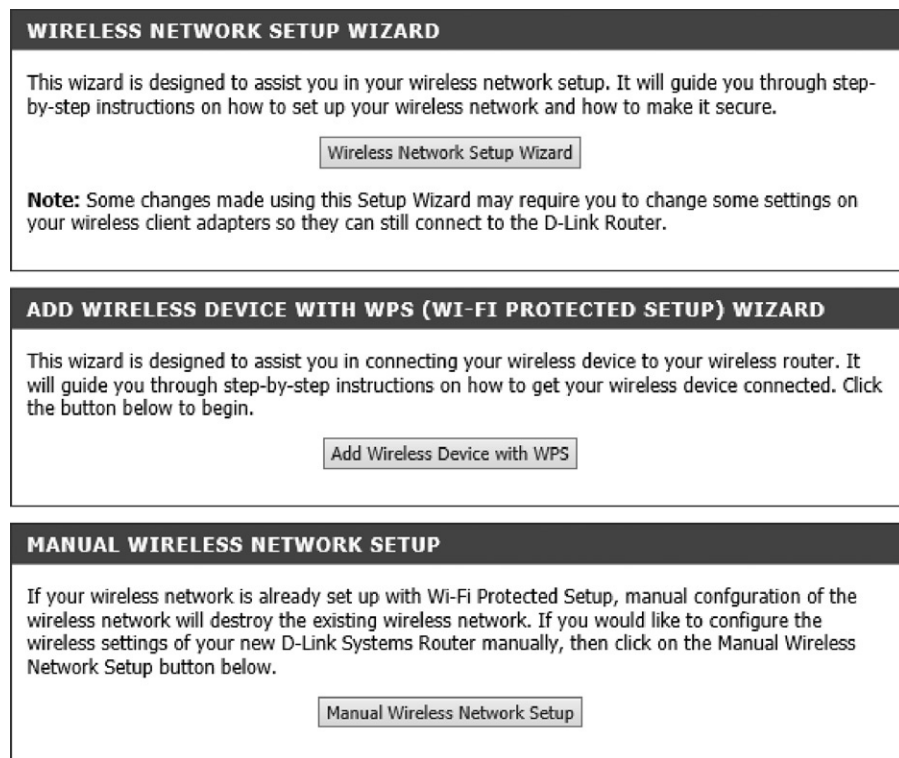
### ***D-Link router***

For the D-Link routers, the Wi-Fi settings are found by clicking the Setup tab at the top and then the “Wireless Settings” tab on the right. Then you can either go through the provided wizard or click on the “Manual Wireless Network Setup” button, which you can see in [Figure 3.5](#).

Selecting the “Manual Wireless Network Setup” button will show you several settings that you can configure, some of which are shown in [Figure 3.6](#) and upon scrolling down the security settings shown in [Figure 3.7](#).

As shown in [Figure 3.6](#), you can see the wireless network name (called the SSID) if you want to use 2.4 GHz or 5 GHz wireless frequency, the Wi-Fi modes that will be used, and the other basic Wi-Fi settings. There is no difference from a security perspective between the two frequencies. Selection of one of the other is simply a preference depending on what other devices you have in your home, which use the same frequencies.

In the security section shown in [Figure 3.7](#), you’ll see the security mode, which in this case is set to WPA-Personal. The WPA section is shown because the mode is set



**FIGURE 3.5**

D-Link wireless settings menu.

WIRELESS NETWORK SETTINGS

Enable Wireless :

☒ Always
 ☐ New Schedule

Wireless Network Name :

MyHomeWifi

x

(Also called the SSID)

802.11 Band :

☒ 2.4GHz
 ☐ 5GHz

802.11 Mode :

Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan :

☒

Wireless Channel :

2.437 GHz - CH 6

Transmission Rate :

Best (automatic)

(Mbit/s)

Channel Width :

20 MHz

Visibility Status :

☒ Visible
 ☐ Invisible

**FIGURE 3.6**

Wireless network settings for a D-Link router.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

Auto (WPA or WPA2)

Cipher Type :

TKIP and AES

Group Key Update Interval :

3600

(seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

.....

**FIGURE 3.7**

Security settings for a D-Link router.

to WPA. This router in this case is allowing for both WPA and WPA2, using TKIP and AES, and the key is updated every 3600 seconds, which is the default setting. At the very bottom of the screen and in [Figure 3.7](#), you'll see the preshared key, which is set to the password that is used to connect to the Wi-Fi network.

---

## NOTE

### what is the difference between 802.11n, 802.11g, and 802.11b?

In [Figure 3.6](#), you see that this router is configured for 802.11n, 802.11g, and 802.11b. These are different versions of the wireless protocol called 802.11. From a security perspective, these different versions are all exactly the same. The first published protocol was 802.11a, the second was 802.11b, and so on. The most commonly used Wi-Fi protocols are 802.11a, 802.11b, 802.11g, 802.11n, and the newest 802.11ac. Each of the newer protocols starting with b, then g, then n, and then ac is faster than the prior versions. Technically, the 802.11a version was faster than the 802.11b version, but the 802.11a version used a different frequency than the 802.11b-802.11n versions. The 802.11ac version is faster than the prior versions but is also using the 5 GHz range much like the 802.11a frequency used. The 802.11n version of the Wi-Fi protocol used both 2.4 and 5 GHz ranges.

While this information isn't specific to security, having this information is important to properly setting up your home Wi-Fi network for maximum efficiency.

---

---

## NOTE

### 2.4 GHz versus 5 GHz?

In [Figure 3.6](#), you'll see something that you don't see in [Figure 3.4](#), which is the ability to select the frequency (called band by D-Link) that the Wi-Fi network can use. Traditionally, Wi-Fi has used the 2.4 GHz range of the wireless spectrum. This is the same part of the wireless spectrum that is used by cordless phones and some other home devices. Because of this and in order to increase speeds, some routers support the use of the 5 GHz range as well. Older routers and older computers won't support this 5 GHz range as it requires different transmitters and receivers.

---

## *NetGear routers*

For NetGear routers, there are two different wireless network settings that are configured, which are accessed via the Advanced tab after connecting to the router and then selecting Setup and then "Wireless Setup." This is because the NetGear router is a brand new device as of the writing of this book in the summer of 2013, and it has both 2.4 and 5 GHz transmitters. The two networks have different names so that the user can identify which network he or she wishes to connect to as shown in [Figure 3.8](#).

Each of these wireless networks shown in [Figure 3.8](#) is configured independently from each other and should only be enabled if they will be used.

The image shows a 'Wireless Setup' window with two sections for configuring wireless networks. At the top, there are 'Apply' and 'Cancel' buttons. The first section, 'Wireless Network (2.4GHz b/g/n)', includes a 'Region' dropdown, checkboxes for 'Enable Wireless Isolation' (unchecked) and 'Enable SSID Broadcast' (checked), a 'Name (SSID)' field with 'MyHomeWifi', a 'Channel' dropdown with 'Auto', and a 'Mode' dropdown with 'Up to 217 Mbps'. The 'Security Options' section has radio buttons for 'None', 'WPA-PSK [TKIP]', 'WPA2-PSK [AES]' (selected), and 'WPA-PSK [TKIP] + WPA2-PSK [AES]'. Below this is a 'Passphrase' field with 'MyPassword' and a note '(8-63 characters or 64 hex digits)'. The second section, 'Wireless Network (5GHz a/n/ac)', includes checkboxes for 'Enable Wireless Isolation' (unchecked) and 'Enable SSID Broadcast' (checked), a 'Name (SSID)' field with 'MyHomeWifi\_5Ghz', a 'Channel' dropdown with '153', and a 'Mode' dropdown with 'Up to 1300 Mbps'. The 'Security Options' section has radio buttons for 'None', 'WPA2-PSK [AES]' (selected), and 'WPA-PSK [TKIP] + WPA2-PSK [AES]'. Below this is another 'Passphrase' field with 'MyPassword' and a note '(8-63 characters or 64 hex digits)'.

**FIGURE 3.8**

NetGear Wi-Fi settings page.

## NOTE

### My experiences with a new Wi-Fi router

Recently, I needed to purchase a new Wi-Fi router. My old Wi-Fi router, which was provided by my Internet service provider, hadn't been upgraded in 5 or 6 years, and the Internet service provider didn't even have an upgrade available. From a security standpoint, the router was just fine; however, because it was an older router, it didn't support the newer faster Wi-Fi speed standards. Specifically, it only supported the 802.11a, 802.11b, and 802.11g standards. The bulk of our home devices support the 802.11n and some are now supporting the new 802.11ac standard, but because the router didn't support these newer standards, we weren't able to take advantage of the faster networking speeds. When I purchased the new NetGear router, I was pleasantly surprised to find out that the new router was configured with WPA2 enabled as the default security level for the Wi-Fi connections on the router instead of having no encryption configured on the Wi-Fi connection, which was the default until just very recently.

The process to change the Wi-Fi protection varies for each Wi-Fi router out there. No matter what kind of router you have, you'll need a username and password to connect to the management webpage. Most if not all routers can be configured by going to the router's IP address from a web browser on any computer within the home network. Finding out what the IP address of the router is can be a little tricky if you don't have the documentation that came with the router handy or if the IP address of the router has been changed. There are a few different approaches that can be taken. On any Windows computer, it can be found by looking at the Wi-Fi Network Connection from within the Network Control Panel. One way to get into the Network Control Panel is to right click on the network icon next to the clock in the task bar, typically located at the bottom right corner of the screen as shown in [Figure 3.9](#).

In this case, I'm connected to a Wi-Fi network so the network icon (the one in the middle of [Figure 3.9](#)) shows the Wi-Fi signal strength. If I was plugged into the router via an Ethernet cable, then the icon would look like a small computer instead. In either case, right click on the menu and select "Open Network & Sharing Center" from the context menu that appears. This will open a window similar to the one shown in [Figure 3.10](#).

If you are using an older version of Windows such as Windows XP, then you may not see an icon similar to that shown in [Figure 3.9](#). This is because in older operating systems like Windows XP, the icon wasn't shown by default. To locate the networking icons in Windows XP, click on the Start button, then select Control Panel, and then double click on the "Network Connections" icon within the Control Panel. This will show you a window similar to that shown in [Figure 3.11](#).

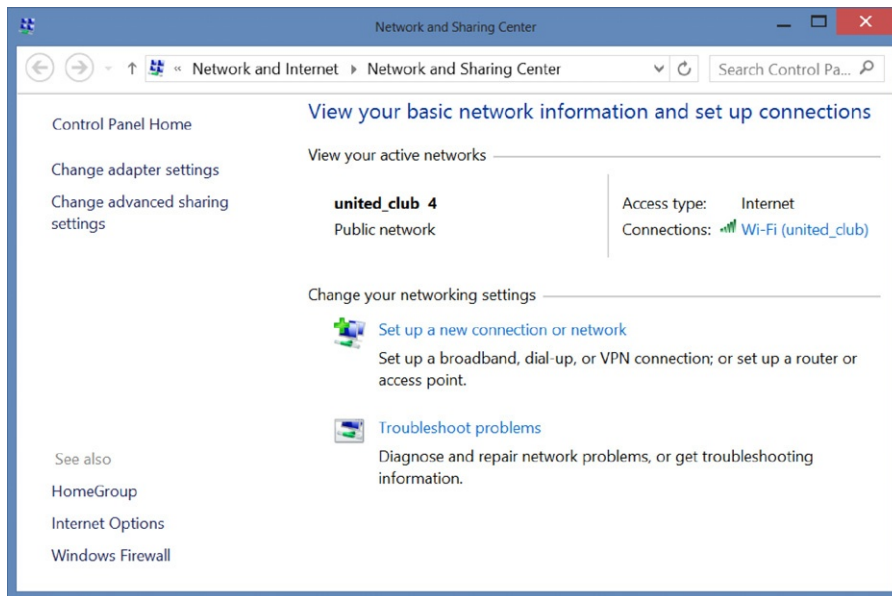
Once the Network and Sharing Center is open, click on the link to the left that says "Change adapter settings." This will open a window similar to that shown in [Figure 3.11](#).

Once the window similar to the one shown in [Figure 3.11](#) appears, you'll need to identify the Network Connection that is being used. Odds are that you'll only have one or two icons in here at the most, and if there are extra ones, they will probably be grayed out and says "Disabled" like the one on the right of [Figure 3.11](#). Find the one that is connected; it will probably have a network name of some sort under the network adapter name. In the case of the window shown in [Figure 3.11](#), this would be

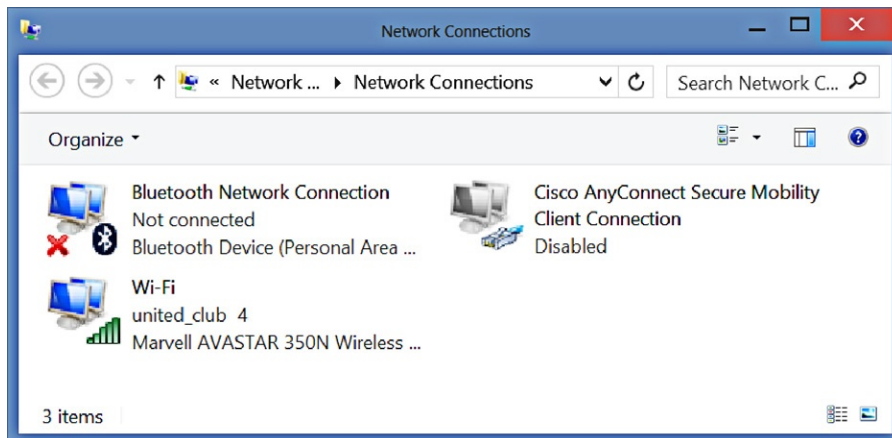


**FIGURE 3.9**

Network icon in the system tray of a Windows 8 computer.

**FIGURE 3.10**

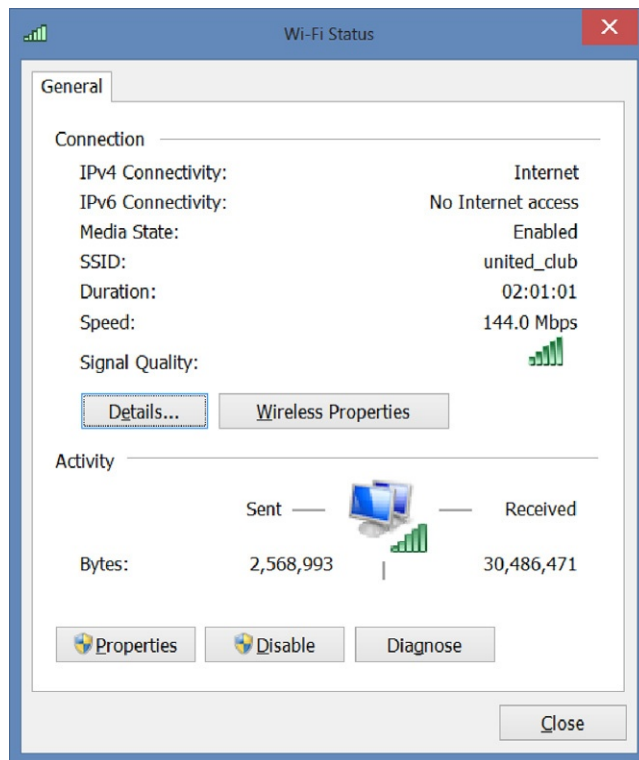
Network and Sharing Center.

**FIGURE 3.11**

Network Connections window.

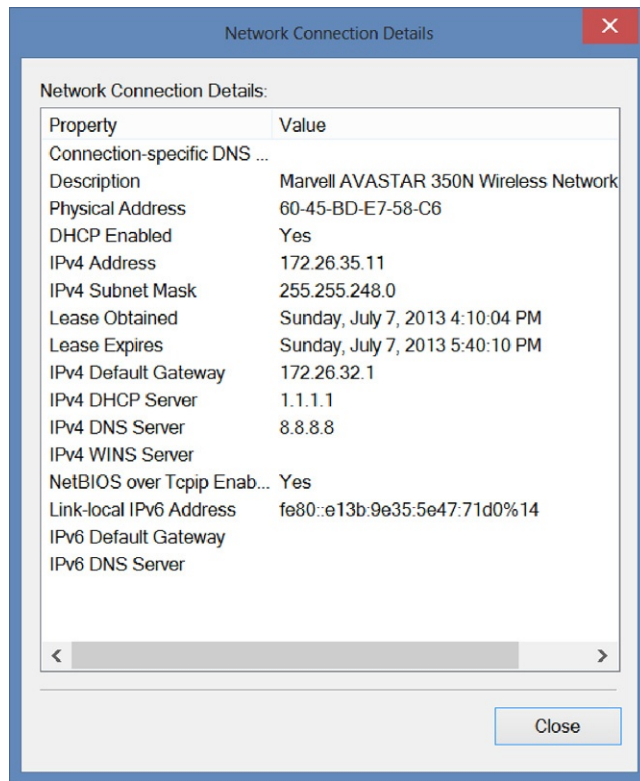
the icon labeled “Wi-Fi”; then under that, it says “united\_club 4” and then under that, it says “Marvell AVASTAR 350N Wireless . . .” This information tells me that the Wi-Fi Network Connection within Windows is called “Wi-Fi,” that I’m connected to a network called “united\_club” (the 4 tells me that it’s the fourth network called “united\_club” that I’ve connected to on this machine), and that the network card is a “Marvell AVASTAR 350N Wireless Network Adapter.” This window on your machine will say something different depending on your Network Connection name, network name, and the brand and model of the network card you are using. The important part on this window is to find the correct icon, which will probably be the only one in color. Once you have identified the correct Network Connection, double click on that Network Connection and you should see a window similar to [Figure 3.12](#).

Once the window shown in [Figure 3.12](#) is visible, the final thing to do is to click on the “Details button” in the middle of [Figure 3.12](#). This will bring up a window similar to that shown in [Figure 3.13](#).



**FIGURE 3.12**

Properties window of a specific Network Connection.

**FIGURE 3.13**

Details window of the Network Connection.

As you can see in [Figure 3.13](#), there are several IP addresses listed; the important one in this case is the “IPv4 Default Gateway,” which is 172.16.32.1. The default gateway, which your home network uses, will probably be different from this network and will probably be 192.168.0.1 or 192.168.1.1 or 192.168.1.254 or 192.168.0.254, but in reality, it could be just about anything.

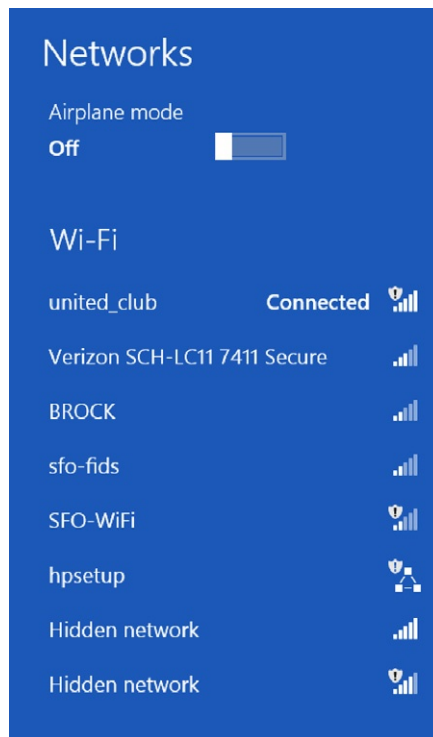
By entering this IP address, you should have access to the management webpage for the home router. Use the username and password, which were configured when the router was first configured. If you don’t have the username and password, you’ll need to contact the company that made the router to get the default username and password or to get assistance in resetting the username and password to something that you can remember. From here, follow the instructions provided by the company that made the router on how to configure it for WPA2 connections.



### *Hiding your wireless network*

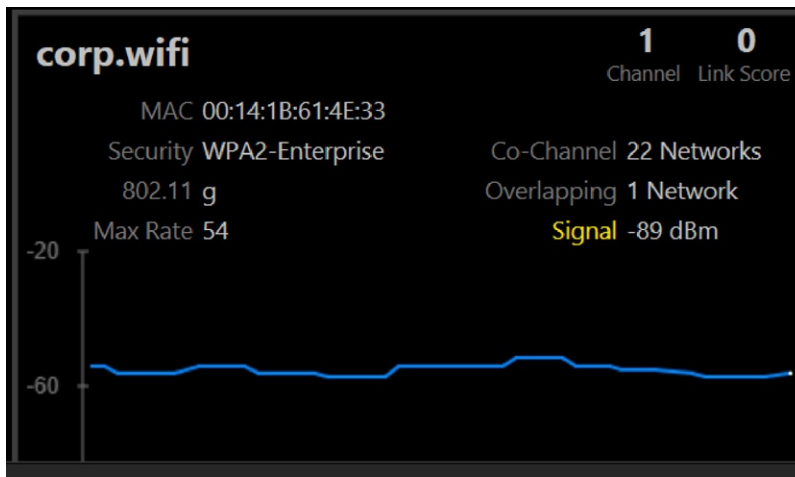
One of the features that people like to turn on in order to protect their Wi-Fi networks is the option to hide the Wi-Fi network. Normally, Wi-Fi networks broadcast their network name in order to make it easy for people to locate the network and connect to it. [Figure 3.14](#) shows the network screen from a Windows 8 computer, which I was using while at San Francisco International Airport. You can see several networks available including the “united\_club” network, which I was connected to at the time.

The theory that people use when configuring their Wi-Fi router to be hidden is that because people can’t see the network when they open the connection window, this makes the network more secure. In reality, this isn’t the case. It is in fact very easy to find “hidden” networks. There are a variety of programs that can be downloaded, which will show you the various hidden network, and a variety of information about those Wi-Fi networks. Using an application called inSSIDer, I can quickly and easily see all the hidden networks in the area. After launching inSSIDer and telling the application to scan the Wi-Fi networks, it quickly shows me several hidden Wi-Fi networks including the one shown in [Figure 3.15](#).



**FIGURE 3.14**

Wi-Fi networks available at San Francisco International Airport.

**FIGURE 3.15**

Screenshot of inSSIDer showing a hidden network.

While hiding Wi-Fi networks will keep the casual person from finding a Wi-Fi network, it won't stop someone who actually wants to find the hidden networks, and hiding the Wi-Fi network shouldn't take the place of properly securing the Wi-Fi Network Connection via WPA2.

One of the reasons that hidden Wi-Fi networks are so easy to find is that just because the Wi-Fi router or access point isn't broadcasting the network name, the machines that are connecting to the hidden network will need to broadcast the network name so that the Wi-Fi router or access point can accept the connection. So while a normal user wouldn't be able to see the hidden access points, someone with some experience in looking for hidden networks just needs to sit and wait for a computer to attempt to talk to the hidden network and capture the hidden network's network name.

If you are going to choose to hide the network to keep random neighbors from attempting to connect to it, that's a good idea in a lot of cases, especially when there are lots of people in the area with Wi-Fi access points. However, this must be teamed up with WPA2 network security to ensure that when people that you don't want finding your Wi-Fi access point do find it, they still can't get connected easily.

### ***MAC address filtering***

Most, if not all, Wi-Fi routers include a feature called MAC address filtering. MAC address filtering allows you to specify the exact computers that are going to be allowed to access the Wi-Fi network. In theory, this is a very sound idea in that only the computers with the correct MAC addresses would be able to connect to the network. The reality is that it isn't all that hard to pretend to be using a different MAC address when connecting to a Wi-Fi network.

---

**NOTE****What is a MAC address?**

A MAC address is the physical ID number that is assigned to every network card on every computer. Every network card in the world has a MAC address, and every MAC address is unique to that specific network card. If your computer has multiple network cards, such as a wired Network Connection and a Wi-Fi network card, then your computer will have two MAC addresses. To find your MAC address, follow the directions in the section of this chapter called “Securing Your Wi-Fi.” On the window shown in [Figure 3.13](#), the MAC address is labeled as the “Physical Address.” In the case of the computer that I took, the screenshot on the MAC address is 60-45-BD-E7-58-C6.

---

There is a variety of software out there, which will let someone scan for all the MAC addresses currently in use in the area (remember we are talking about wireless networking so all this information is simply being broadcast by all the machines in the area). Once an attacker has the MAC address of a computer that is allowed to connect, it is a simple job to temporarily change the MAC address of the computer that they are using so that they can get past the MAC address filter.

---

**NOTE****MAC filtering is not good for allowing access or blocking access**

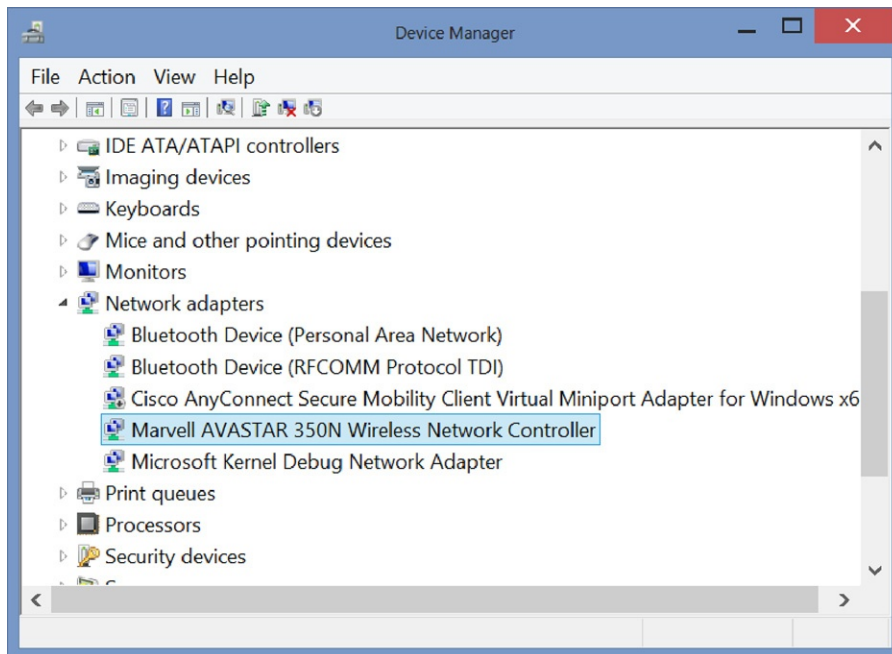
Some of you readers may be parents who have configured their home Wi-Fi to prevent the kids from using the Internet during certain hours or the night or to prevent them from using the Internet altogether. And these systems work great, until the kids figure out that they can simply change the MAC address of their computer, which lets them bypass the restrictions. This happens because these time-limiting systems all rely on using the MAC address of the computer that is being blocked from having access during specific times. By simply changing the MAC address, which is shockingly simple to change, all the restrictions simply go away as the MAC address doesn't match anymore.

---

### Changing the MAC address in Windows

Changing the MAC address of a Wi-Fi card in Windows is surprisingly simple.

The first step is to open the Control Panel. The version of Windows you are using will determine how this is done. In Windows 7 and below, click on the Start menu and then click on the Control Panel option from the Start menu. In Windows 8 or Windows 8.1, bring up the Start menu and then type “Control.” The Control Panel option will be on the list. Clicking the Control Panel option from the list will bring up the control panel. At this point, the instructions are the same. At the top right of the control panel, you'll see a drop-down menu that probably says “View By: Category.” Change this dropdown to say “View By: Small Icons.” In the new list of icons, find and open the icon labeled “System.” From here, click on the link in the upper left that says “Device Manager.” In the Device Manager window that opens, find the “Network Adapters” menu and expand it as shown in [Figure 3.16](#).

**FIGURE 3.16**

The Device Manager with the network adapters menu tree opened.

After the Device Manager opens, double click the Wi-Fi Network Card. On the new window that opens, select the Advanced tab. From there, find the MAC address option if available and simply change one character of the MAC address (only using the numbers or the letters A-F). When you click OK, the MAC address has been changed. Not all network cards allow for the MAC address to be changed, but with a little searching around, any determined teenager would be able to find the information to change their MAC address.

### Changing the MAC address in Apple OS X

Changing the MAC address on an Apple computer is slightly harder, just because it requires the use of the command prompt. To change the MAC address on your Apple OS X or newer machine, start by opening a command prompt window on the machine. From there, run the command “ifconfig” to see what the current MAC address is. If you combine the ifconfig command with the grep command, this will be easier to find.

```
ifconfig en1 | grep ether
```

Using ifconfig with the grep command.

Use of the `ifconfig` and the `greg` commands should return something that contains the MAC address of the computer. Changing the MAC address is pretty straightforward. We need to use the `sudo` command so that the `ifconfig` command that we are using is run with root (or administrative) permissions.

```
sudo ifconfig en1 ether 00:a1:a2:a3:a4:a5
```

Using `ifconfig` to change the MAC address.

Once the MAC address has been changed, it can be verified using the `ifconfig` command shown earlier.

### Letting others onto your Wi-Fi network

Friends and Wi-Fi networks are a dangerous combination. Having your friends have access to your Wi-Fi network isn't all that dangerous; it's the fact that letting your friend's computers onto your Wi-Fi network now gives your friend's computers direct access to your computer, meaning that any software installed on their computer, such as a virus, for example, would then have access to your computer and the virus may try and install itself onto your computer. Given that viruses are one very common way for personal information to be compromised on home computers, having someone else have access to your home computer network with a laptop, phone, tablet, etc., which may or may not have a virus on it, isn't the greatest of ideas.

There are a couple of options to solve this problem. The first is to create a pocket network that is a different Wi-Fi network from the Wi-Fi network that you put your computers onto. This second network would still give them Internet access, but it wouldn't let them connect to your computers or have any software that was installed on their computer such as viruses have access to attempt to install themselves on your computer.

Another option that is available in some home routers, which have the ability to create a guest network, for just this specific reason. The guest network would be a totally separate network name; I might call my home Wi-Fi network "Cherry Home" while the guest network would be called "Cherry Guests" as shown in [Figure 3.17](#). These guest networks are a little different from the normal Wi-Fi networks that we connect to when it's our home network. The Wi-Fi router knows that anyone on the Guest network should be isolated from the normal network. This keeps anything that is installed on our friend's computer from having access to our home computer network. We don't want the Guest network to be wide open to the outside world. We want this network to be secured with WPA2 just like our network, just using a different password, one that we are OK with giving to our guests. The reason that we don't just want this guest network open to the entire world is because if someone was going to drive past our home and see the open network, we wouldn't want them doing something on our home Internet connection that might not be legal as that activity might be traced back to our home (don't forget the sidebar earlier in this chapter titled "You may be legally responsible for what others do on your computer network").

**Guest Network Settings**

Apply Cancel

---

**Wireless Network (2.4GHz b/g/n) - Profile**

☒ Enable Guest Network

☒ Enable Wireless Isolation

☒ Enable SSID Broadcast

☐ Allow guest to access My Local Network

Guest Wireless Network Name (SSID):

---

**Security Options - Profile**

☐ None

☐ WPA-PSK [TKIP]

☒ WPA2-PSK [AES]

☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

---

**Security Options (WPA2-PSK)**

Passphrase:  (8-63 characters or 64 hex digits)

---

**Wireless Network (5GHz a/n/ac) - Profile**

☒ Enable Guest Network

☒ Enable Wireless Isolation

☒ Enable SSID Broadcast

☐ Allow guest to access My Local Network

Guest Wireless Network Name (SSID):

---

**Security Options - Profile**

☐ None

☒ WPA2-PSK [AES]

☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

---

**Security Options (WPA2-PSK)**

Passphrase:  (8-63 characters or 64 hex digits)

**FIGURE 3.17**

Guest Network Settings from a NetGear router.

## OTHER DEVICES ON THE NETWORK

The home network has a large number of devices connected to it, usually over Wi-Fi. These can include devices that you would expect to find on the network such as your desktop and laptop computer, which are hopefully all running with firewalls and the accounts have passwords on them. However, there could be a lot of other devices connected to your home Wi-Fi network as well. This could include your cable box, DVD player, TV, burglar alarm, home automation devices (which could control things like light switches, power outlets, garage door openers, and holiday lights), stereo systems, door locks, baby monitors, security cameras, refrigerators, and probably many other devices.

---

**NOTE****You'd be amazed at all the devices on your network**

The number of network-connected devices found on the typical home network is staggeringly high. Just looking around my own home, I can count at least 17 devices on my home network, before I count a single laptop computer, desktop computer, or tablet such as an Apple iPad, HP TouchPad, or Microsoft Surface. These include three televisions, three cable boxes, three Wi-Fi-enabled remote controls, three X-Box 360s, three Blu-ray DVD players, burglar alarm, and the printer.

---

These extra devices all can pose a risk of a privacy breach within the home. Where someone is able to get into the home network and be able to access these devices, it would become potentially very easy for someone to begin to learn much more about you and your life than you probably want exposed. For example, if someone was able to gain access to your alarm system through your home Network Connection, they could very easily figure out when you are away and when you aren't making it very easy to figure out when to break into your house. They might even be able to disable your alarm remotely or just power it off so that it can't send a signal to the alarm company when the break-in is going to happen.

The devices that just sit on your home network don't pose the most risk; the devices that publish the information so that you can view it from anywhere are the most dangerous. The perfect example for this are the new baby monitors that can stream a video and audio feed to the Internet so that parents can keep an eye on the baby from another room, the neighbors' house, or even their office miles away. Some of these include the ability to use speakers on the baby monitor so that you can talk to the baby if they wake up and just need to hear your voice in order to calm down and go back to sleep. Many products like this are designed for convenience and not with any sort of security in mind, often not requiring any password or that the default password be changed. With these devices publishing the data to the Internet where basically anyone can view the feeds is a major data privacy risk. By using a variety of easy-to-find tools, or sometimes even a quick search on Google, dozens or hundreds of openly accessible video devices can be viewed and sometimes controlled via the public Internet without the device owner being aware that someone is viewing their device.

All this sounds pretty scary and farfetched. We've all seen these sorts of things in TV shows like CSI, NCSI, and Law & Order and assumed that this sort of thing is totally impossible to actually happen. In reality, this is actually very possible and in fact has actually happened to a family with a baby monitor in Houston, Texas. In this case, the baby monitor has speakers, a microphone, and a video feed and is remote controllable. Someone was able to break into the remote feed of the baby monitor, likely through a poorly configured password or lack of password, and see into the baby's room and talk to the baby, even going so far as to try and wake the child up.

---

**NOTE****Sadly this isn't fiction**

Everything that I've just talked about we've all seen on television over and over on just about every cop crime drama out there. Even Dr. Who has seen people talking through the baby monitors once or twice (that's totally different and is for a totally different kind of book), but the sort of situation that I have just talked about with people looking in on other people's baby monitors and taking them over and talking to the kid can and has actually happened. I won't go into the gritty details, instead leaving that for you to read online at <http://basicsofdigitalprivacy.com/go/baby>, but this is an actual home privacy threat that is something that does in fact need to be dealt with both by the people that buy these devices and by the people that make these sorts of devices.

---

The easiest way to make sure that devices you purchase will support proper log-ins is to only purchase new devices (used devices from family, friends, and yard sales should be avoided whenever possible). When purchasing the new devices, read the box and it should say something about authentication and that it supports SSL (Secure Socket Layer), which is the same data encryption that you use when doing online shopping on websites like Amazon and eBay.

**SUMMARY**

A properly configured home network is very important when it comes to protecting yourself. While the chances of someone driving by your home network and attempting to gain access to it aren't that high, it is very possible that a friend or neighbor could have a virus on their computer that they don't even know about. If that friend or neighbor were to put their computer on your home network, any virus that they had on their computer could attempt to access your computer. Once installed on your computer, that virus would do whatever it was programmed to do, which oftentimes these days involves looking for your personal information and sending it to some sort of criminal.



# Securing Your Home Computer

---

## INFORMATION IN THIS CHAPTER

---

- Data encryption for the home user
- Why you should be encrypting data
  - Native Windows data encryption
  - Native Apple data encryption
  - Other companies data encryption
- What do those website security logos mean?
- When Tech Support calls you
- Internet games and downloads

While we hope that no one will steal our home computer and that we will never lose our laptop, the reality is that at some point, we will end up losing a computer somehow. A study done by Intel, available at <http://basicsofdigitalprivacy.com/go/oneinten>, found that 10% of laptops purchased will be lost or stolen within the first year of ownership. Of those laptops stolen, only 3% of those laptops will ever be recovered and returned to their owners. That means that 97% of the laptops that are stolen and the data that they contain remain with the thief or the person that the thief sells the laptop to.

Where laptops are stolen is an interesting set of numbers to review. It is assumed that most laptops are lost or stolen at airports. The reason behind this though is that airports are busy places and the last thing that most people want to worry about at the airport is the location of their laptop at they run from flight to flight. While there are many laptops left at airports every year, the reality is that not that many laptops are actually stolen at airports, due mainly to the fact that there is a high degree of security at the airport compared to everywhere else that we travel. Since not just anyone can walk into an airport and get past the security checkpoint, given that you have to have a valid boarding pass to get past the airport security line, the odds of someone within the airport being there just to steal someone's laptop is pretty slim. According to the Intel-funded study, available at <http://basicsofdigitalprivacy.com/go/oneinten>, the places that we consider the safest would be where the most laptops are actually stolen from, with homes and hotel rooms accounting for over 40% of laptop thefts. Additionally, another 33% of laptops, which are lost, are lost while in transit (taxi, trains, subways, airports, etc.). Another 12% of laptops are lost within our

workplace, in other words, taken by a coworker or other person who has access to our place of business, with the remaining laptops being taken at an unknown location or a location that couldn't be identified by the study participants.

---

## NOTE

### Why the focus on laptops?

This introduction focuses on laptop computers because they are much more likely to be stolen than desktop computers. The primary reason that they are more likely to be stolen than desktop computers is that they are portable so they leave the house. Even within the home, during a break-in, a thief will take a laptop over a desktop as the laptop is much lighter and easier to carry and easier to take into a shop to get into the operating system so that they can use the laptop or sell the laptop as their own.

---

---

## DATA ENCRYPTION FOR THE HOME USER

The best way to prevent your personal information from being exposed to someone who has taken or found your computer is to encrypt the information within the computer. This will protect the information in such a way that if someone who doesn't have the password or key for the encryption system attempts to gain access to the information, they won't be able to. Within the information technology industry, data encryption is considered to be the gold standard when it comes to protecting information from access by unauthorized people. This trust in data encryption comes from the fact that the strongest levels of data encryption, which are commercially available today, are considered to be virtually unbreakable.

---

## QUESTION

### What is "Virtually Unbreakable"?

Unfortunately, no data encryption is totally unbreakable. Any level of data encryption, no matter how complex and how well designed, can be broken eventually. The protection provided by data encryptions comes from the amount of time that it takes to break the encryption and gain access to the information that has been encrypted.

When it comes to companies, they will attempt to mitigate the risk of encryption being broken by changing the keys that protect the data on occasion so that if someone breaks into the system today and gets a copy of the data, then they get a copy of the data 6 months from now and they would need to break both encryption systems independently, making it harder to get access to the newer data. For the home user, this typically isn't needed as the data will only be taken once, when the actual computer is stolen.

As mentioned, data protection through data encryption is determined by the amount of time that it will take to break the data encryption. The first data encryption algorithm, which was widely used, was called Data Encryption Standard (DES) back in 1975 and was approved for use by US federal agencies by the US government in 1977. At that time, many people were critical of the usefulness of the DES algorithm because of the relatively short key, which is used to encrypt the data, which were 56 bits or 7 characters. Despite this short key length, the DES algorithm was still safe to use until the mid-1990s at which time it became possible to build computers powerful enough to figure out the key in a short enough time frame that breaking the key would be considered useful. In 1998, the Electronic Frontier Foundation

(EFF) built a computer for \$250,000, which was able to figure out the key for some data that were encrypted by DES in just 56 hours. The next year, in 1999, another system was assembled, which was able to perform the same test against a similar piece of data in just 22 hours. Today, DES isn't used to encrypt any information, which must remain secret for very long as even a modest home computer has the CPU power to figure out the key for data encrypted by DES within a very short period of time.

For modern data encryption, an encryption algorithm called Advanced Encryption Standard (AES) is used. AES supports several different key lengths depending on how strong the encryption should be. These key lengths are 128 bits (16 characters), 192 bits (24 characters), and 256 bits (32 characters). In the corporate world, decisions need to be made as to what key length should be used. Different key lengths are used when cost-benefit analysis is performed between the CPU processing power required to use the longer key length and the risk that the data are left open to by having the data encrypted by the lower levels of encryption. This is because the longer the encryption key, the more CPU processing power is required to encrypt and decrypt the data. In the consumer world of home computers typically, we use the strongest layer of encryption as only a single user will be accessing the data on the computer at any one time so the cost of accessing the data is minimal when using the strongest levels of encryption.

Going into the more advanced differences between the different key lengths of AES data encryption is beyond the scope of this book. Some of this information has been documented within the latest edition of *Securing SQL Server* written by Denny Cherry and published by Syngress.

---

As home users, we need to know how to set up and use the data encryption options within the devices that we use, as these devices can be easily lost or stolen, so that if our device falls into the hands of someone who shouldn't have them, our data can't be easily accessed and used by them to steal our identity, blackmail us, or release information, which we wouldn't want to be released to the public.

Different operating systems such as Microsoft Windows and the Apple operating system have different processes for setting up data encryption on the disks, and different versions of these operating systems have different features and configuration options. Understanding how data encryption can protect your data from being taken, and what sort of threats data encryption protects you against is very important when configuring data encryption.

## Native Windows data encryption

When using a computer running the Microsoft Windows operating system, which is running Windows Vista or newer versions (including Windows 7 and Windows 8), there is a feature called BitLocker, which will encrypt the data on the hard drive. When using Microsoft's BitLocker, there are a few data encryption options available to you and a couple of different options that you need to be aware of. Microsoft's Windows Vista and Windows 7 support the use of BitLocker for the entire disk only. This means that the entire disk needs to be encrypted, which can take quite awhile to configure. Starting with Microsoft's Windows 8, the BitLocker application supports encrypting the contents of either the entire hard drive or just a folder within the hard drive.

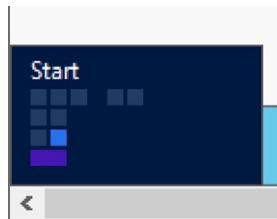
### ***Encrypting a disk in Windows***

Turning on data encryption for an entire disk is very easy to do. The first step is to open the control panel. On Windows Vista and Windows 7, this is done by clicking on the Start menu button on the task bar, typically found at the bottom left of the screen, and then clicking on “Control Panel.” On Windows 8, the Control Panel can be opened by bringing up the Start menu. This is done by putting the mouse in the lower left corner until the Start menu button appears as shown in [Figure 4.1](#). On Windows 8.1, click the Start button, which is typically found in the lower left-hand corner of the screen, and then follow the rest of the instructions below of Windows 8.

Once the Start button shown in [Figure 4.1](#) appears and the button is clicked, the Start menu appears. Once the Start menu appears, type the word “control” and the search menu will appear along with the search results as shown in [Figure 4.2](#). Clicking on the “Control Panel” button will open the “Control Panel.”

No matter which version of the operating system being used, at this point, the Control Panel should be shown on the screen, similar to that shown in [Figure 4.3](#), which is from Windows 8, but other versions of the Microsoft Windows operating system will look very similar.

Within the Control Panel, click on the “System and Security” link at the upper left of the Control Panel. This will open the System and Security menu of the Control Panel, which shows a variety of options similar to the options shown in [Figure 4.4](#).



**FIGURE 4.1**

Windows 8 Start button.

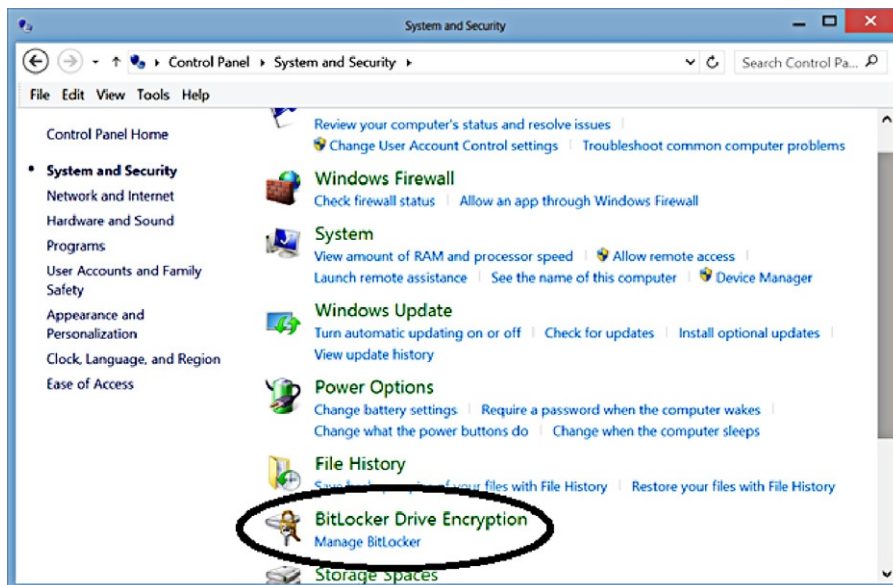


**FIGURE 4.2**

The Windows 8 Start menu after searching for the word “control.”

**FIGURE 4.3**

The Windows Control Panel.

**FIGURE 4.4**

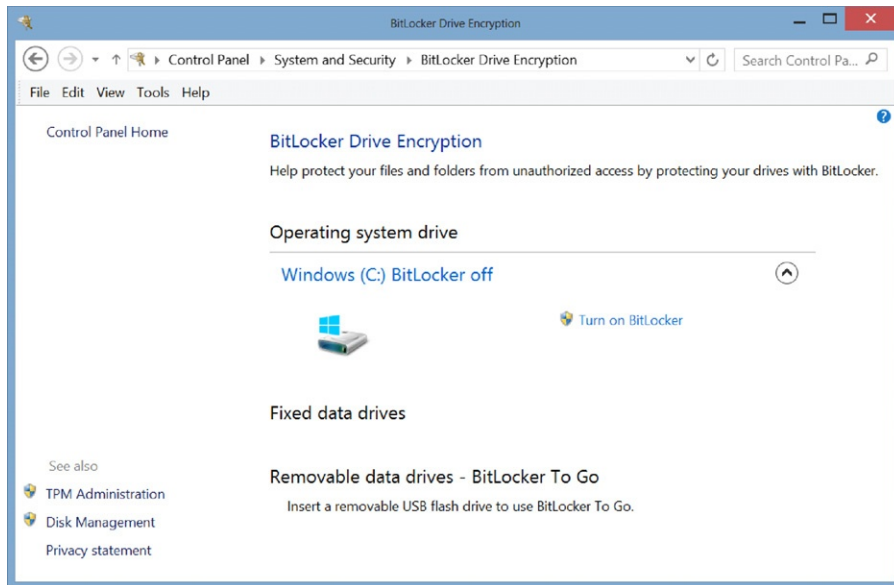
The System and Security menu of the Control Panel.

From within the System and Security submenu of the Control Panel, you'll see the BitLocker Drive Encryption menu option circled in [Figure 4.4](#). Clicking the Manage BitLocker menu link from within the System and security menu of the Control Panel will launch the BitLocker Drive Encryption menu shown in [Figure 4.5](#). From this window, data encryption can be configured for each drive on the system. Each disk can have BitLocker enabled separately from the other drives on the system. This allows you to configure BitLocker on only the drive, which contains your sensitive data, without needing to enable BitLocker on the disks that contain less sensitive data.

As an example, if your personal data was stored within the My Documents folder on the C: drive and your MP3 collection was installed on a different drive such as the D: drive, you would want to encrypt the data on the C: drive but not the data on the D: drive.

To enable BitLocker on the drive, simply click the "Turn on BitLocker," which can be found on the right-hand side of the window shown in [Figure 4.5](#) in the middle of the window.

When you turn BitLocker on for one of the drives for the first time, you will be prompted to specify how the recovery key should be saved. The recovery key is used to allow you to access your files in the event that BitLocker has data decryption problems. It also allows you to take the hard drive from this computer and insert it into another Windows computer running the same version of Windows or newer and still



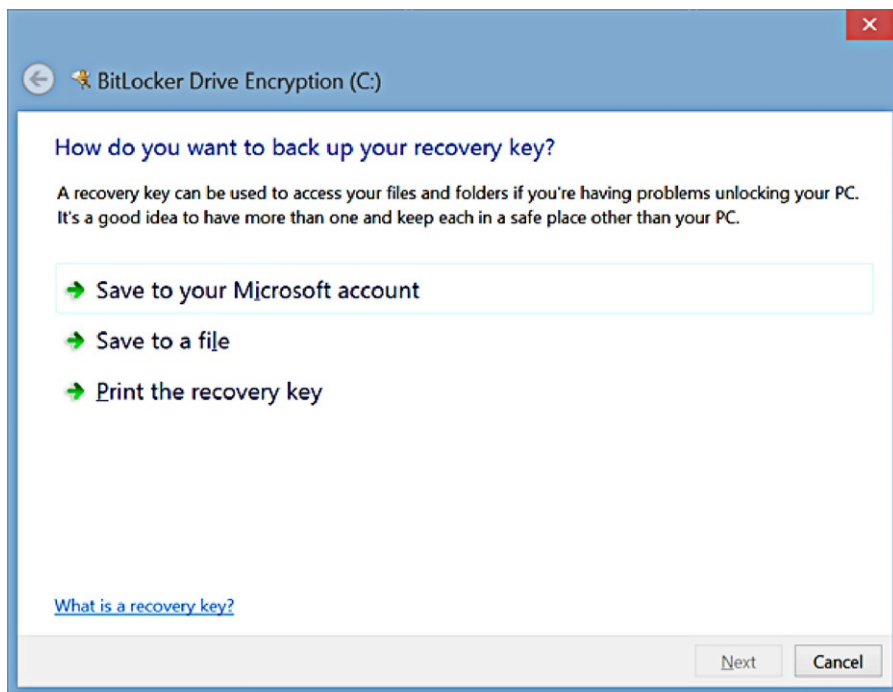
**FIGURE 4.5**

The BitLocker Drive Encryption feature within Windows.

be able to access the files on the hard drive. The screen to save the recovery key will look similar to that shown in [Figure 4.6](#). From this screen, shown in [Figure 4.6](#) on a Windows 8 computer, allows you to save the key to your Microsoft account, to a file on your local computer or to print a physical copy of the key on your printer.

Saving the password to your Microsoft account requires that you are using a Windows 8 or newer computer and that you log in to the computer using your Microsoft account (formerly called a Windows Live account). Using this option will upload the key to the Microsoft servers where it will be securely stored. Doing this is only a good idea if your Microsoft account is secured using a strong password (password policies are discussed in [Chapter 2](#)). If your Microsoft account is not secured using a strong password and your Microsoft account were to become compromised, then the person who accesses your Microsoft account could gain access to your recovery password.

Saving the recovery password to a file is typically a good idea, provided that the file is then removed from the computer and stored on a CD, DVD, or USB drive, which is then stored in some sort of secure location such as a wall or gun safe or a safe deposit box at your local bank. The same applies if you choose to print the



**FIGURE 4.6**

The recovery key window of the BitLocker wizard.

recovery key to your printer in order to store a hard copy of the key. You wouldn't want to store either the file with the key or the printed copy of the key with or near the computer that the key protects because if someone steals the computer or the computer is lost in some other way, you wouldn't want the person who has the computer and isn't supposed to have the computer to have the key to access the data either. When saving the recovery key to a local file, the file must be created on a disk, which isn't an encrypted disk. If you only have a C: drive like the computer that was used to take the screenshot in [Figure 4.6](#), you will need to have a USB drive to connect to the computer that you can save the key to in order to back up the key.

Without saving the backup of the BitLocker key, you will not be able to continue through the wizard. The next screen of the wizard will be asking you how much of the disk to encrypt. The options are to encrypt only the disk space that has been used or to encrypt all the disk space. The difference between the two is that the latter option will encrypt what is called the white space or the space on the disk that doesn't have any data written to it yet. The former of the two options will be faster but will leave any files that you have deleted but that still exist on the disk unencrypted. The latter option will encrypt everything even the files that have been deleted.

The next screen asks you if you are ready to encrypt the drive and if you want to run the systems check. The system check, which BitLocker runs, will ensure that BitLocker is able to read the recovery keys and the encryption keys, and then, it will begin the process of encrypting the entire hard drive of the computer. At this point, after the "Start Encryption" button, which can be seen in [Figure 4.7](#), is clicked, the computer is rebooted automatically and the BitLocker system will encrypt the hard drive after the reboot is completed.

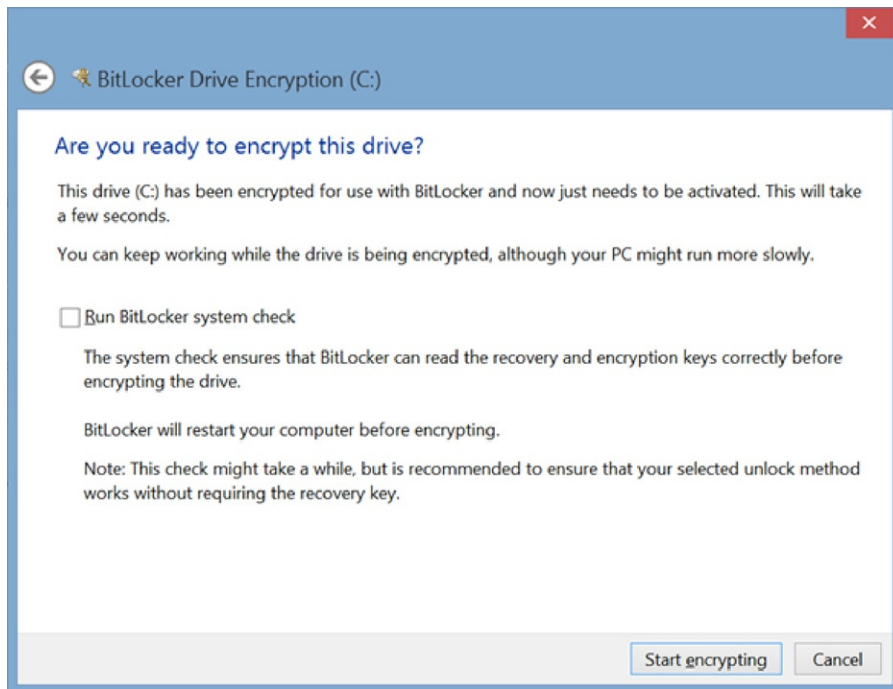
### ***Encrypting a disk in Mac OSX***

Much like the Windows operating system, the Apple OSX operating system also includes a way to encrypt the entire disk. While the Windows operating system has the BitLocker system, the Apple OSX operating system has a software package called FileVault. As Apple talks about in their Knowledge Base article number ht4790, which you can review at <http://basicsofdigitalprivacy.com/go/ht4790>, you need to be running Apple OS X Lion or Mountain Lion and you'll need to have "Recovery HD" installed on your startup drive.

FileVault is enabled and configured from within the System Preferences. Within System Preferences, open "Security & Privacy" and then click the FileVault tab as shown in [Figure 4.8](#). From here, you can set the master password, which allows you to unlock any account on the computer even when it has been encrypted. You can also turn FileVault on by clicking the "Turn On FileVault" button.

After clicking the "Turn On FileVault" button, all the users of the computer will need to enter their password if you want them to be able to turn on the computer. If the users don't enter their password, they won't be able to turn on the computer or wake up the computer when it is sleeping or hibernating.





**FIGURE 4.7**

Final screen of the BitLocker wizard.



**FIGURE 4.8**

FileVault tab within the Security & Privacy section of System Preferences.

Next, you will be shown your recovery key, which will be different for each computer. Be sure to write down this password and store it in a safe place as this password will be needed if you lose access to your data. The copy of the key that you keep should not be stored on the computer that you are encrypting as if you lose your password, you won't be able to access the key, so you will have lost everything on the computer. You will at this point be given the option to store the recovery key on Apple's servers. This protects you from losing the encryption key. Apple will secure the encryption key with a series of questions and answers based on personal information about you. When putting these answers in, make sure that you remember exactly how you put them in because if the answers are even slightly wrong, Apple's applications won't be able to decrypt the key and allow you to use it.

At this point, the computer will reboot pretty quickly. When it does, log in to the computer like normal. This will allow the FileVault application to continue encrypting the hard drive. Normally, this initial encryption process takes a few hours to complete.

Additional information about changing your key and decrypting the drive can be found in Apple's Knowledge Base article ht4790, which you can review at <http://basicsofdigitalprivacy.com/go/ht4790>.

---

## WHAT DO THOSE WEBSITE SECURITY LOGOS MEAN?

Lots of websites out there have security logos on them. They are there to make you feel better about purchasing products from them or to make you feel better about uploading personal information to them. There are a variety of websites that provide these security logos, and they all mean basically the same thing—nothing. That's right; these logos that we want to see to ensure that the websites are providing a secure environment for doing business with the company that has the logo doesn't mean anything at all.

These logos usually mean that the website does meet some very basic security requirements when it comes to browsing the secure website, but they don't actually mean all that much security has been put in place. Just because the website has these logos doesn't mean that the data is stored in an encrypted format, or that the company is doing any auditing of what data the employees access in the system, or that there aren't any security patches that haven't been installed on the web servers or the database servers.

---

### NOTE

#### **Don't trust everything you read on the Internet**

The sad reality about these logos is that they really cannot be trusted. There is nothing stopping someone who runs a website from simply downloading these logos from the Internet and uploading them to their website and posting them for all to see. This would be the same way

that the Norton logo was placed into this book in fact. There was no review of this book before I put the Norton logo shown in Figure 4.9 into this book, but the logo is sitting right there. I could easily put that logo on my websites and there wouldn't be anything that Norton could do to stop me.



**FIGURE 4.9**

The logo from Norton, which shows that a website is “secure.”

The logos, which I’m talking about, are the ones similar to the ones shown in Figure 4.9, which are available from a variety of companies such as Norton, VeriSign, Trustwave, and McAfee, among others.

The first problem with these sorts of logos is that they are pretty simple to simply copy and paste into your website. The perfect example is this book; this book obviously hasn’t been vetted by VeriSign or Norton as being properly secured, but there is their logo right there as Figure 4.9. I could easily place the graphic, which is this logo, and upload it to my website, and suddenly, the website looks like it is secure but it doesn’t actually have to be.

As pointed out by Troy Hunt in his blog post, which you can read at <http://basicsofdigitalprivacy.com/go/troypost>, websites aren’t secure just because they have logos on them. My favorite piece from Troy’s post is shown in Figure 4.10 where the website “Top Cashback” talks about how secure their website is.

Just because they have these logos doesn’t prove that the website is doing everything possible to secure their information. The reason that this is such a problem is because of the trust that the general public has with these logos. According to the Norton website (as of the writing of this book in the summer of 2013), which is owned by Symantec,

1. 77% of consumers recognize the Norton Secured Seal,
2. 65% of consumers agree that a website displaying the Norton Secured Seal is safe to browse and won’t give them a virus,
3. 55% of consumers agree that a website displaying the Norton Secured Seal means that the website protects their online privacy.

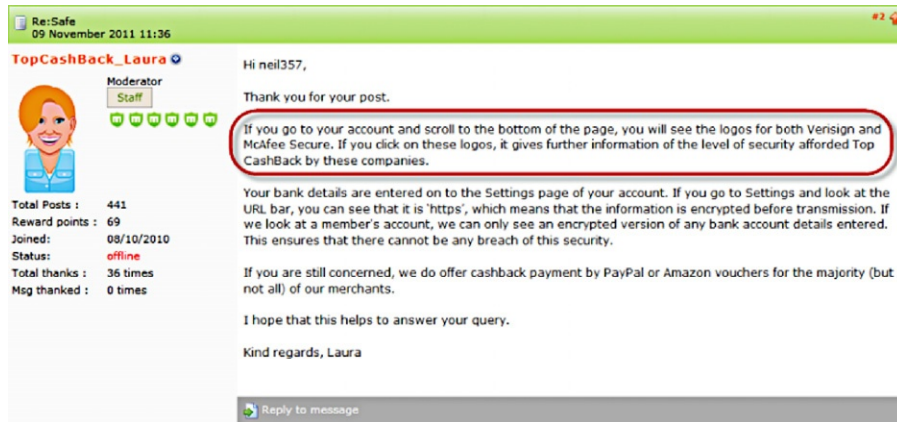


FIGURE 4.10

A website telling you that their site is secure because it has logos on it.

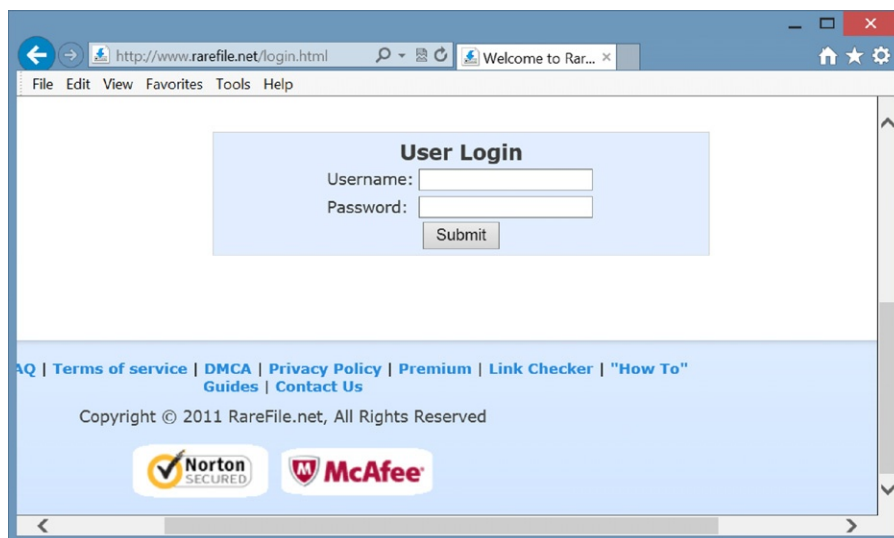
I've got issues with every one of these sales points that are listed here and broken down one by one:

#1 People have been taught and trained to think that these logos are important and that it's all they need to look for.

#2 There is no guarantee that having the Norton Secured Seal shown in Figure 4.9 guarantees that the website won't give you a virus. Over the years, there have been several occasions where the banner ad services that most of the websites use have served out viruses with the ads either because the banner ad website got a virus or because the person who created the virus was able to sneak an ad into the system, which has a virus as a part of the ad. No matter how the virus gets into the ad network, it's the website that'll be serving the ad with the virus in it to the end user.

#3 These logos don't mean anything about protecting their online privacy. It doesn't mean that the website is securing your data on their servers. It doesn't mean that the company is protecting its end users from Internet attacks like cross site scripting errors or that all the communications between the web browser and the server are being done through the most secure possible levels of communication or that the website requires that you use a fully secure password. In fact, having these logos don't actually mean that the website is even using any encryption between the web browser and the web server as shown in Figure 4.11.

You'll see that the site [rarefile.net](http://rarefile.net), as of the summer of 2013, has both the Norton and McAfee logos, but the URL in the URL bar at the top starts with `http://` instead of `https://`, which tells us that the data aren't being encrypted between the web browser and the web server.

**FIGURE 4.11**

[rarefile.net](http://rarefile.net) with security logos and no data encryption.

What all this means is that when you see these logos, you need to still be just as careful when using these websites as these logos are basically meaningless when it comes to proving that a website is secure and safe to use.

---

## WHEN TECH SUPPORT CALLS YOU

There are variety of companies and people out there that want your money. Some of them will buy your identity online for a few dollars, some of them will dig through a company's trash to find your personal details, and some of them will simply call you and ask you for your money, and a large number of people will simply hand it over.

A popular scam at the time of writing this book in the summer of 2013 is for someone to call you up and tell you that they are from large companies' technical support department and that they are calling to tell you that you have a virus and that they will help you get the virus off of your computer. They'll start off helping you for free, usually by having you install some software on your computer. Then, they will tell you that you need to pay them to complete the support. At this point, the software, which they have installed on your computer, probably includes something called a key logger. A key logger is designed to keep track of every keystroke that you enter. The more complex of them will watch for specific strings such as typing in 16 numbers in a row followed by four more numbers and then three more numbers. You'll probably recognize this pattern as being a credit card number (16 digits, 15 for

American Express), the expiration date (4 digits), and the security code on the back of the card (3 digits). They will also watch for things like common tax numbers such as the 9 digits numbers we use here in the United States as Social Security or Tax ID Numbers. When you give them your credit card number, they'll charge a small amount of money to the card usually a couple of hundred dollars telling you that it is the fee to remove the virus. Sometimes, they will tell you that the fee is to give you a proper license of Windows for your computer because your license was stolen (also called pirated).

No matter how much these people charge you, they aren't selling anything that is legitimate. The virus removal wasn't real, and in fact, they probably installed a virus on your computer as a part of the process. If they sold you a Windows license or a Microsoft license (or really a license of any kind), that isn't real either. They have no way of knowing if your license for Windows is real or not, and they have no ability to sell you a Windows license. The people who are running this scam are very good at it, and this scam is very inexpensive for them to run. With a few Google Voice accounts or using some other forms of free Voice over IP (VoIP) technology, they can call anyone from anywhere and look like they are calling from anywhere that they want to be calling from. If you are in the United States, they will appear to be calling you from the United States. If you are in England, they will call you from an English phone number, the same goes for France, Germany, Australia, etc.

Dealing with these scammers is very simple. As soon as they tell you that they are from Microsoft's Tech Support and you didn't call Microsoft's Tech Support, just hang up the phone. Odds are they will just move on to someone else. If you made the mistake of giving them your credit card number, it is OK; things can be done to fix this. First, call your credit card company and explain what happened and tell them how much they said that they charged you and that you got scammed. The credit card company can simply reverse the charge. This shouldn't cost you anything as they will simply take the money back from the account that charged your credit card (this may vary depending on your credit card company and your card member agreement as the country or state that you live in). You'll also want to have the credit card company cancel that card number and issue you a new one. The worst part of all this is that you won't have access to the credit card for a few days, while you wait for the new card to be e-mailed to you.

A large number of people that are taken by this scam don't call the credit card company because they don't want to admit that they got scammed. **DO NOT** be one of these people. These scammers have been running this scam for a long time, and they are very good at it and very convincing with their sales pitch. By not reporting it, you are putting money directly into their pockets and encouraging them to continue with the scam against other people. If required by your credit card company, contact the police and report the scammer and get a police report. In reality, this probably won't do anything to the people running the scam as odds are they aren't in your country or even in a country that your law enforcement could get to them in. The police won't laugh at you and they won't embarrass you when you report it. They

understand that there are lots of people running these scams and that lots of people get caught up in these scams. Get the police report, get the charges refunded, and get a new card number. No harm, no foul.

---

## NOTE

### Some people are getting even

These scammers who pretend to be from Microsoft's Tech Support call as many people as possible. However, sometimes, they get someone who works in the IT field, and sometimes, they get someone who works in Security within the IT field. A perfect example of this is my friend Troy Hunt ([www.troyhunt.com](http://www.troyhunt.com)) who does a lot of work in IT Security. In one instance, the scammers called Troy and Troy recorded the call, during which he attempted to scam the scammer back by wasting as much of the scammers time as possible. Troy wrote a blog post about the call and posted the video that you can watch at <http://basicsofdigitalprivacy.com/go/scammervideo>.

This sort of stunt shouldn't be tried by someone who isn't experienced in dealing with scammers as Troy is. He lets the scammer connect to a virtual machine, which is a computer that is configured specifically so that he can have a little fun with the scammer without putting his actual computer at risk.

---

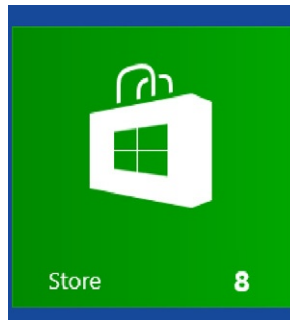
---

## INTERNET GAMES AND DOWNLOADS

Things, which are downloaded or run from the Internet, are one of the many ways that a virus can get on to your computer. There are currently over 100,000 different computer viruses in existence, although most of those aren't actually found in the wild on the Internet. For the most part, there are about 300 or so viruses that you really need to worry about at any one time; however, each of those base viruses could have dozens of variants, which are all slightly different from each other.

For a computer virus to attack your computer, it needs to have access to your computer. The easiest way for it to get access to your computer is for you to download it either via an application such as a computer game; a flash game, which you play on a website; or an ad, which you view on a webpage. When you install an application, you assume that the application doesn't have any malicious code within it. An application can be written to do just about anything with your computer that the developer wants to do, and you don't have to be aware of what the application is doing. As an example, just because you are playing a card game on the screen doesn't mean that the application isn't also going through all your files on your computer looking for credit card numbers and e-mailing any that it finds to the application's creator.

When it comes to downloading games from the Internet or playing games online, only use trusted sources to download the games and applications from. Some places, which are typically safe to download games from, include websites such as [msn.com](http://msn.com), [download.com](http://download.com), [FaceBook.com](http://FaceBook.com), and [games.yahoo.com](http://games.yahoo.com) to name just a few. Random websites, which are publishing just a couple of games for download and aren't major publishers, should not be taken at their word that they are safe to download from.

**FIGURE 4.12**

The Windows 8 Store icon from the Windows 8 Start Menu.

### Application stores

With the introduction of Windows 8, you now have the Windows Store, which is available through the Store button on the Windows 8 Start menu as shown in [Figure 4.12](#).

The Windows Store is a great place to download applications and games as those games and applications have been reviewed by Microsoft. This review process ensures that the games follow Microsoft's terms of service and that the application isn't being published by a computer that Microsoft knows as a scammer. While Microsoft doesn't inspect every line of code within the applications, they do check to make sure that the application isn't doing things that the developer says that it shouldn't be doing by using some automated testing processes during their review process.

This goes right along with the Apple Store on the Apple operating system. Apple does an excellent job making sure that the applications, which are hosted within the Apple Store, are free from viruses and malware and are safe to install on your computer.

In either case, Windows or Apple, this doesn't mean that you shouldn't have an antivirus installed on your computer. There are a wide variety of antiviruses out there and many of them do a very good job. Some are better than others and some cost more than others.

### Windows antivirus software

For the Windows operating system, Microsoft has an antivirus application called Microsoft Security Essentials, which they have released for free on their website at [www.microsoft.com/security\\_essentials](http://www.microsoft.com/security_essentials). There are also several other very good products out there such as Sophos ([www.sophos.com](http://www.sophos.com)), McAfee ([www.mcafee.com](http://www.mcafee.com)), Norton Security Essentials ([www.norton.com](http://www.norton.com)), and Trend Micro ([www.trendmicro.com](http://www.trendmicro.com)). Some of these take less memory than others, while some cost less than others.



---

**NOTE****Antivirus application suggestions are a religious debate**

While the use of antivirus applications is pretty much accepted by everyone, which antivirus application to use is a hot topic. Everyone in the IT field and many home users have their favorites that they recommend to anyone around. Personally, I'm a big fan of the Microsoft Security Essentials for myself and most of the members of my family. This is because Microsoft Security Essentials does a pretty good job and it is updated fast enough by Microsoft for the low-risk Internet browsing habits of myself and most of the members of my family. For the family members who have what we'll politely call less safe Internet browsing habits, they have either a second computer specifically for those unsafe habits or an antivirus that is a little more robust such as Sophos that I mentioned earlier.

I don't really want to start a fight between you and the members of your family, which have an opinion on the topic; if someone in the family or a friend strongly recommends a specific product and you trust their opinion (and especially if they work in the IT field), then take their recommendation. When deciding on a specific antivirus software for your computer, here are a few things to look at:

- How often do they update their virus definitions?—More often is better.
- How often do they update their software?—More often is better.
- Do they offer free upgrades?—Yes is better.
- Do they work with other companies to ensure that virus threats are found faster?—Yes is better.

That said, we aren't good enough friends for me to come over and fix your computer, so if you end up having problems, try one of the other ones that I mentioned in this section; they all have a free trial.

---

**Apple computers need antivirus software**

There is a long-held belief that because you are using a Mac, you can't get a virus on your computer. This couldn't be further from the truth. While it is true that there are less viruses running around the Internet that attack the Apple operating systems, there are plenty of them out there, and without an antivirus installed, you'll have no idea that one has tried to install itself on your computer.

Back in the day (the day being the late 1990s), there weren't any viruses for the Mac computer. This wasn't because the Apple operating systems of the day were more secure than the Windows operating systems of the day. It was purely a numbers game for the virus writers; in the late 1990s, there weren't enough people using Apple computers compared to the number of people using Windows computers. Back in the late 1990s, Microsoft had well over 90% market share with Apple having between 5% and 8% market share. This means that as a virus writer, if you are going to spend money writing a virus and you want to make the most money possible off of that virus, then you want to target most computers possible, which are Windows computers. Today, the market has changed and Microsoft's Windows operating system no longer has such a strong market share position with the Windows operating system now having less than 90% market share. This means that it is starting to become profitable for people to make viruses for other operating systems including the Apple operating system.

---

**NOTE****Not all viruses are for profit**

While a large number of viruses are written for profit, there are some viruses that are written simply to show off to other virus writers just how cool the virus they have written is. Back when viruses were first coming out, there were a lot more viruses, which were written just for the “sport” of it. In more modern days, most viruses are written to steal data and/or make someone money, either the virus writer or the person who hired the virus written, usually by stealing your money.

---

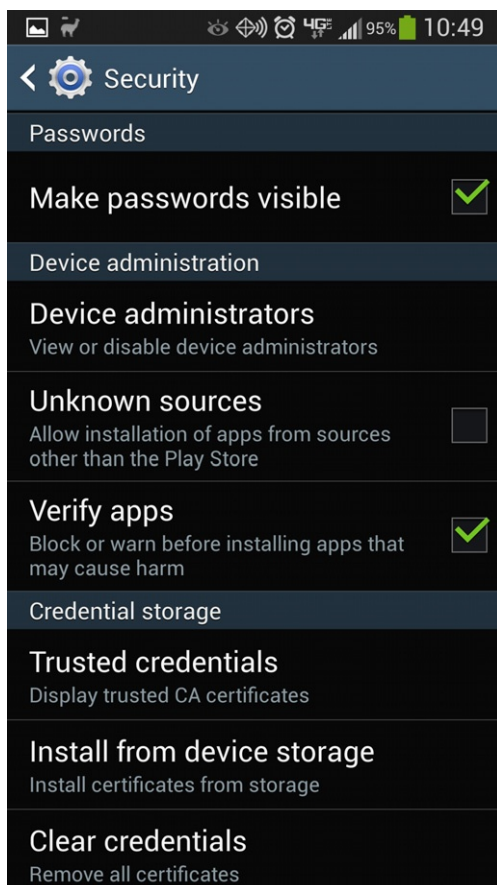
**Cell phones and tablets**

Cell phones are the newest attack vector for viruses as there are now cell phone-specific viruses out there. These viruses can be installed just like any normal application on the cell phone, often installed as a part of another application, which looks like another popular application. There are other ways to get a virus on cell phones. There have been flaws out there in some cell phones, which have allowed viruses to spread from phone to phone via text and picture messaging. You can read more about the specifics of the history of these mobile viruses at [http://basicsofdigitalprivacy.com/go/mobile\\_virus](http://basicsofdigitalprivacy.com/go/mobile_virus). The official application stores such as the Android Market, Apple App Store, and Microsoft Store are the safe places to install applications from. Other application stores such as the Amazon Appstore are usually safe, but there are no guarantees. Other market places out there aren’t considered safe at all. They claim that they are safe, but they aren’t considered safe by the companies who make the phones or the companies who run the antivirus companies.

The Windows and Android mobile operating systems both have antivirus applications available for them. These antivirus applications can help ensure that there is nothing running on the phones, which there shouldn’t be. For Android phones, the best way to ensure that there are no viruses installed is to make sure that the phone is configured to only allow installation of applications from the Play Store. Where you configure this will depend on the version of the Android operating system. Typically, it will be found within the Security section of the Settings icon. If the “Unknown sources” check box is unchecked, then the phone will prevent the installation of applications from third-party application stores as shown in [Figure 4.13](#). When this setting is disabled, any application store such as the Amazon Appstore won’t be available.

The recommendation is that if you are using another well-known application store such as the Amazon Appstore that you enable the “Unknown sources” setting each time you plan to install an application, then disable the setting as soon as the application has been installed. It is also recommended that you install an antivirus on the phone to ensure that you are protected from every application that is installed and updated no matter which application store the application is installed from.

With the iOS for the iPhone, there are antivirus applications available but they require that the phone be jail-broken so that the antivirus can be installed. This breaks

**FIGURE 4.13**

Security section of the Application settings with the Unknown sources setting disabled.

Apple's security model for the iOS operating system, which is a pretty locked down operating system. While jailbreaking, the phone is a whole different conversation; if the iPhone (or iPad or iPod) is jail-broken, it is still recommended that an antivirus is installed.

---

## NOTE

### Why all the attention to Android

Have you noticed that of the three major platforms, Android, iOS, and Windows Mobile, Android gets the most information in this section? That's because Android is the most open platform of the three, which means that it is the most susceptible to a virus.

---

Viruses for cell phones typically do two different things. The first thing they do is monitor your keystrokes and attempt to capture the usernames, passwords, credit card information that you enter for websites like Amazon and eBay, and your application store (or marketplace, etc.) account information. The other thing that these viruses will attempt to do is spread to everyone that you know. This is done via the phone numbers and e-mail addresses in your contact list. Your contacts will all get a text message and/or an e-mail that will have an attachment or a link, which will attempt to install the virus on their devices.

One last thing that these viruses may attempt to do is to dial phone numbers with specific US area codes, which charge you money just for making the phone call with the profits of these numbers being paid to the virus writers. These area codes include 809, 284, or 876 and a few others. The reason that these US area codes can charge high rates per minute is because these aren't actually in the United States. These numbers are actually based out of the Caribbean Islands so US billing laws don't apply as the Caribbean Islands aren't a part of the United States. The charges for these calls simply show up on your cell phone bill.

If you get hit with one of these viruses, contact your cell phone provider if you see calls on your cell phone bill to these area codes that you didn't make. The cell phone providers will work with the phone company where these numbers are based to attempt to get your charges reversed. This does require that your cell phone company will work with the offshore phone company as the charges are billed from the offshore phone company and your cell phone company can't refund the charges directly on their own.

## SUMMARY

When it comes to protecting the information on your computer from being viewed after a computer theft, data encryption is your best bet. Data encryption will force the person who is trying to read your data to have your password in order to get access to that data. When protecting yourself from a virus, an antivirus product installed on your computer and cell phone is critical in ensuring that the information that you place on the computer or cell phone isn't going to anyone but the people that are supposed to get the information.

# Posting Information Online

# 5

---

## INFORMATION IN THIS CHAPTER

- Kinds of information that shouldn't be posted online
- How to protect information that is posted online

This chapter talks about what you really shouldn't be posting online and how to protect what you do post online.

---

## KINDS OF INFORMATION THAT SHOULDN'T BE POSTED ONLINE

These are the kinds of answers that you'll typically hear when it comes to what you shouldn't be posting on the Internet on social media websites:

- Anything personal
- Anything you wouldn't want your grandmother and/or grandfather to see
- Anything you wouldn't want your parents to see
- Anything you wouldn't want your kids to see
- Anything you wouldn't want your boss to see
- Anything you wouldn't want your insurance company to see
- Anything you wouldn't want the government to see

A lot of this comes down to personal embarrassment at family gatherings (see the statements with grandparents, parents, and kids), getting fired (see the statement about your boss), losing your insurance (see the one about your insurance company), or getting arrested (see the one about the government). If you post something online, then odds are that someone that you don't intend of seeing it will see it. A perfect example is shown in [Figure 5.1](#).

---

### NOTE

#### Where did [Figure 5.1](#) come from?

You may be asking yourself "If people aren't supposed to be posting pictures of themselves online, how did you get this picture of someone in a bar bathroom?" That's a fair question. Thankfully, the answer wasn't very far away. The person in the picture isn't me (thankfully)

**FIGURE 5.1**

Example of someone doing something that they probably wouldn't want posted online in a bar bathroom.

but a friend of mine who was willing to have the picture included in the book as a fine example. Thankfully, many of my friends have no shame and are willing to do just about anything if it will help another friend get a point across.

And yes, this really is a picture of a couch in a men's room. It's from a small bar called Busch Garden (there's no "s" at the end) in Seattle, Washington, that some of us like to frequent when we are in town.

Anything that is posted online, be it text, photo, video, or anything else that we come up with in the future should be assumed that once it is online it will be online forever. Even if information is deleted from an online service such as [flickr.com](https://www.flickr.com/), [twitter.com](https://twitter.com/), and [facebook.com](https://www.facebook.com/), there is no guarantee that the information that you try to delete will actually be deleted. First of all, it's likely that the site that hosts it won't be deleting the files right away, if at all. In many cases, the End-User License Agreement (EULA) usually says that anything that is posted on these sites legally becomes their property and they can use them as they see fit.

For example, looking at the Facebook license agreement as of the summer of 2013, Facebook specifically says in the End User License Agreement (EULA) in Section 2.2, shown in [Figure 5.2](#), that "...removed content may persist in backup copies for a reasonable period of time (but will not be available to others)." There is nothing in the agreement that says what a "reasonable period of time" will be. It could mean days, months, or even years depending on how long Facebook decides

- delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
  3. When you or others who can see your content and information use an application, your content and information is shared with the application. We require

**FIGURE 5.2**

Screenshot of part of the Facebook EULA.

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the

**FIGURE 5.3**

Section 2.1 of Facebook's EULA as of the summer of 2013.

how long they should keep copies of their backup tapes. While Facebook doesn't publish their backup policies, there are many companies who keep backups for several years and others who keep a periodically taken backup forever.

## NOTE

### Define periodically

Reading the prior section, I'm using some incredibly vague words to describe vague situations. Let me be a little more specific with an example. A company that I worked for several years ago had a policy for keeping backups forever. In this case, backups were taken daily and were kept for 2 weeks. On Sunday, there was a weekly backup that was taken and was kept for a month. On the first of each month, there was a backup taken that was kept for 7 years. On the first of January, a backup was taken and that backup was kept forever. This would mean that if you uploaded a file to their service in March then deleted it on January second the file would be kept on their tape backups forever.

We can learn more about how Facebook deals with deleted data when we look at Section 2.1 of their license agreement (as of the summer of 2013) that states that you give Facebook a license to use your intellectual property (your photos and videos) for no cost until you delete the content as shown in [Figure 5.3](#). However, if a friend on Facebook shares your Intellectual Property (IP), then Facebook continues to have the license to use your IP until everyone that shares the photo or video has also deleted it.

This tells us that when you upload a picture and someone you are friends with shares it and you then delete the file, it won't be deleted because others will still have shared it. So if you delete it, it isn't actually deleted. It could live on Facebook's site without you having control of the file that you uploaded.

Reading the Flickr End User License Agreement, we first see that because the site is owned by Yahoo, we are bound by the Yahoo agreement. The Yahoo agreement as of the summer of 2013 doesn't specifically mention what happens when you delete specific content. The only reference talks about the fact that if you delete your account, your information may be retained in their archived records after your account has been deleted as shown in [Figure 5.4](#).

Based on the fact that Flickr is all about posting images online and people being able to download those photos, we need to be really sure that anything that we upload to Flickr is safe to be seen by others, forever. Because of this, if you post something to Flickr, you should expect that even if you go and delete that image, you could easily expect to see that picture come back online somewhere else.

There are some SD cards that you can purchase for camera that allow the camera to automatically upload the photos that are taken with the camera to the sites such as Flickr automatically. These include cards like the Eye-Fi cards. It's easy to forget that you have a card such as the Eye-Fi card installed in the camera, so you could end up taking pictures that you don't necessarily want uploaded to the Internet.

When it comes to the Twitter Terms of Services (TOS) as of the summer of 2013, there is nothing listed in the terms of services at all about what happens to tweets that are deleted. This lack of information extends to pictures that are uploaded to the Twitter photo-sharing service. Part of this may be because there is a feed from Twitter to the United States Library of Congress. This feed is allowing the Library of Congress to archive every tweet that has been posted to the Twitter service. What happens to these archived tweets when the user that posted the tweet deletes it isn't explained.

We can assume that tweets aren't actually deleted from Twitter's database. This is shown a little bit on the Twitter Support site under the topic of Deleting a Tweet that is available at <http://basicsofdigitalprivacy.com/go/DeleteTweet> and is shown in a note on the page as of the summer of 2013 as seen in [Figure 5.5](#). This tells us that the Tweets that you delete aren't actually deleted since they will show up in Twitter Search. Search data on Twitter are only available for a small period of time so at the longest, the tweets will fall out of search when they simply expire from the search window.

You can delete your Yahoo! account by visiting our [Account Deletion](#) page. Please [click here](#) to read about information that might possibly remain in our archived records after your account has been deleted.

**FIGURE 5.4**

Account deletion section of Yahoo's EULA.



**Note:** Deleted Tweets sometimes hang out in Twitter search, they will clear with time.

### FIGURE 5.5

Note showing that tweets aren't deleted right away.

---

## NOTE

### Why am I bringing this up?

You may be asking yourself why I'm talking about all these legal stuff on these specific sites. The reason that I'm bringing this up is because you need to know what these sites are doing with all the information that you have uploaded. If you end up posting something that you don't want other people to see, such as something you regret posting the next day, deleting may not remove it because there is no guarantee that what was posted is actually going to be deleted.

Most of the time, people post things that they end up regretting the next day because drinking (or other recreation) is often involved. At these times, people tend to make poor decisions about what they should be posting online. Unfortunately there isn't any sort of filter on cell phones or computers to prevent people from doing stupid things online. This sort of thing takes the old problem of drunk dialing old boyfriends or girlfriends to an all new level. With drunk dialing, the only person that you've shown the stupidity to is the person on the other end of the phone, assuming that they even answer. Now with social networking websites, you've got the ability to tell the entire world what sort of stupid thing you've been doing.

---

Posting information online can have actual major consequences for the people that post them. CNN and BuzzFeed have put together a great montage about 10 people who posted online stupid things that they have done that have ended up getting them fired. You can find the CNN article and video at <http://basicsofdigitalprivacy.com/go/CNNFired>. This includes the Taco Bell employee who licked taco shells, a teacher who thought that her male students were attractive and how much she liked smoking weed (the mostly naked pictures that her students could easily enough find probably didn't help either), the Australian miners who did the "Harlem Shake" and posted it online, among several others.

---

## NOTE

### More about the teacher

Of the 10 people highlighted in the CNN and BuzzFeed article and video that are posted earlier, I'd have to say that the dumbest of all was the teacher. Teachers are often held to a higher standard than others because they deal with kids as a part of their job. This isn't anything new and has gotten a lot more lax over the years. All that said if you'd like to see exactly what it'll take to get yourself fired from a teaching position, you can read the details at <http://basicsofdigitalprivacy.com/go/teacher>.

It should be noted that she has denied doing anything wrong, but in the end, she still lost her job over her Twitter account.

---

---

## HOW TO PROTECT INFORMATION THAT IS POSTED ONLINE

Most if not all of the social networking services allow you to protect information that you post online so that you can control who sees the information that you post online. It is very much recommended that you protect the information that you post online so that people that you don't want seeing your social networking posts can't see them. Just keep in mind that these protections only apply to new items that you post and not to items that were already posted online.

---

### NOTE

#### Things change online

With everything being talked about in this section, please keep in mind that the functionality available from these services may be different from what is listed in this book. The reason for this is that services like Twitter and Facebook are always changing as they attempt to improve their services. Because of this, the settings may not look exactly like the examples shown in the book and where you click might be a little different. All these settings and instructions are current as of the writing of this book, which was in the summer of 2013.

---

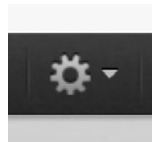
### Twitter

Twitter offers you the ability to protect your tweets by protecting your account. When you protect your tweets on Twitter, this prevents anyone from seeing your Tweets until you approve them to be able to follow your account. This prevents your tweets that you made after making your account protected from showing up in Search.

You can change your settings by logging into the Twitter webpage on a computer and click on the gear icon at the top right of the screen that looks something similar to that shown in [Figure 5.6](#).

On the setting page, scroll down to the Tweet Privacy setting that should be around halfway down the page. Checking the box next to the in the Tweet Privacy setting, shown in [Figure 5.7](#), will turn your account into a protected account and only your followers will be able to view your tweets.

Keep in mind that there are still ways that tweets from a protected account can be shared and therefore viewed by others. The first way would be by a follower doing an "old style" retweet. This is where someone takes a tweet that is a protected tweet, which can only be seen by the person's followers, and is then tweeted by someone with "RT" in front of the tweet. Now everyone who follows the second person can see the tweet that the first person posted.



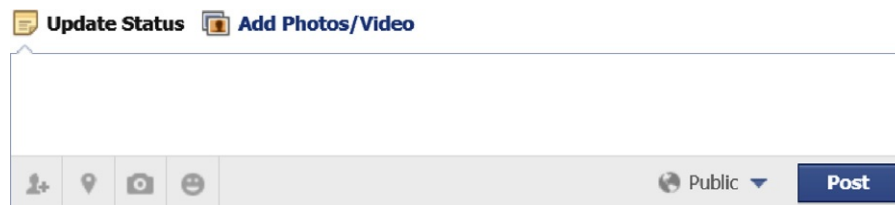
**FIGURE 5.6**

Twitter settings button.

---

**FIGURE 5.7**

The Tweet Privacy setting from the Twitter settings page.

**FIGURE 5.8**

Facebook new post dialog.

To spell this out a little easier, let's assume that we have a person named Kris who has protected her tweets because she doesn't want people that she doesn't know to see her tweets. She tweets something that Steve sees that he wants to share with his followers. Steve then retweets the tweet that Kris posted making it so that people who follow Steve but not Kris can now see Kris's tweet.

Unfortunately as long as you are using Twitter, there is no way to prevent this situation from happening as you can't prevent another user from retweeting your tweets.

## Facebook

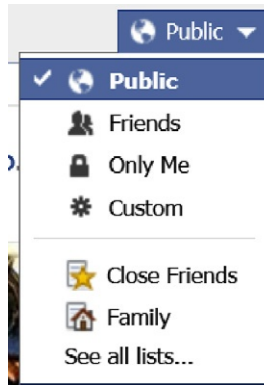
When posting something on Facebook, there are a couple of ways to limit the people who can view your posts.

### *Securing a specific Facebook post*

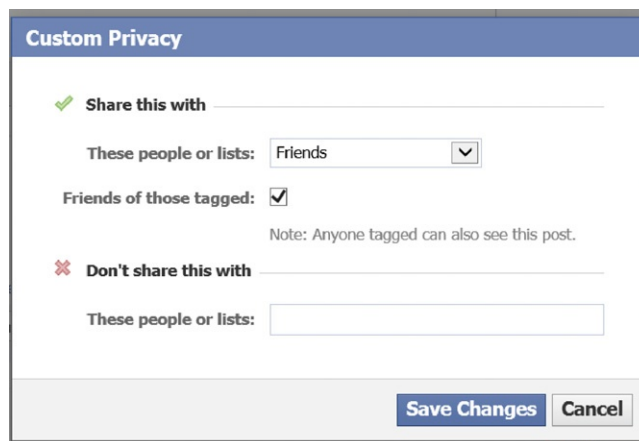
The first is to secure the actual post itself. When writing up a new post on Facebook, you've probably seen the little grayed out drop-down menu next to the post button as show in [Figure 5.8](#).

Normally when things are grayed out, they are disabled but this isn't the case with Facebook. When you click on the drop-down menu shown in [Figure 5.8](#), you'll get a drop-down menu that will look similar to the one shown in [Figure 5.9](#). This drop-down allows you to configure who has the ability to see this specific post. You can leave the setting at Public that is the default that will allow everyone on Facebook to see the post if they went to look at your wall.

By selecting “Friends” from the menu shown in [Figure 5.9](#), only people who are your friend on Facebook would be able to see the post. By selecting “Only Me” from the menu shown in [Figure 5.9](#), you are the only person who can see the post. The most powerful option on the menu shown in [Figure 5.9](#) is the “Custom” option. By selecting this option, another menu is shown that allows specific people or groups of people that you have set up within Facebook to see or not see the post. This new menu shown in [Figure 5.10](#) allows you to specifically list out people that you do or do not want to be able to see the post.

**FIGURE 5.9**

Facebook permissions menu.

**FIGURE 5.10**

“Custom Privacy” menu in Facebook.

The screenshot shown in [Figure 5.10](#) shows the default version of this screen where you can select a specific group of people to allow to see the post then the “Don’t share this with” section where you can exclude people from this list.

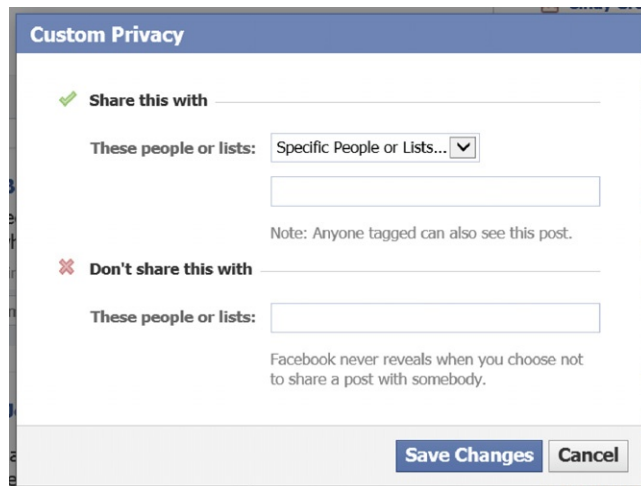
As shown in [Figure 5.10](#), there is a dropdown in the “Share this with” section. This defaults to “Friends” when opened. The other options on this list are “Friends of Friends” that would allow your friends as well as their friends to be able to see the post. The other option of note is the “Specific People or Lists. . .” option that allows you to specify that the post should only be visible to the specific people that are put into the dialog box that appears when “Specific People or Lists. . .” is selected as shown in [Figure 5.11](#).

If, for example, I wanted to post a message on Facebook where I complained about the work that my friend Thomas LaRock was doing while working at the technical editor of this book (he did a fantastic job, it’s just an example), I probably wouldn’t want him to see that post on Facebook. So in order to do this, I would select the “Share this with” setting to Friends so that only my friends can see the post, and then in the “Don’t share this with” section, I would put Tom’s name as shown in [Figure 5.12](#).

After making the changes and clicking the “Save Changes” button, you’ll be shown something similar to that shown in [Figure 5.13](#). The post can then be written and posted as normal with only the limited people being able to see the post.

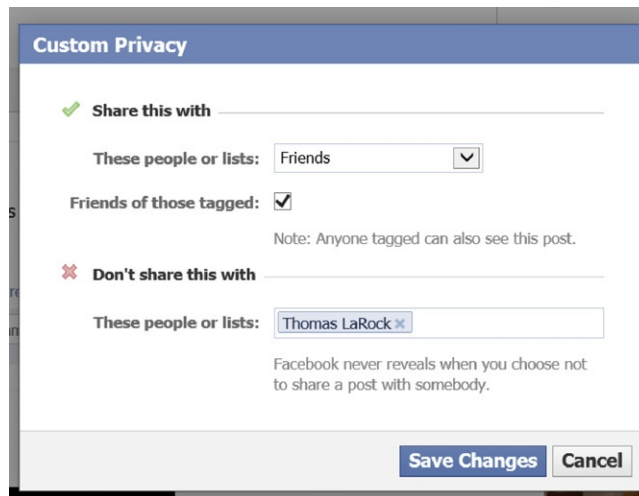
### ***Setting Facebook privacy settings***

One place where Facebook is doing a better job than some of the other social networking websites is in the privacy settings. The Facebook privacy settings allow you to configure who by default can see your new posts, who can contact you,

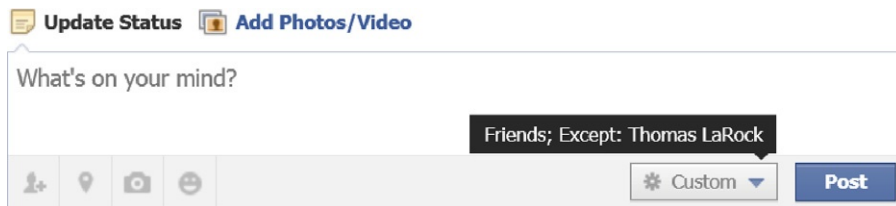


**FIGURE 5.11**

The “Custom Privacy” dialog box with the setting changed to “Specific People or Lists . . .”

**FIGURE 5.12**

Facebook's "Custom Privacy" screen filled out.

**FIGURE 5.13**

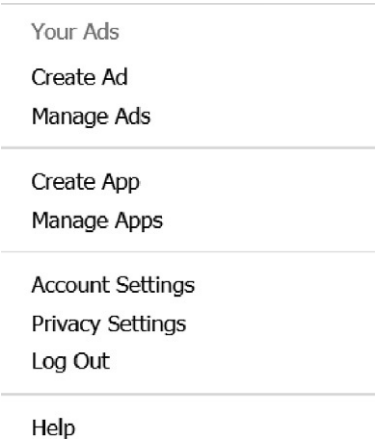
Facebook new post dialog with the viewing of the post limited.

**FIGURE 5.14**

Facebook settings icon.

and who can search for you using your e-mail address or phone number. The privacy settings can be found by clicking the little light blue gear on the upper right-hand side of the Facebook webpage shown in [Figure 5.14](#).

Once clicking on the icon shown in [Figure 5.14](#) a menu similar to the one shown in [Figure 5.15](#).



**FIGURE 5.15**  
Facebook settings Menu.

**Privacy Settings and Tools**

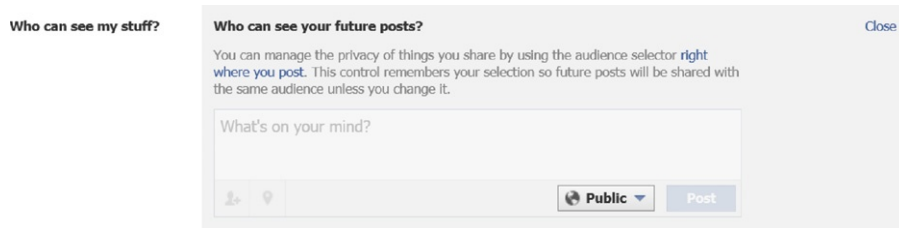
Who can see my stuff?	Who can see your future posts?	Custom	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address or phone number you provided?	Everyone	Edit
	Do you want other search engines to link to your timeline?	On	Edit

**FIGURE 5.16**  
Facebook Privacy settings.

By clicking on the “Privacy Settings” option in the menu shown in [Figure 5.15](#), the actual screen that allows you to change the privacy settings will be shown, which will look similar to what is shown in [Figure 5.16](#).

The first section shown in [Figure 5.16](#) allows you to change who can view your posts. By clicking on the “Edit” link next to “Who can see your future posts?,” the screen will be changed to look something like what is shown in [Figure 5.17](#).

By clicking on the “Public” drop-down menu, you can customize the permissions much like when a new post is being written as shown in [Figures 5.10–5.12](#).

**FIGURE 5.17**

Customizing the future posts permissions on Facebook.

**FIGURE 5.18**

Sample Facebook post.

When making changes to permissions via the “Who can see your future posts?” setting, these changes only affect new posts. If the permissions for older posts need to be changed, the only option for changing the permissions in bulk is to limit the past posts to only being visible to your friends. This is done by clicking the “Limit Past Posts” link to the right of “Limit The Audience for Old Posts on Your Timeline” option shown in [Figure 5.16](#).

If permissions from older posts need to be changed one by one, this can be done by going to your wall on Facebook and locating the specific post that you wish to edit. Once the post has been located, click on the small gray gear next to the time when the post was made as shown in [Figure 5.18](#).

After clicking on the gray gear shown in [Figure 5.18](#), a menu will be shown that looks similar to the one shown in [Figure 5.9](#). The settings can then be changed using the screens shown in [Figures 5.10–5.12](#).

With these various settings, you’ll be able to prevent people who you don’t want to see specific posts from being able to see them. This same technique is used to secure pictures, videos, etc., on Facebook.

## Flickr

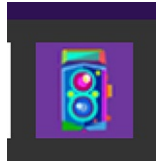
Like Facebook and Twitter, the other social networking websites that have been mentioned in this chapter, Flickr includes some privacy settings that can be used to keep the pictures that are being posted online from being viewed by people that you wouldn’t want them viewed by. There are a variety of settings available to you and understanding each one and what exactly it controls is key to keeping your personal data on Flickr private.



Accessing the privacy settings on Flickr is quite easy. Simply go to the Flickr homepage [www.flickr.com](http://www.flickr.com) and log into the site using your normal username and password that you use for the site. After logging in put your mouse on the small avatar icon in the upper right corner of the screen as shown in [Figure 5.19](#). In this example, the avatar is the default avatar that yours should look similar to.

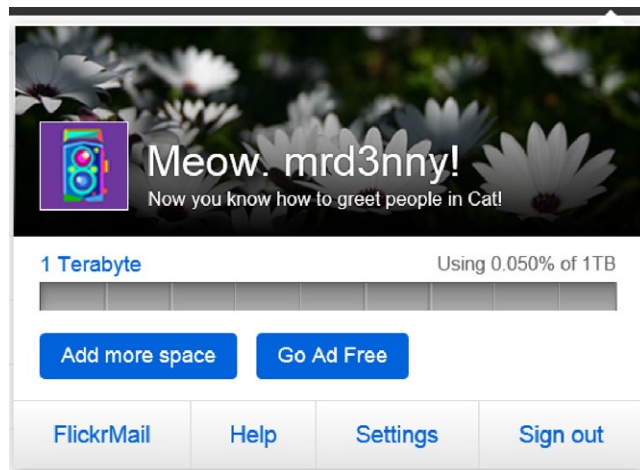
When your mouse has been placed over the avatar, a menu should appear similar to the one shown in [Figure 5.20](#). If the menu doesn't appear, click on your Avatar that should cause the menu to appear as well. Once the menu has appeared, click on the settings link shown at the bottom of [Figure 5.20](#).

The settings page has four tabs with all the privacy settings being shown on the "Privacy and Permissions" tab. Clicking on this tab will show you the various settings.



**FIGURE 5.19**

Example of an Avatar on Flickr's homepage.



**FIGURE 5.20**

Pop-up menu on Flickr's site.

The first permission shown on the Privacy and Permissions tab, partially shown in [Figure 5.21](#), is the ability to control who has access to all your original picture files that have been uploaded.

By default, this setting is configured to allow anyone to download the original files as shown in [Figure 5.22](#). There are four other options available with this setting: “Only you,” “Your friends and family,” “Your contacts,” and “Any Flickr member.”

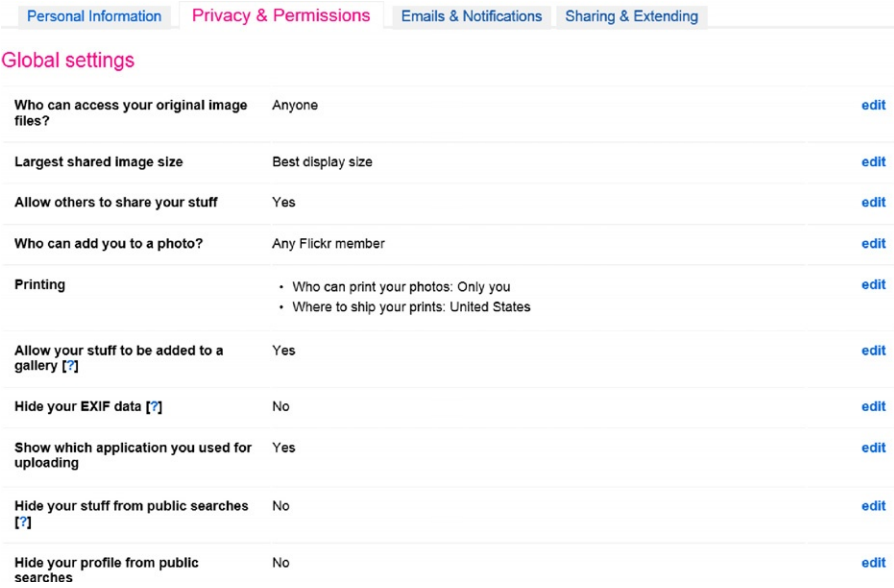


FIGURE 5.21

Partial view of the “Privacy and Permissions” settings.

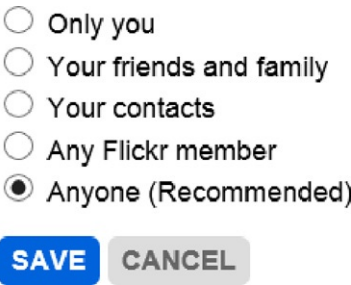


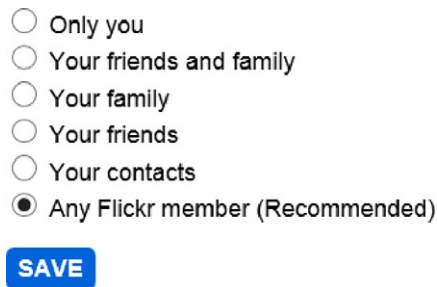
FIGURE 5.22

Settings options for who should be able to access the original files on Flickr.

The “Only you” setting prevents any other member from seeing your pictures. The “Your friends and family” setting allows anyone who you have configured as being a friend or a member of your family to be able to see your pictures and no one else. The “Your contacts” setting allows anyone who is configured on Flickr’s website as a contact to be able to see the setting. The final option “Any Flickr member” allows anyone who is signed into the Flickr website the ability to view the pictures that have been uploaded.

The next setting down the list shown in [Figure 5.21](#) is “Who can add you to a photo?,” which is a very important setting when it comes to ensuring that you maintain the most possible control over your online presence. When others are allowed to tag you in pictures that they have posted on Flickr, these pictures can impact both your online and your off-line reputation. At the beginning of this chapter, we learned about the fact that we need to ensure that we don’t post information online that we don’t want others to see online. Well what happens when someone posts information about us and we can’t control it? This setting gives us the ability to control that, at least on the Flickr website. The “Who can add you to a photo?” setting is the most detailed setting we have control of so far as shown in [Figure 5.23](#).

The six options that are shown in [Figure 5.23](#) are not set with the best possible privacy option configured by default. By default, Flickr is configured to allow anyone who uploads a photo with you in it to be able to tag you in the photo. While Flickr recommends this setting to be the default setting, this is for their benefit, not yours. They benefit from this setting being enabled by making a more dynamic platform that allows for the easiest sharing of photographs and videos possible. However, this is purely in their best interest and not in yours. Your best interest as the user of Flickr (and other social networking sites in general) is to ensure that while using the service, you have as much control over your data as possible, which isn’t going to work well with the social networking sites’ best interest. The setting that should be used, which is in your best interest, is to select the “Only you” option shown in [Figure 5.23](#). This way, you maintain complete control over what pictures can be assigned to you.



- ☐ Only you
- ☐ Your friends and family
- ☐ Your family
- ☐ Your friends
- ☐ Your contacts
- ☒ Any Flickr member (Recommended)

**SAVE**

**FIGURE 5.23**

“Who can add you to a photo?” setting options.

An acceptable setting from a personal data privacy perspective would be to allow people that you trust to be able to tag you in pictures, also known as your family, which is one of the available options. The other options such as “Your friends,” “Your friends and family,” “Your contacts,” and “Any Flickr member” settings allow people who probably aren’t in your most-trusted circle to be able to tag you in pictures.

The next setting with regard to privacy to adjust is the “Who can see your EXIF data?” setting. Before we can decide if we want to allow others to see our EXIF data, we need to know what the EXIF data are. The EXIF data are information that is stored within the photograph and stores a variety of information about the photograph. This information includes information about the camera, the lens, the shutter speed, the date and time the picture was taken, and, in a lot of cases, the GPS location of the picture. Having the GPS information available to anyone on the Internet tells people potentially where your home is, where your office is, where you’re, where your friends live, where you vacation, etc. You can turn this feature off within the camera or camera phone. Check with the technical support department for your camera for more information about how to disable this feature. Based on all this information turning off the EXIF data from being available to people who are viewing your photographs online may be a good idea for many people. The EXIF setting only allows to be turned on or to be turned off. For the sake of personal privacy, the setting of “Hide my EXIF data?” should be set to “Yes” as shown in [Figure 5.24](#).

The next setting on Flickr’s privacy settings page that we need to worry about is the “Who can see what on your profile” setting as shown in [Figure 5.25](#). This allows various groups of people to see the four settings that this setting controls. These four settings are “E-mail address,” “Instant messaging names,” “Real name,” and “Current city.” By default “E-mail address” and “Instant messaging names” are available only to people who are your contacts while “Real name” and “Current city” are available to anyone.

Again, like with the EXIF setting, the settings shown in [Figure 5.25](#) are not set with your best interest in mind. This is because it allows anyone to see where you most recently uploaded pictures from. Like with the settings discussed earlier in this section, these settings, specifically the “Current city” setting, should be set for trusted people only such as the option from the list “Family and Friends.” This setting is the most restrictive of the available options for these settings.

### Who can see your EXIF data?

Hide my EXIF data? ☒ Yes

**FIGURE 5.24**

Flickr’s EXIF setting.

## Who can see what?

You can control who is able to see different parts of your profile. For each of the items below, select who should be able to view it. (We've tried to set intelligent defaults for you!)

Email address	Any of your contacts (default) ▼
Instant messaging names	Any of your contacts (default) ▼
Real name	Anyone (default) ▼
Current city	Anyone (default) ▼

**FIGURE 5.25**

Flickr's "Who can see what" setting.

---

### NOTE

#### The most restrictive isn't always restrictive enough

While it is good that Flickr gives you the ability to control these settings, in my opinion, these settings aren't restrictive enough. In today's always on, always online, social media world, the concept of friends in the online world and the concept of friends in the off-line world aren't always the same. When using this setting, it is important to remember that you are only marking people who are actually friends or family members as friends or family, respectively, so that people that shouldn't have access to this sort of information don't get it by accident.

---

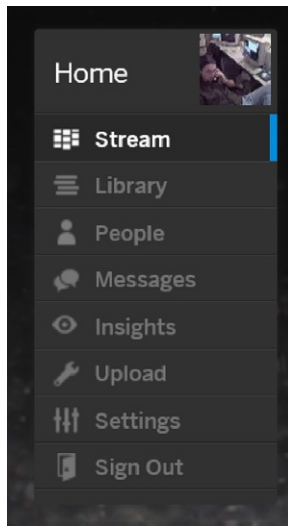
## MySpace

Privacy settings on the MySpace website are probably the least flexible of all the social networking sites that I have seen. The only option that MySpace gives you is the ability to configure a profile as a "Restricted Profile." Having a restricted profile means that you have to approve all connection requests before they will be connected to you. A restricted profile also limits "certain content is limited to profiles you have allowed to connect to you" according to the MySpace webpage.

Changing the profile setting from a public profile to a restricted profile is a pretty basic process. First, log onto the MySpace website at [www.myspace.com](http://www.myspace.com). Then click on the settings button on the main menu, shown in [Figure 5.26](#), typically shown on the left of the webpage.

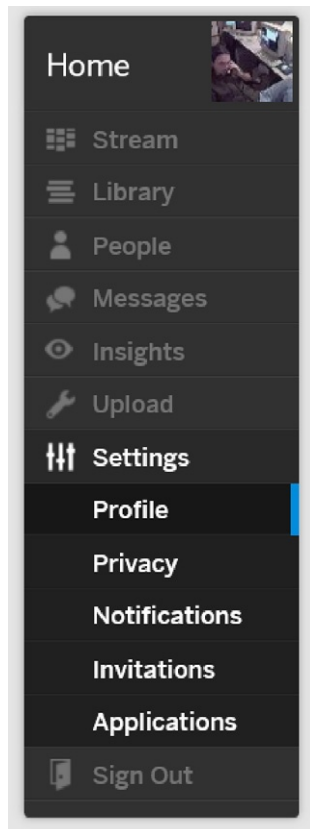
Once the settings menu has opened, as shown in [Figure 5.27](#), several additional options become available including the Privacy Settings option. Selecting the Privacy option from the menu allows you to view the full privacy settings menu.

As stated, the MySpace website only has a single privacy setting. This setting, shown in [Figure 5.28](#), allows you to change your profile from public to restricted and back as needed.



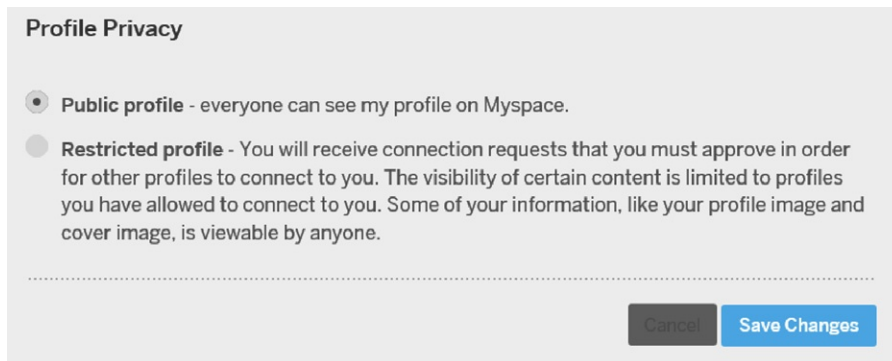
**FIGURE 5.26**

MySpace home menu.



**FIGURE 5.27**

Settings menu selected.

**FIGURE 5.28**

Profile Privacy setting on the MySpace homepage.

## SUMMARY

As we've seen in this chapter, there is a variety of information that simply shouldn't be posted online. While it may seem like a good idea to post your entire life online, there are people out there who can use the information that you post online against you. This includes family members, employers, bosses, potential employers, and law enforcement. Many of the social networking sites include some sort of privacy settings, as shown throughout this chapter where you have been shown how to change the privacy settings of Twitter, Facebook, Flickr, and MySpace.

Not all of the social networking sites include privacy settings, and not all of the privacy settings are created equal some sites giving much more fine-grained control than other sites give. When selecting the social networking site to use, be sure to select social networking website that provides the level of privacy over your personal data that you want to give.

# Who's Watching What You Do?

# 6

---

## INFORMATION IN THIS CHAPTER

- How can someone watch what I do?
- How can a government watch what I do?
- How can I stop people from watching what I do?

This chapter talks about how others including other people and various governments are able to see what you are doing online. We will also talk about some of the things that you can do to prevent others from watching what you do online and why you may or may not want to do these things.

---

## HOW CAN SOMEONE WATCH WHAT I DO?

When it comes to what people can see you are doing on the Internet, the amount of what they are watching will totally depend on how secure you have made your online life and how determined they are to see what you are doing. There are two basic tasks that you do on the Internet, sending and receiving e-mail and browsing the web.

---

### NOTE

#### Some assumptions

For the purposes of this chapter, there are a few assumptions that are going to be made. The first one has to do with sending and receiving e-mail. When talking about sending and receiving e-mail, it is assumed that you are using an e-mail client such as Microsoft Outlook, Eudora, OSX Mail, and Windows 8 Mail. This includes using the e-mail app on your phone like the "Mail" app on Android, Apple, Windows Mobile, and BlackBerry phones.

---

Many of the solutions to preventing people from viewing what you are doing online will be rather technical. Throughout this chapter, they will be broken down into the most digestible parts possible. One of the problems with a lot of these sorts of highly technical solutions is that they are made by IT professionals for IT professionals without very much thought being given to how to make these solutions more accessible to the general public at large who doesn't necessarily have the technical experience or knowledge to configure these solutions. Most if not all of these solutions have documentation, but often, this documentation is written for IT professionals and often makes a lot of assumptions about the technical experience of the reader.



## E-mail

When it comes to monitoring e-mail that someone sends and receives, there are a couple of different methods that someone can use. The easiest is going to be to install something on your computer that tracks all the e-mails that are received by you and sent to you. There are a variety of applications out there that can do this. Some are easy to detect and others are much harder to detect, with some being detected by anti-virus software and some not being detectable by antivirus software. While you might consider all of these sorts of applications as viruses, some applications in this category are actually legitimate software packages out there that do the sort of things that are being talked about in this section.

---

### NOTE

#### Full disclosure

Some full disclosure here. I've got quite a bit of experience working in this sort of space. Several years ago, I worked for a company that made a desktop monitoring application that could capture e-mails that you received or that you sent. That software was sold just like any other software that you could purchase with the basic idea for the home user product being that you could monitor what your kids were doing on the Internet to ensure that they weren't doing something online that they shouldn't be doing. In the business version of the product, we were monitoring to make sure that employees were doing things that they should be doing and that they weren't sending out customer information out via e-mail.

---

When monitoring software is installed on the computer that they are monitoring, the software works in few different ways. One option is to monitor the network protocol that is used by all e-mail clients to talk to the e-mail servers. In the past, this method would have been mostly useful, but over the past few years, most e-mail servers today require encrypted connections so monitoring the network ports isn't all that effective.

The second option that is available to the software developer who creates the monitoring software is that he or she can talk to the e-mail software using the application programming interface (API), which has been published by the e-mail software developer. This API would allow the person who is writing the monitoring software to read any e-mails that the software sends or receives. Because the monitoring software is asking the e-mail software for the e-mails after they have been received from the server, any encryption that is used in the communication process between the server and the user's computer would be bypassed.

A third option that would be available to companies such as the Internet backbone providers would be to monitor the network traffic at the e-mail server side. While the network traffic between the e-mail application and the e-mail server is most likely encrypted, odds are the network traffic between the e-mail server that you use and the e-mail server that the person you are e-mailing uses isn't encrypted as shown in [Figure 6.1](#). While some e-mail servers are configured to communicate with other e-mail servers using an encrypted connection, this is not the default communication method.

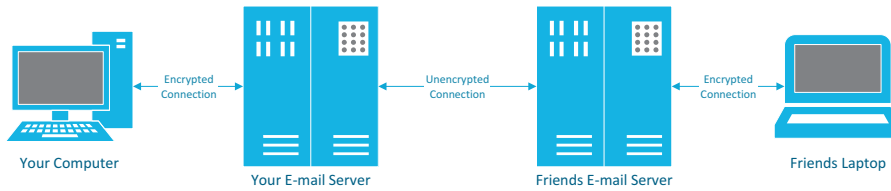
**FIGURE 6.1**

Diagram showing which connections are typically encrypted and which connections are not typically encrypted.

Communication between e-mail servers is not encrypted by default. However, it is possible that e-mail servers can be configured to request encrypted connections when transmitting from one e-mail server to another, but since it is not a default setting, this configuration is often skipped. Unfortunately, there is no way as a user of the e-mail server to see if the server is configured to request an encrypted server to server connection.

Another way that e-mails can be viewed is by the Internet service provider that owns the e-mail server that the mail is delivered to. Employees at the Internet service provider such as the technical support department and the systems administration team would have access to view the e-mails within the customers e-mail box. Depending on how the security at the Internet service provider has been configured, these employees may only have access to view the header information of the e-mails that would include who sent the e-mail, who received the e-mail, the subject of the e-mail, and when the e-mail was sent and when it traveled through each of the e-mail servers that handled the e-mail.

## NOTE

### Having access to e-mail

Back in my late teens and early 20s, I worked for a large Internet service provider in Southern California starting in their technical support department. As a routine part of our job as technical support representatives, we would deal with helping people troubleshoot problems with their e-mail. At this time, over 99% of the home Internet users were using dial-up Internet. This meant that e-mails needed to be small in order for users to download them. The large majority of e-mail problems that users would call up about were because they weren't able to download their e-mail because it would time out when attempting to download the e-mails.

The first step in troubleshooting this problem for customers would be to log into the users mailbox. We could then view the list of e-mails that were in the user's mailbox. We could then view the contents of the message and tell the customer what the contents of the e-mail were before deleting the e-mail. Once the e-mails that were too large were deleted, the customer would be able to download their e-mail.

Now in this case, the system was set up in such a way that the user's username and password were required in order for the technical support rep to access the user's mailbox. The members of the systems administration team did not have this same restriction. They

*Continued*

could, if needed, access a user's mailbox directly and delete specific e-mails as needed as well as delete e-mails if needed, and the customer would never know that the e-mails had been deleted.

The same applies to company e-mail systems at most companies. The systems administration team can access the e-mail of every employee in the company if needed without the person, whose mailbox it is, knowing that the systems administrator had accessed the e-mail.

In addition to the servers that are used to send the e-mail and the server that receives the e-mail as shown in [Figure 6.1](#), there could be any number of e-mail servers between the two servers that we can see in some sample e-mail headers in [Figure 6.2](#).

```
Received: from mail130-va3-R.somecompany1.com (10.7.14.254) by
VA3EHS08E008.somecompany1.com (10.7.40.28) with Microsoft SMTP Server id
14.1.225.23; Mon, 30 Apr 2012 12:26:19 +0000
Received: from mail130-va3 (localhost [127.0.0.1]) by mail130-va3-R.somecompany1.com
(Postfix) with ESMTD id 762811C048E; Mon, 30 Apr 2012 12:26:19 +0000 (UTC)
X-SpamScore: -1
X-BigFish: PS-1(zzbb2dI93711c89bh936eKc857h98dKzz1202h1082kzz8275eh8275bh8275dh186M4376pa1495iz2dh2a8h65bh839hd25h)
X-Forefront-Antispam-Report: CIP:207.46.4.203;KIP:(null);UIP:(null);IPV:(null);H:SN2PRD0102HT029.prod.somecompany2.com;RD:non
Received: from mail130-va3 (localhost.localdomain [127.0.0.1]) by mail130-va3
(MessageSwitch) id 13357887766367_10498; Mon, 30 Apr 2012 12:26:17 +0000
(UTC)
Received: from VA3EHS08E014.somecompany1.com (unknown [10.7.14.237]) by
mail130-va3-R.somecompany1.com (Postfix) with ESMTD id 51AD81A0083; Mon, 30 Apr 2012
12:26:16 +0000 (UTC)
Received: from SN2PRD0102HT029.prod.somecompany2.com (207.46.4.203) by
VA3EHS08E014.somecompany1.com (10.7.99.24) with Microsoft SMTP Server (TLS) id
14.1.225.23; Mon, 30 Apr 2012 12:26:16 +0000
Resent-From: <mailinglist@somecompany.com>
Received: from mail1109-va3-R.somecompany1.com (216.32.180.115) by
SN2PRD0102HT029.prod.somecompany2.com (10.27.90.112) with Microsoft SMTP
Server (TLS) id 14.15.65.3; Mon, 30 Apr 2012 12:26:18 +0000
Received: from mail1109-va3 (localhost [127.0.0.1]) by
mail1109-va3-R.somecompany1.com (Postfix) with ESMTD id 600A316057E for
<mailinglist@somecompany.com>; Mon, 30 Apr 2012 12:26:12 +0000
(UTC)
Received: from mail1109-va3 (localhost.localdomain [127.0.0.1]) by mail1109-va3
(MessageSwitch) id 1335788770273116_4366; Mon, 30 Apr 2012 12:26:10 +0000
(UTC)
Received: from VA3EHS08E002.somecompany1.com (unknown [10.7.14.250]) by
mail1109-va3-R.somecompany1.com (Postfix) with ESMTD id 3948C40071 for
<mailinglist@somecompany.com>; Mon, 30 Apr 2012 12:26:10 +0000
(UTC)
Received: from chloutboundpool.messaging.somecompany.com (216.32.181.186) by
VA3EHS08E002.somecompany1.com (10.7.99.12) with Microsoft SMTP Server (TLS) id
14.1.225.23; Mon, 30 Apr 2012 12:26:09 +0000
Received: from mail1211-ch1-R.somecompany1.com (10.43.68.241) by
CH1EHS08E010.somecompany1.com (10.43.70.60) with Microsoft SMTP Server id
14.1.225.23; Mon, 30 Apr 2012 12:26:08 +0000
Received: from mail1211-ch1 (localhost [127.0.0.1]) by
mail1211-ch1-R.somecompany1.com (Postfix) with ESMTD id 26AF63E0706 for
<mailinglist@somecompany.com.FOPE.CONNECTOR.OVERRIDE>; Mon, 30
Apr 2012 12:26:08 +0000 (UTC)
Received: from mail1211-ch1 (localhost.localdomain [127.0.0.1]) by mail1211-ch1
(MessageSwitch) id 1335788766502782_1737; Mon, 30 Apr 2012 12:26:06 +0000
(UTC)
Received: from CH1EHS08E011.somecompany1.com (snatpool2.int.messaging.somecompany.com
[10.43.68.233]) by mail1211-ch1-R.somecompany1.com (Postfix) with ESMTD id
73F4E3C027F; Mon, 30 Apr 2012 12:26:06 +0000 (UTC)
Received: from VA3DIAHUB054.RED001.local (65.55.171.153) by
CH1EHS08E011.somecompany1.com (10.43.70.11) with Microsoft SMTP Server (TLS) id
14.1.225.23; Mon, 30 Apr 2012 12:26:06 +0000
Received: from VA3DIAHUB054.RED001.local ([10.8.234.199]) by
VA3DIAHUB054.RED001.local ([10.8.230.53]) with mapi; Mon, 30 Apr 2012
05:26:12 -0700
```

**FIGURE 6.2**

E-mail headers from a sample e-mail.

The e-mail headers shown in [Figure 6.2](#), which are from an e-mail that I received from a mailing list that I'm subscribed to, are read from bottom to top with each server that receives and processes e-mail starting with "Received:". In the case of this example, we can see 16 different servers that the e-mail past through from the person who sent the e-mail until it was received by my mailbox. The e-mail headers show that the e-mail passed through a variety of servers each with their own domain name and appearing to be from a few different companies. There are a variety of reasons why different companies handled this e-mail. The sending company could have some of their antivirus services outsourced to another company that would mean that this additional company would need to receive the e-mails, or the third company could be used to help manage outbound e-mail routing, or it could simply be that the company has a very large e-mail sending infrastructure because they have to be able to handle billions of e-mails per day, and so they have configured a large complex system to assist them in the handling of these e-mails.

All these servers that are processing this e-mail as it was moved from the sender to my e-mail box could have been configured to store this e-mail for any period of time, allowing the administrator to view the e-mail without the knowledge of the person that sent the e-mail or from me the receiver of the e-mail.

## **Web browsing traffic**

Viewing the web traffic or someone who is browsing the Internet isn't quite as easy as viewing their e-mails. The primary reason for this is that e-mails sit on servers and can be viewed at any time that they are sitting on the server so long as the person trying to view them either has the username and password for the e-mail account or has the needed rights to the e-mail server by working for the company that owns the server that the e-mails were received by or the server that they were transmitted through.

With web browsing, the network traffic isn't being processed through a large number of servers. Network traffic from browsing the Internet also happens in real time. After the webpage has been requested and transmitted from the server to the user's computer, there's no trace of the specific data that were transmitted between the user and the server.

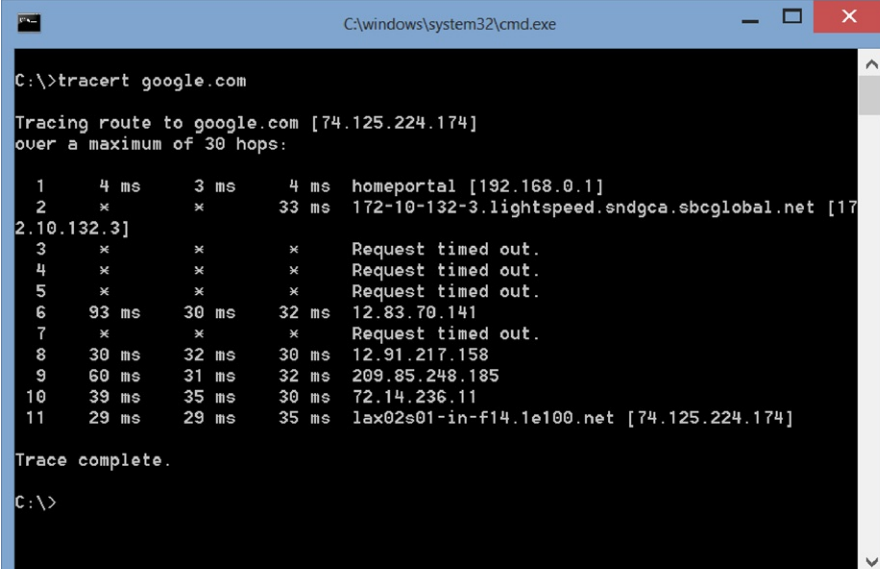
### ***Intercepting traffic directly on your machine***

The easiest way for someone to track the specific webpages that a specific person is looking at online is to install software on the user's computer that tracks the URLs and to capture a full copy of the webpages that the user is looking at. The biggest reason that this is the best solution for tracking a user's online activity is because many websites on the Internet require a secure connection between the user's computer and the web server. This secure connection means that the web server encrypts the network traffic before it is sent to the user's computer, and if it is intercepted before being relayed to the end user, the certificate will not match correctly and the user's web browser will inform them that the certificate does not match the web server correctly.

Like capturing e-mail on a user's computer, there are a wide variety of software packages that are available to capture web browser traffic. Some of these are legitimate software packages that can be used by parents to monitor what websites children are visiting and who they are talking with in forums and on Facebook, etc.

### *Intercepting traffic on the Internet*

Capturing people's network traffic as it is transferred between the web server and the user's computer is quite a complex task. The reason that this task is so complex is because of the massive amount of data that are transferred across the Internet at any given time and the fact that capturing a user's specific network traffic requires capturing that network traffic on one of the routers between the web server and the user's computer. These routers are very secure and managed by large Internet service providers who specialize in managing these routers. Each website that is accessed by a user has a different set of routers between the user and the website. We can see the list of routers or at least some of them by using the "tracert" command on Windows computers or the "traceroute" command on Linux and Mac OS X computers. The output from the tracert command is shown in [Figure 6.3](#).



```

C:\windows\system32\cmd.exe

C:\>tracert google.com

Tracing route to google.com [74.125.224.174]
over a maximum of 30 hops:

  1    4 ms    3 ms    4 ms  homeportal [192.168.0.1]
  2    x      x      33 ms  172-10-132-3.lightspeed.sndgca.sbcglobal.net [172.10.132.3]
  3    x      x      x      Request timed out.
  4    x      x      x      Request timed out.
  5    x      x      x      Request timed out.
  6   93 ms   30 ms   32 ms  12.83.70.141
  7    x      x      x      Request timed out.
  8   30 ms   32 ms   30 ms  12.91.217.158
  9   60 ms   31 ms   32 ms  209.85.248.185
 10   39 ms   35 ms   30 ms  72.14.236.11
 11   29 ms   29 ms   35 ms  lax02s01-in-f14.1e100.net [74.125.224.174]

Trace complete.

C:\>

```

**FIGURE 6.3**

Output from the tracert command.

Some of the routers between the user and the [google.com](http://google.com) website are configured to not show themselves. This is why those servers report back a “Request timed out” instead of responding with their name and IP address.

In order to capture the most network traffic possible that was being transmitted to the user’s computer, monitoring closer to the user would need to happen. In this case of this sample user shown in [Figure 6.3](#), this would mean capturing the data from the router in the [sbcglobal.net](http://sbcglobal.net) datacenter (which is also known as AT&T). Assuming that these data could be captured by someone, much of these data would be encrypted. Websites such as banking websites, shopping websites, and even many social networking websites all secure the data using Secure Socket Layer (SSL) encryption. This means that the data that are captured from the network would be encrypted and unreadable by the person that captured it, unless they were able to break through the encryption that was used.

---

## HOW CAN A GOVERNMENT WATCH WHAT I DO?

Governments are the biggest threat when it comes to monitoring data on the Internet as a whole. This is because they have massive resources available that they can call upon either by normal monitoring means like monitoring data via network routers as discussed earlier, by inserting rouge code into the operating systems of routers, or by having companies insert backdoors into data encryption code through threats or legal mandate.

The chances of a government putting rouge monitoring code into network routers are a minimal risk. The companies that run the public Internet are very careful when it comes to where they purchase their routers and other networking equipment from. Because the supply chain is ensured, with these companies typically purchasing their equipment directly from the companies that build the hardware, there is very little risk of the equipment being compromised.

In late 2006, the companies that run the public Internet were found to be capturing all of the Internet traffic that passes through their networks for the US government. The most well-known example of this was AT&T’s monitoring of their Internet traffic via room 641A in their facility at 611 Folsom Street in San Francisco, CA, which was at the time owned by SBC and rented to AT&T. The existence of this room within this facility and its use were revealed by an AT&T employee and were the subject of a 2006 class action lawsuit against AT&T. Rumors of other rooms such as this one at other facilities exist, but the existence of other capture rooms like this has not been confirmed. Even though a lawsuit was filed, no information about room 641A or the other rooms like it that may exist was ever brought to light. This is because during the course of the legal proceedings between the Electronic Frontier Foundation (EFF) and AT&T, the US Congress granted the Internet service providers that were

involved in this wiretapping program retroactive immunity from for their involvement. More details can be read about this room and the resulting law suits at [http://basicsofdigitalprivacy.com/go/room\\_614a](http://basicsofdigitalprivacy.com/go/room_614a).

The data encryption that is used to secure basically everything important that we do on the Internet was not designed by any specific government or government agency. Because the data encryption wasn't designed or built by any specific government or their agencies, they were not able to directly insert any backdoors into the data encryption process. However, it appears as of the writing of this book in the summer of 2013 that the National Security Agency (NSA) has been able to get some the technology companies that have built a lot of the data encryption that is in use today to install some sort of backdoor into their data encryption technologies.

There are several excellent articles on the Internet. Two of the most accessible that include links to several other articles can be found at <http://basicsofdigitalprivacy/go/nsa1> and <http://basicsofdigitalprivacy/go/nsa2>.

## **SSL versus the NSA**

The NSA has been working hard to break the encryption called SSL, which is used to secure all encrypted Internet traffic. The reason that they want to break the protection that is provided by SSL is so that they can monitor and track those who wish to attack the United States. The side effect of their attempts to break SSL encryption is that they would be able to record and view the web browsing of American citizens, which, as of the writing of this book, is questionably legal at best. By breaking the SSL encryption, not only online shopping but also the secure virtual private networks, which are used to encrypt corporate communications between company offices and for remote workers, are compromised.

According to reports available in the summer of 2013, the NSA has devoted large amounts of money and computing power to the task of breaking SSL encryption algorithms. This is being done by the NSA by building very large and powerful supercomputers which they use to attempt to break the encryption on the data which has been encrypted via the SSL specification.

Through various methods, the NSA has built up a huge collection of encrypted data. Through documents that were released in the summer of 2013, some of which can be read at <http://basicsofdigitalprivacy.com/go/nsa3>, it has been exposed that starting in 2010, the NSA made breakthroughs in breaking the SSL encryption, allowing them to access "vast amounts" of data that have been collected over the years.

According to documents that have been released around the summer of 2013, the NSA does have some policy data collection. According to these policies, available for viewing at <http://basicsofdigitalprivacy.com/go/nsa5>, data collected on US citizens can only be kept for up to 5 years or until such time that the communication is found to be not relevant to the original basis of the data collection. This policy

however only applies to unencrypted information. Data, which are encrypted, that the NSA has collected can be kept indefinitely until the time that it can be decrypted and analyzed. Depending on how well the NSA has done with breaking the entire SSL encryption standard, this means that encrypted data could be kept on servers operated by the NSA for years or decades.

---

## NOTE

### Five years from when?

In the prior paragraph, I state that the data that are captured can only be retained for 5 years, but I don't specifically say when that 5-year clock starts. The reason that I'm specifically vague here is because the law doesn't specifically say when that 5-year clock starts either. The assumption is that it is 5 years from the time that the data are collected, but that is just an assumption.

---

---

## HOW CAN I STOP PEOPLE FROM WATCHING WHAT I DO?

Now that you've read about how easy it is for others to monitor your online activities, your next question should be how to prevent people from monitoring Internet activities.

---

## NOTE

### This is scary stuff

If reading this section of this chapter and the various articles that have been referenced (<http://basicsofdataprivacy.com/go/nsa1>, <http://basicsofdataprivacy.com/go/nsa2>, <http://basicsofdataprivacy.com/go/nsa3>, <http://basicsofdataprivacy.com/go/nsa4>, and <http://basicsofdataprivacy.com/go/nsa5>) hasn't scared you away from posting sensitive information that you don't want others to see online, it should have. Assuming that everything that has been posted about the NSA's ability to break the SSL encryption is true, it means that either there are backdoors in the encryption protocols or, with enough CPU power, the encryption can be broken.

If there is a backdoor in the SSL encryption that the NSA is able to use to get through the SSL encryption, then it stands to reason that someone else will be able to make use of that backdoor at some point in the future. If the NSA was able to brute force their way through the SSL encryption protocols, then that means that they are breakable and that someone else can break through them as well; it's just a matter of time.

---

## E-mail

Preventing people from viewing e-mails that you are sending requires a two-phase approach. The first is to properly secure your computer as discussed in [Chapter 4](#) and your home computer network as discussed in [Chapter 3](#). This is your best chance of making sure that no one is able to install anything on your computer that can capture your e-mails. When it comes to the people who receives the e-mails that you send or the people that e-mail you, there's nothing you can do about their computers.



**NOTE****Helping others secure their computers**

It's time for a quick sales pitch here, which I feel really bad about putting in here, but the nice thing about being the person who writes the book is that you get to decide what goes into the book.

If you've found the information in this book useful when it comes to securing your computers and helping you to protect your personal privacy, which I hope that it has (if it hasn't, please go to <http://basicsofdigitalsecurity.com/go/feedback> and let me know), please let the people that you send sensitive data to know about the book so that they can secure their computers in order to protect themselves and to help protect you as well.

As for preventing people from intercepting e-mails in transit, this is something that we can do something about quite easily. When possible, we want to be sure that we are using secure encrypted communications to communicate between the e-mail application and the e-mail server. When using mail services like Gmail or Yahoo! Mail and accessing the e-mail's webmail application, the connection is going to be secured by default using the SSL protocol. If you are using a third-party e-mail client such as Outlook and Eudora, the use of the SSL protocol is required when sending and receiving e-mail. The instructions for setting up e-mail clients securely are fully documented on the Internet and can be found at [http://basicsofdigitalprivacy.com/go/yahoo\\_mail](http://basicsofdigitalprivacy.com/go/yahoo_mail) for the Yahoo! Mail instructions and at <http://basicsofdigitalprivacy.com/go/gmail> for Google's Gmail service. For other services, you'll need to check with the technical support department of your e-mail service.

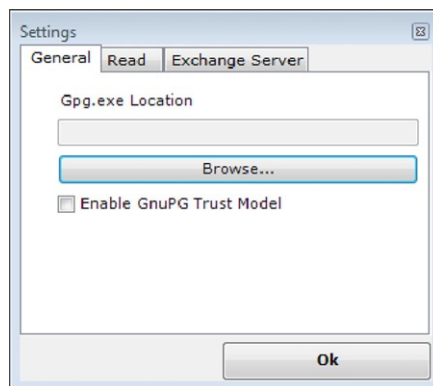
Securing the communication between the e-mail client and the e-mail server is only half of the work. We still need to ensure that the e-mails are encrypted as they travel from server to server over the Internet. This is done with an encryption process called Pretty Good Privacy (PGP). Using PGP in order to secure your e-mails requires both doing some prep work on your computer and giving people that you will be e-mailing some information so that they can read your e-mails.

The first step in setting up PGP is to ensure that your e-mail client supports PGP. In order to do this, you'll need to check with the manual that comes with your e-mail software or contact their technical support department.

***Setting up PGP on Microsoft's Outlook 2013***

The first step to getting PGP setup and configured in Microsoft's Outlook 2013 e-mail client is going to be to install some additional software on your computer. You'll need to download and install two specific pieces of software. The first is the Outlook Privacy Plugin that can be found at <http://basicsofdigitalprivacy.com/go/outlook1> and a piece of software called Gpg4win that can be found at <http://basicsofdigitalprivacy.com/go/outlook2>. Make sure that Outlook is closed when installing these two applications.

After installing the Outlook Privacy Plugin and Gpg4win open Outlook, you should then be prompted with a dialog box that asks you to locate the `gpg.exe`

**FIGURE 6.4**

GPG location dialog.

application that should be similar to [Figure 6.4](#). By default, the GPG application will be located in C:\Program Files\GNU\GnuPG\pub.

---

## NOTE

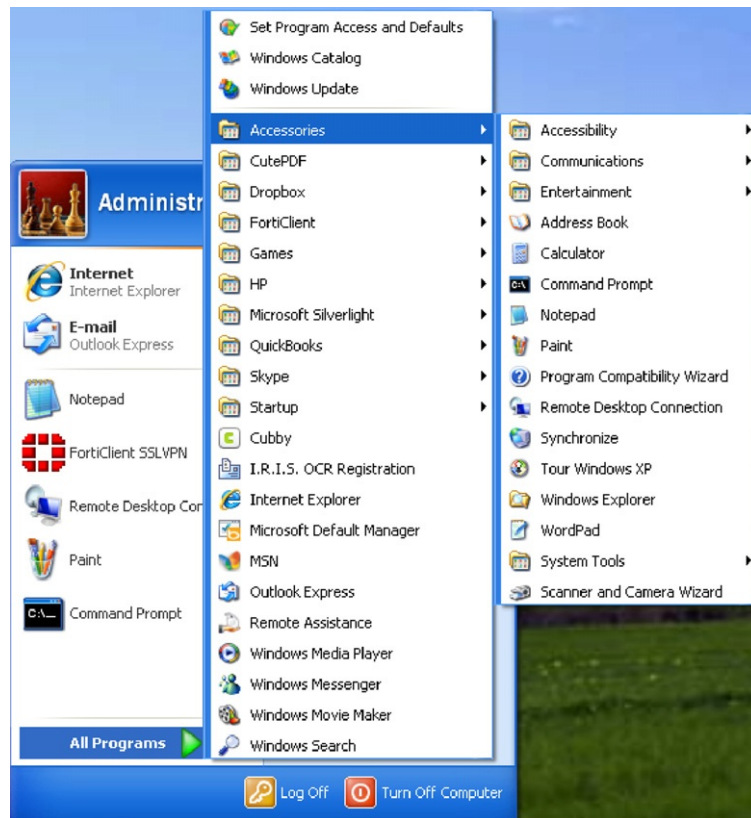
### Windows 8.1 support

As of the writing of this book in the summer of 2013, the Outlook Privacy Plugin does not work correctly on Windows 8.1. While this will change at some future date, there is no way of knowing if this support will change between the writing of this book and the printing of this book, much less your reading of this book.

As this section of the book was written just days after Windows 8.1 was officially released, not all software available on the market has been updated to support Windows 8.1, so some things aren't working just yet, and this is one of those things. As the Outlook Privacy Plugin is an open-source community-built project, it will be updated in the near future to support Windows 8.1. Until then, either another plug-in to support PGP e-mail encryption would be needed to encrypt e-mails in Outlook 2013 on Windows 8.1 or you'll have to wait for this plug-in to be upgraded. As of the writing of this book, the newest version of the Outlook Privacy Plugin is Beta 34. If there is a newer version available for download from <http://basicsofdigitalprivacy.com/go/outlook1>, this may have the support for Windows 8.1 that you need.

---

The next step in the process is to include a public and private key pair. These public and private keys are what are used to secure the e-mails. The private key is used by the sender to encrypt the e-mail, while the public key is used by the receiver to decrypt the e-mails. Generating these keys requires that a command line application be used to create these keys. This is done with the GPG application. To do this in Windows XP and Windows 7, click on the Start menu, select "All Programs," and then select Accessories. If using Windows XP, select the "Command Prompt" option as shown in [Figure 6.5](#). If using Windows 7, right click on the "Command Prompt" option and select "Run as administrator" as shown in [Figure 6.6](#).

**FIGURE 6.5**

Windows XP Start menu.

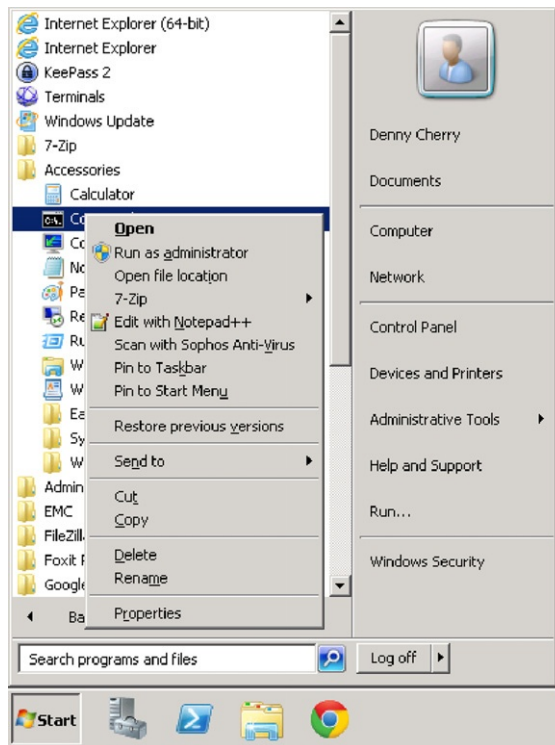
If using Windows 8, bring up the Start menu by placing your mouse cursor in the lower right-hand corner until the Start menu button appears as shown in [Figure 6.7](#) then click on the Start button.

If using Windows 8.1, click on the Start button usually located in the lower right-hand corner of the screen, shown in [Figure 6.8](#).

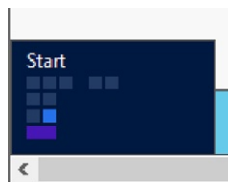
When using Windows 8 or Windows 8.1, the Start menu will have now appeared. At this point, simply type “cmd” and the Command Prompt icon will be shown on the screen that will be similar to [Figure 6.9](#).

With the Command Prompt icon from [Figure 6.9](#) visible, right click on the Command Prompt icon and then select the “Run as administrator” option from the menu that appears at the bottom of the screen as shown in [Figure 6.10](#).

From here, the instructions for Windows XP, Windows 7, Windows 8, and Windows 8.1 are the same.

**FIGURE 6.6**

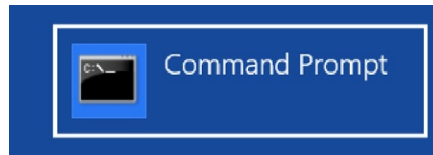
Windows 7 Start menu.

**FIGURE 6.7**

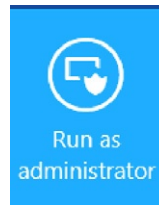
Windows 8 Start button.

**FIGURE 6.8**

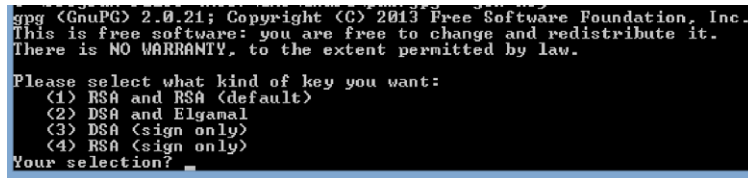
Windows 8.1 Start button.

**FIGURE 6.9**

Windows 8 and 8.1 Command Prompt icon.

**FIGURE 6.10**

Windows 8 and Windows 8.1 "Run as administrator" menu option.

**FIGURE 6.11**

Menu shown by the GPG application.

Within the command line window that has opened change to the directory that has the GPG application. This is done with the CD command as shown in Example 6.1 and pressing the Enter key.

```
cd "c:\program files\gnu\GnuPG\pub"
```

Example 6.1: Changing the directory to the GPG folder

After changing into the correct directory, run the gpg command and specify the –gen-key command as shown in Example 6.2. Note that there are two dash marks in front of the gen-key switch.

```
gpg --gen-key
```

Example 6.2: Command to generate new public and private key

A menu will now appear that gives four different options as shown in [Figure 6.11](#). Option 1 allows you to create RSA keys, which is the recommended option. Select this option by pressing the number 1 and pressing the enter key.

The next step is to enter the key size that you would like to use. The default is a key size of 2048 bits. The higher the number that is used for the key length, the harder it will be for someone to break through the encryption. The trade-off between high levels of encryption is that they require high amounts of CPU power to encrypt and decrypt the data. For maximum protection, a key length of 4096 bits is recommended.

The next step asks how long the key should be valid for. The default is for the key to never expire that requires an input value of 0. To specify expiration of the key in a number of days, enter a number. To specify the key expiration in a number of weeks, enter a number with a “w” after it. To specify the key expiration based on months, enter a number with an “m” after it. To specify the key expiration based on years, enter a number with a “y” after it. If the key is set to expire, that means that e-mails won’t be readable after the key expires. This means that as the key is preparing to expire, a new key would need to be generated so that e-mails could continue to be secured. Each time a new key is created, the people who receive e-mails will need to receive a new copy of the public key.

At this point, in the process, you will be prompted to enter your name and e-mail address. This key will be used with and any comment that you wish to specify. After entering this information and confirming that it is correct, you’ll be prompted to enter a new password for the key twice, and then the key will be generated. As it prompts you on the screen, you’ll want to type on the keyboard and/or move the mouse around randomly in order to help randomize the information that is used to create the key.

Next, we need to export the public key so that we can give it to the people that we will be e-mailing encrypted e-mails to. This is done in the command window again using the gpg program as shown in Example 6.3, replacing the example e-mail address with the e-mail address specified when creating the key.

```
Gpg -export -a "mrdenny@dcac.co" > public.asc
```

**Example 6.3:** Code to export your public key

Within Outlook, you’ll need to tell the Outlook Privacy Plugin to use the key. This is done within Outlook by clicking on the Add-Ins tab and then clicking Settings. This will open a new window from which on the “Compose” tab, you’ll need to select the PGP key that should be used when sending e-mail.

### ***Sending encrypted e-mails***

E-mails are not sent as encrypted e-mails by default within Outlook. You have to specifically tell Outlook that you want the e-mail to be signed and encrypted. To do this within the compose e-mail window, select the Sign and Encrypt options within the OpenPGP section of the ribbon at the top of the window as shown in [Figure 6.12](#). Once these options are selected, the e-mail will be encrypted when it is sent, which means that the person receiving the e-mail will need your public key in order to open the e-mail.

---

## **NOTE**

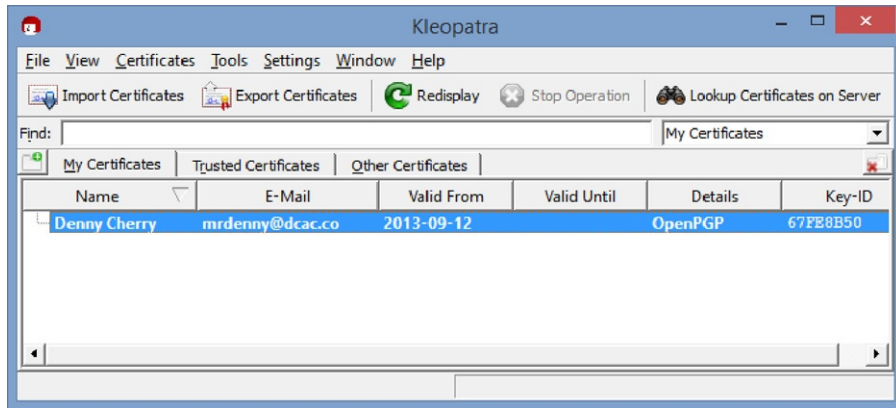
### **Supported e-mail types**

As of Outlook 2013, only plain text e-mails are supported for encryption and signing. This means that no graphics, fonts, or colors can be specified within the e-mail body.

---

**FIGURE 6.12**

OpenPGP menu options from the Outlook ribbon.

**FIGURE 6.13**

Kleopatra main screen.

### ***Importing a public key from another person***

The preferred method of giving out the keys is to give the key to someone on a thumb drive or another secure transfer method. Some people will e-mail out the key, but this means that anyone to intercept the e-mail with the public key would then be able to decrypt the e-mails that are later sent.

Anyone who is receiving your e-mails will need to import your public key into their computer. Gpg4win includes an application called Kleopatra, which will allow them to import this public key. To find Kleopatra, they will need to first install Gpg4win, which they will need in order to send secure e-mails, as well as any plug-ins, which are required for their e-mail client. After Gpg4win is installed, Kleopatra can be found in Windows XP and Windows 7 by clicking on the Start menu then All Programs, then selecting the Gpg4win program group, and then selecting Kleopatra. In Windows 8 and Windows 8.1, click the Start menu and type in Kleopatra to locate the application. To import a public key, simply click on the “Import Certificates” button in the upper left-hand corner of the application as shown in [Figure 6.13](#).

When you send someone an e-mail, which is encrypted and they have your public key imported into their system, the e-mail will be shown just like it normally would be. If the person receiving the e-mail does not have your public key imported into their system, then the e-mail either will not show or it will show as scrambled text that is totally unreadable. The same applies when someone e-mails you an e-mail that is encrypted with this private key.

---

## NOTE

### Why aren't instructions for my e-mail client shown here?

There are dozens if not hundreds of e-mail clients out there, some more popular than others. For simplicity sake, I've opted to show the steps for setting up Outlook 2013 (which should basically be the same as for Outlook 2010). These steps should be fairly close to some of the other e-mail providers out there. If they aren't, a search on the Internet for "{*My Email Application*} PGP Setup" where {*My Email Application*} is the name of your e-mail client should find you the specific instructions for your e-mail application. If you can't find the specific instructions online, contact the technical support department or ask for assistance online at one of the technical forums such as <http://superuser.com>.

---

## Web browsing

One of the ways that web browsing traffic is tied to a specific person or more specifically to an account with an Internet service provider is by tracking the data from an IP address.

---

## NOTE

### What is an IP address?

Much of this section is going to resolve specially around IP addresses, so a little background on what IP addresses are and how they work should be useful here.

Every device on the public Internet has a public IP address that allows computers on the Internet to talk to each other. IP addresses come in two versions that are used on the public Internet, version 4 and version 6. Version 4 IP addresses (IPv4) are made up of four numbers with each number between 0 and 255 with a period between each number, for example, 213.17.28.19. Version 6 IP addresses (IPv6) are made up of five groups of characters with four characters in each group and a semicolon between each one, for example, fe80:ad17:6915:8438:c088. IPv4 has been in use since the Internet was first used by the public, while IPv6 has first been introduced in the late 2000s. IPv6 has gotten very little traction with Internet service providers or with customers due mostly to the huge amounts of money that Internet service providers will need to pay to upgrade older hardware so that it can support the new IPv6 standard.

The original concept of an IP address is that it uniquely defines a computer on the network, with the Internet simply being the largest network of computers in the world. However, because of the massive number of devices on the Internet, IP addresses are not tied to any one specific computer. A networking protocol called Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to end users' systems such as your broadband router if you have a high-speed Internet connection or to your computer directly if you have dial-up Internet access. DHCP is used so that you are connected, but when you disconnect from the Internet,

*Continued*



by tuning off your router if you have a high-speed connection or by disconnecting the dial-up connection if you have dial-up Internet access, the IP address can then be used by another user. This allows the Internet service provider to have higher utilization numbers for their IP addresses as getting IP addresses from the international association that assigns IP addresses to Internet service providers requires that Internet service providers have 90% of their IP addresses in use before they can request more IP addresses.

Typically, each home Internet connection has a single IP address assigned to it, with each computer on that home network sharing the single public IP address as discussed in [Chapter 3](#). This is how companies and/or government agencies are able to tie a specific IP address to a specific person.

One of the ways that we can prevent people from watching what you do on the Internet is to mask the IP address that your network traffic is actually coming from. There are two basic ways of doing this. The first is by using an anonymizer, which makes your network traffic appear to come from a variety of different places throughout the world. A very well-known anonymizer is called Anonymouse and is available from <http://anonymouse.org/>. By using Anonymouse or one of the other anonymizer services, you simply type in the URL that you wish to browse to, and your web browsing connection is routed through the Anonymouse servers.

The Anonymouse website shows specifically what information they are masking when you use their service. When browsing from an example computer, the information returned by the Anonymouse server is shown in [Figure 6.14](#).

The information shown in [Figure 6.14](#) provides a surprising amount of information when you know how to read it. The IP address is a pretty straightforward piece of information as that is the IP address of the router that the sample computer was connected to. The second line, which is labeled as the host, provides us with some location-based information and tells us who the Internet service provider is. In this case, the Internet service provider is [sbcglobal.net](http://sbcglobal.net), which is one of the domain names that belongs to AT&T. The second thing that we can see is some basic information about where the IP address is used. The part of the hostname, which says `sndgca`, is a telecommunication industry abbreviation for San Diego, CA. Looking at the third line, which is labeled “Browser & OS,” this gives us a good deal of information about the computer and the web browser that is being used. The web browser that is being used is a Mozilla 5.0 compatible web browser. Specifically, the web browser is MSIE 10.0 or Microsoft Internet Explorer 10.0. The operating system is Windows NT 6.2 or Windows 8. WOW64 tells us that this is a 64-bit operating system running a 32-bit web browser. The “Touch” tells us that this is a touch enabled computer.

<b>IP</b>	172.10.132.29
<b>Host</b>	172-10-132-29.lightspeed.sndgca.sbcglobal.net
<b>Browser &amp; OS</b>	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; Touch)

**FIGURE 6.14**

Information reported to websites from a sample computer when not using an anonymizer service.

The hostname, which is assigned to the IP address, is not something that can be controlled by the end user whose computer the IP address is assigned to. This is assigned by the company that owns the IP address and is configured by them.


When using the Anonymouse service, this information is changed quite a lot as shown in Figure 6.15.

The biggest downside to using the Anonymouse service or really any of the other anonymizer services is the fact that you have to go to the anonymizer’s webpage for each new webpage that you want to browse to. For example, instead of being able to go directly to this books website [www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com), you instead have to first browse to [www.anonymouse.com](http://www.anonymouse.com) and then you put the URL [www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com) into the text box on the Anonymouse website, as shown in Figure 6.16. Realistically, this isn’t that big of a problem if the goal is to only

IP	193.200.150.137
Host	anonymouse.org
Browser & OS	http://Anonymouse.org/ (Unix)

FIGURE 6.15

Information reported to websites from a sample computer when using the Anonymouse service.



AnonWWW

AnonEmail

AnonWWW

AnonNews

Many **mice** surf the web under the illusion that their actions are **private and anonymous**. Unfortunately, this is not the way it is. Every time you visit a site **for a piece of cheese**, you leave a **calling card** that reveals where you are coming from, what kind of computer you use, and other details. And many **cats** keep logs of all your visits, **so that they can catch you!** This service allows you to surf the web without revealing **any** personal information.

**It is fast, it is easy, and it is free!**

Enter website address:

http://www.basicsofdigitalprivacy.com x

Surf anonymously

for example: "http://www.yahoo.com"

Your Calling Card **without** Anonymouse

Your Calling Card **with** Anonymouse

FIGURE 6.16

The Anonymouse website prepared to browse anonymously to [www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com).

browse to some websites anonymously. If however every website that you browse to should be done anonymously, this isn't the easiest solution to use; this however is where VPN solutions come into play.

There are a number of VPN solutions that can be used to give yourself a measure of privacy so that websites that you are visiting have no way of knowing your actual home IP address. Where an anonymizer will mask your IP address, hostname as well as the browser and operating system a VPN provider will only mask the IP address and hostname.

VPN services give you a couple of additional perks beyond just changing the IP address that your web browser traffic appears to come from. Depending on the service that you use, this could also change the country that it appears that your web traffic is coming from. This includes not just normal web browsing traffic but also e-mail traffic, online video streaming traffic, and anything else that is done on the Internet.

---

## NOTE

### **Some services work differently depending on what country you are in**

There are many services out on the Internet that work differently depending on what country you are in. Some example of this, including BBC's iViewer, which allows you to watch TV shows on the BBC website, only works in the United Kingdom. Another example is Netflix that has very different content catalogs available depending on what country you are located in, depending on the agreements that Netflix has with the content publishers. Other services that are used when connected to via a VPN connection may not respond as expected and may require a different VPN connection or that the VPN isn't used at all.

---

There are VPN services that are free to use and there are other services that are pay services. Some of the free services include both free and paid services that give you the ability to try the service for free before paying for the higher-end service. In order to keep costs down, many of these services limit the amount of data that you can transfer on a daily or monthly basis. Upon reaching the data transfer limits, these services simply disconnect you from the service until the next month.

How each of these VPN services works depends on the specific service. Some are configured much like a normal corporate VPN connection, while others use a browser plug-in.

The list of available VPN services changes often. As of the writing of this book, some of the VPN services include GPass, which is at <http://www.gpass1.com/gpass>, which provides free VPN services. Another option is CyberGhost, which is at <http://cyberghostvpn.com/>. CyberGhost provides a free service that allows for up to two hours of Internet traffic at once before forcing you to disconnect and reconnect. Additionally, CyberGhost offers paid-for services, which include more servers to route the connection through and does not have any limits on how long you can stay connected for. Another free VPN service is called SecurityKISS, which is available at <http://www.securitykiss.com>. SecurityKISS offers both free and paid-for services. The free service allows for 300 MB of data transfer per day, while the paid-for services include data transfer from 20 GB up to an unlimited amount of data transfer.

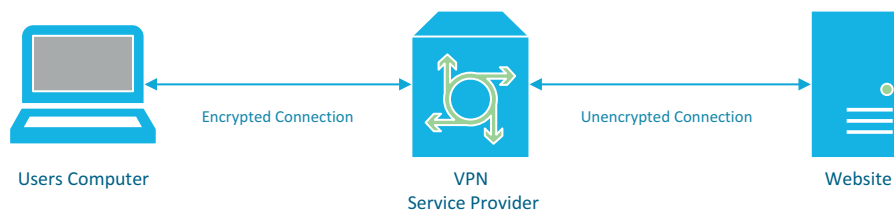
**FIGURE 6.17**

Diagram of encrypted and unencrypted connections.

When using these VPN connections to hide or mask your network traffic, keep in mind that the network traffic isn't going to be completely invisible. Only the network traffic between your computer and the VPN provider isn't going to be easily visible to anyone who is looking for it. However, any network traffic that isn't otherwise encrypted would be visible to someone who is watching for the traffic that is coming from the VPN service provider to the web server that is being viewed as shown in Figure 6.17.

Another option available to you is to use a system called Tor. When the Tor protocol was first written, it was designed and deployed as what is called an onion routing project for the US Naval Research Laboratory. However, the project was released to the public and is used today by large numbers of people to communicate securely over the Internet.

According to the Tor website (<http://basicsofdigitalprivacy.com/go/tor>), "Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy."

Tor works by bouncing a person's web traffic requests through a variety of servers called nodes. Each node between the client computer and the server only knows about the prior machine in the chain, and the next machine in the chain, meaning that no single machine in the chain, including the person's computer and the server at the end of the chain, has no way to know the entire chain process.

There are a variety of applications that can be configured to use Tor, but not all applications can. While the Tor website does not contain a complete list of applications that can be used with Tor, it does have a variety of settings and instructions for popular applications so that you can use many applications over the Tor network.

## Consequences

There are a few consequences when it comes to using an anonymizer service or a VPN solution to mask your actual IP address. The first of these consequences is the ease of use, and the second consequence is increased government scrutiny from various government agencies.

***Ease of use***

Anytime we add security, we add complexity to the process. In the case of browsing the web using an anonymizer service, we add to complexity of needing to ensure that each new website that we browse to is done via the anonymizer. In some cases, depending on what web browser you are using, there may be plug-ins to help ensure that this is happening. You would need to check with the specific anonymizer, usually in their Frequently Asked Questions or their forum to see what assistance they can provide with regard to getting a plug-in. Typically, these sorts of plug-ins are available for Firefox and/or Chrome web browsers.

---

**NOTE****Security usually isn't easy**

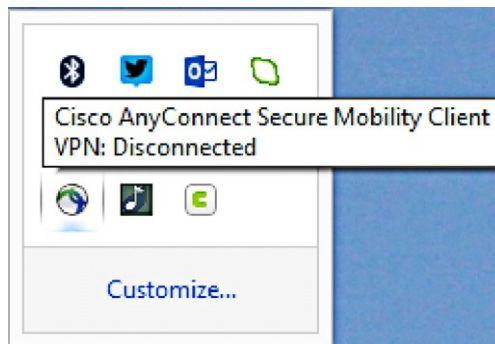
There's an old adage when it comes to security. If it's easy, it probably isn't secure. The same applies here as well. The more we want to ensure that our data are kept private, the more work we have to do to do that.

---

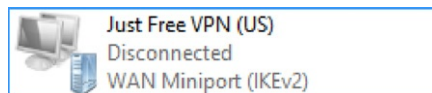
Using a VPN connection to ensure that our data are secure while being a little easier to deal with than simply an anonymizer, there are still things that you need to do to ensure that your connection is secure. The first thing that you need to do is make sure that your VPN is connected before opening any applications that are Internet-connected. In the world of applications that check in automatically with the companies that developed them when the computer boots up, this can be quite hard to do to say the least. Depending on the type of VPN connection software that is being used, it may or may not be possible to have the VPN connect before logging into the computer so that by the time that you are logged into the computer and your desktop is visible, the VPN connection has already connected and is routing all of the network traffic across the encrypted connection.

VPN connections can sometimes drop and need to be reconnected. When using a VPN connection to encrypt all network traffic between you and the Internet to ensure that someone isn't monitoring your network connection, you will need to keep an eye on the status of the network connection to ensure that you are always connected. How you do this will depend on the VPN connection software that you are using. The Cisco AnyConnect VPN software, for example, shown in a disconnected state in [Figure 6.18](#), sits in the system tray and doesn't provide much of an interface to tell you that it has become disconnected. As the state of the VPN connection changes, there is a small pop-up that appears, but it disappears rather quickly, and if you happened to not be looking at the screen when the connection dropped, then you might not notice that you were in a disconnected state.

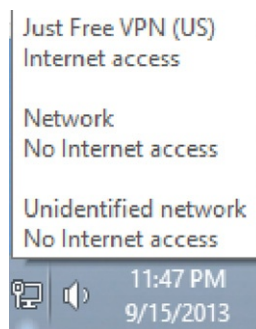
The Windows VPN connection can be checked in a couple of different ways. The first is within the "Network Connections" icon with the control panel. If the connection is disconnected, it will be labeled as such, as shown in [Figure 6.19](#).

**FIGURE 6.18**

Cisco AnyConnect VPN software in a disconnected state.

**FIGURE 6.19**

Windows VPN connection in a disconnected state.

**FIGURE 6.20**

Windows Network Status dialog.

Another way to verify if the Windows VPN is connected is to simply place your mouse over the network connection icon in the system tray next to the clock. When you place your mouse over the icon, shown in the lower left of [Figure 6.20](#), the status of each network connection being used is shown. In this case, the computer has two different networks configured and the VPN connection that is connected. Upon the VPN being disconnected, the VPN would no longer be visible in the dialog box.

These VPN connections are just a couple of the wide variety of VPN software packages that are available. Check with your VPN provider or the VPN software vendor for specific details if a different VPN software package is being used.

### ***Government scrutiny***

Using data encryption techniques such as those shown in this chapter can have some unintended consequences when it comes to government scrutiny. When it comes to programs like the PRISM program within the United States, the specifics of which were leaked to the press and can be read at <http://basicsofdigitalprivacy.com/go/nsa4>, when you are a person who the government thinks is currently outside of the United States, the NSA, according to Section 1, paragraph 2, of Exhibit A ([http://basicsofdigitalprivacy.com/go/nsa\\_a](http://basicsofdigitalprivacy.com/go/nsa_a)), can collect your Internet usage information. With many of these services, the specific point is to make it appear like you are outside of the United States, so as far as the PRISM data collection is concerned, you are outside of the United States and therefore they can collect your data, even if you are inside the United States. To make things even worse for encrypting your data, if the NSA isn't able to figure out where you physically are, the assumption is that you are not within the United States.

Looking at Exhibit B ([http://basicsofdigitalprivacy.com/go/nsa\\_b](http://basicsofdigitalprivacy.com/go/nsa_b)), Section 5 talks specifically about domestic communications, or communications that the NSA knows to be within the United States. According to this section, "communications identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines in writing that" "the communication is reasonably believed to contain technical data base information" where technical database information is defined as "Technical data base means information retained for cryptanalytic, traffic analytic or signal exploitation purposes." What that means in a slightly easier to read version is that if the data are encrypted and the NSA hasn't broken the encryption when they realize that you are within the United States, the director of the NSA can order that the information be kept so that they can continue to attempt to break the encryption.

A little further down the document in Section 5(3)(a), we see that "In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in cryptanalysis." In other words, if they have captured encrypted data, they can keep these data forever and use it to continue to develop software that attempts to break the encryption.

When using systems like Tor to attempt to protect your network traffic from snooping by groups like the NSA, keep in mind that odds are this will be pushing your network traffic to a node in another country making your now encrypted traffic collectable by the NSA where they are able to keep your network traffic forever.

## SUMMARY

As we have seen in this chapter, there are ways of encrypting network traffic so that you can do the best possible job ensuring that the information that you send out over the Internet isn't visible by data thieves or by government agencies. However, when doing so, this may have the unintended consequence of closer government scrutiny because the government wants to know that you aren't talking about something that may be of interest to them, and because they don't technically know for sure where in the world you are at that moment, they make the assumption that it is OK for them to monitor you, potentially storing the captured information for as long as they would like.

There are a variety of ways to encrypt data as it flows over the Internet including PGP, VPN connections, and Tor, among others, which were not discussed here. Each one of these methods has upsides and downsides to them, and the goal when reviewing the various options is to find a solution that works for you, the user of the computer. You want a solution that will provide you with a level of data and privacy protection without being such a cumbersome solution that it isn't feasible for you to use on a daily basis.



# Laws and Internet Privacy

# 7

---

## INFORMATION IN THIS CHAPTER

- How much information you should share with companies?
- Risks of sharing too much information online
- Knowing how companies protect your information

This chapter talks about how the Internet and the various laws around the world apply.

---

## THE LAW AND CHANGING TECHNOLOGY

When it comes to technology, in general, the legal system (regardless of what country you are in) can't keep up. New services and technologies change at a much faster pace than the legal systems can keep up with. Often, they end up being laws that directly conflict with technology, or we could even end up with different laws, some allowing the new service or technology and others that prohibit it.

When it comes to data privacy and specific government regulations, there are often large gaps between when a specific technology becomes available and when laws come into effect regarding that technologies use. In the United States, for example, there are no laws that tell companies what they are allowed to do with personal information that they collect from customers online even though companies have been collecting information from customers on the Internet for over 10 years. There are a variety of laws that have to do with electronic communications such as the Electronic Communications Privacy Act of 1986 (ECPA, codified at 18 U.S.C. §§ 2510-2522) that you can read the text of at <http://basicsofdigitalprivacy.com/go/ecpa>. This law is one of the primary laws used to govern electronic communications, which includes Internet access, but it was written before what we consider to be the Internet of today was created.

## PRISM

In the spring of 2013, it was revealed that the US National Security Agency (NSA) Internet has a monitoring program called PRISM. With this system, the NSA is able to monitor a huge amount of information and much of that information can be stored forever. With the NSA's PRISM program, the basic goal was to gather Internet

communications data of anyone who isn't inside the United States in an attempt to figure out who is talking to terrorists so that they can use the information gleaned from this work to stop a future terrorist attack.

This means that the NSA has data collectors on the Internet backbones around the world. These Internet backbones are simply fiber optic cables, which run from data-center to datacenter moving everyone's Internet traffic around the world. These fiber optic cables in many countries do not belong to the government but instead to private companies. The NSA would have needed to get the companies who own these backbone lines to work with them to give them access to the data. For the countries that do regulate Internet access within their national borders and where the countries' government owns the Internet links, the NSA would need to have a deal in place with that government that would allow it to monitor all this Internet traffic. The question becomes why would another country's government want to provide the NSA access? There could be a variety of reasons, all of which one can assume would be classified by both governments, those we can assume that helping the NSA would carry some favor with the US government at some point. The assumption exists that a data sharing policy would be in place for the data that the NSA gets from that country as it is processed. An example of this can be found with the Dutch spy agency called AIVD, which can be read about more at <http://basicsofdigitalprivacy.com/go/aivd>, where, according to the article, which references a Dutch newspaper article, AIVD agents have access to data that have been captured and analyzed by PRISM within just 5 minutes or less of a request for the information.

The way the PRISM system works in some cases is that the system doesn't actually track information as it travels across the Internet backbone. Instead, the NSA demands that companies such as Google, Microsoft, and Verizon hand over the data that they need on a regular basis so that they can go through this information. One of the key reasons that the NSA likes gathering the data from these large companies is that even if the network traffic between servers is encrypted when that data is stored, it will be stored with headers in plain text so that the NSA can just read the headers. Even if the data were stored by these companies using some sort of data encryption, because these companies have the encryption keys, they are able to simply decrypt the data when handing it off to the NSA.

---

## **NOTE**

### **Corporate responses**

The companies listed may or may not actually be handing over information. According to statements that many companies have released while newspapers were doing research into the PRISM program, these companies do not, in many cases, simply hand over data to the NSA (unless the NSA has gotten really good about breaking into datacenters).

### **Facebook**

We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law.

**Google**

Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a backdoor for the government to access private user data.

**Apple**

We have never heard of PRISM. We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order.

**Microsoft**

We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it.

**Yahoo!**

Yahoo! takes users' privacy very seriously. We do not provide the government with direct access to our servers, systems, or network.

**Dropbox**

We've seen reports that Dropbox might be asked to participate in a government program called PRISM. We are not part of any such program and remain committed to protecting our users' privacy.

**Paltalk**

We have not heard of PRISM. Paltalk exercises extreme care to protect and secure users' data, only responding to court orders as required to by law. Paltalk does not provide any government agency with direct access to its servers.

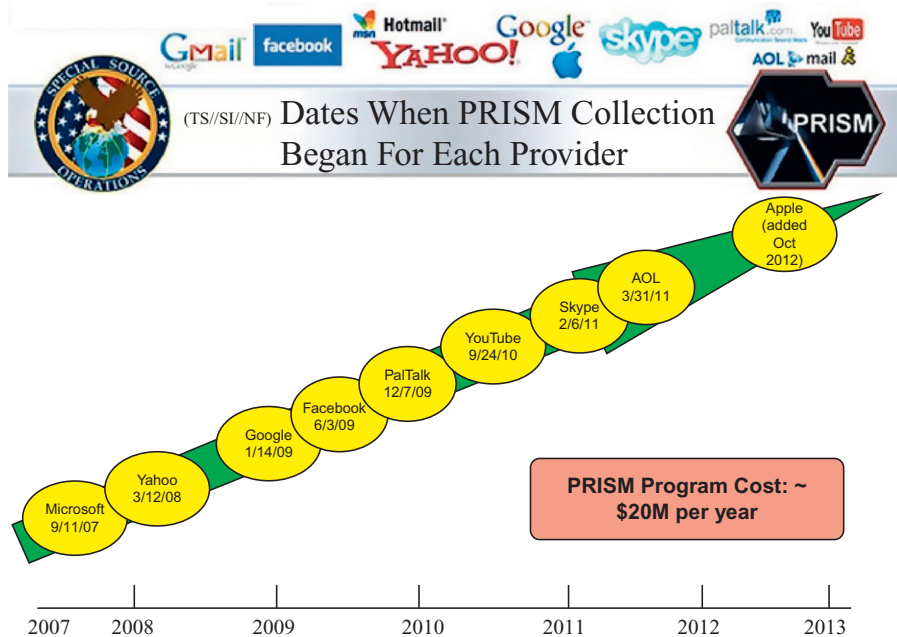
**AOL**

We do not have any knowledge of the Prism program. We do not disclose user information to government agencies without a court order, subpoena or formal legal process, nor do we provide any government agency with access to our servers.

The statements from these companies were given to TechCrunch, which it posted at <http://basicsofdigitalprivacy.com/go/techcrunch>. These specific companies release statements about the PRISM program because they are specifically named in the documents that were released about the PRISM program. Specifically, they are mentioned in a PowerPoint slide deck that was used to bring new NSA analysts up to speed on the program that can be found at the mentioned TechCrunch article and in [Figure 7.1](#).

Why then would companies outside of the United States want to get into bed with the NSA? There are a few possibilities:

1. The NSA is able to convince these companies that they have to follow US law because they may or may not be doing business with people within the United States.
2. The NSA is able to get the government of the other country to force the companies within their country to do what the NSA wants.
3. The NSA uses operatives from either the NSA or the CIA to force the companies to do what they want, probably without the company's knowledge.
4. Good old-fashioned threats.

**FIGURE 7.1**

Slide reported to be from a PowerPoint slide deck about PRISM.

No matter how it happens, the fact is that it is happening, and if you talk to people in other countries, those data are being captured somewhere and handed off to the NSA in some way.

### Canadian version of PRISM

According to the Toronto *Globe and Mail*, the United States isn't the only country where its citizens need to worry about the government tracking everyone that you talk to. In Canada, there is a program that sadly doesn't have a name as great as the US NSA program called PRISM (at least as far as we know as of the writing of this book in summer of 2013). This program, which you can read more about at <http://basicsofdigitalprivacy.com/go/Canada>, works in much the same way as the US program capturing what the mass media and press calls the metadata about the conversation. These metadata include things like who is talking to who online, when the conversation happened, and for how long, without tracking the actual conversation. When dealing with phone calls, the same sort of metadata are captured with the data being captured being the phone number who made the call, the phone number that was called, the date and time of the call, and the duration. It isn't a stretch to assume that GPS location is also included if the call is made to a cell phone as that information would be available to the cell phone company.

This program that is run by the Communications Security Establishment Canada was first approved by the elected government in 2005 by then Defense Minister Bill Graham. According to the *Globe and Mail* article, which you can read in full at <http://basicsofdigitalprivacy.com/go/globe>, this program was shut down for a period of time starting in 2008 and was restarted in 2011 when then Defense Minister Peter MacKay signed a new order allowing the program to be restarted and starting other classified espionage programs.

---

## IS ALL THIS LEGAL?

When it comes to monitoring programs like PRISM and the Canadian version that we don't know the name of or versions of this program run in other countries, a big question tends to be, how are these programs legal?

Well the frank answer is that they might not be, but that'll depend on who you ask and how you ask the question.

Focusing on the United States for a minute, as that's where I live so those are the laws that I know the best, the law is murky on this at best. Here in the United States, we have the constitutional right against self-incrimination. However, the courts have ruled recently that communications that are heard by a third person aren't private, and if that third person wants to tell the government about the conversation, they are allowed to. Along with that, the courts have ruled that the fact that a conversation itself between two people while being privileged, the fact that the conversation happened isn't privileged. This is how the NSA program that may catch communications of people within the United States gets through. All they are capturing is the fact that it happened and who it was with.

Let's compare an online situation with an off-line situation. In the off-line world, if two people are sitting in a park having a conversation, a government employee, most likely a city police officer, can make note of the people sitting next to each other talking without any legal issues. However, if he pulls out a long range microphone to listen in, odds are, he'll need a warrant. In the online world of voice over IP (VoIP) communications, the same rules apply. The government is able to get the status of the call from the VoIP provider without issue, but if they want the contents of the VoIP call, they will need a warrant before the VoIP provider is required to record the call for them.

At some point, I would imagine that the courts will rule on the issue of needing a warrant just to get the metadata of the call, but as of the summer of 2013, the issue hasn't been brought before any court that has been able to strike it down.

---

### NOTE

#### I'm not a lawyer

While reading through this section, keep in mind that I'm an IT professional, not a lawyer. My understanding of the law is by that of a layman, not a professional lawyer.

---

---

## IS ALL THIS MORAL?

The answer to this one is a lot easier than the “is this legal” question. The answer here, in my mind, is no, but please don’t take my word for it. Every person has to make this decision for themselves, and there really is no right or wrong answer here. A government that tracks the technology usage of everyone on the planet is really not at all moral. Could a system like this do what it’s supposed to do, which is to stop a terrorist attack? The answer there is possibly. But is it worth the invasion of people’s privacy that it takes to gather data at this level? The answer there is a personal answer, but my answer is no.

---

### NOTE

#### Everyone has their own opinion

In order for us to consider ourselves a civilized society, we have to draw a line in the sand of what we will and won’t do, with a good litmus test being would we want another to do this to us. For me, this line, or at least one version of it, would be that we don’t invade the personal liberties of people around the world just so that we can attempt to prevent a terrorist attack that may or may not be about to happen.

I have no problems with targeted tracking of people based on other evidence that has been gathered through boots on the ground style of spying at all, because, in my opinion, that’s how we gather useful, actionable intelligence.

I’ll do my best to make this the end of my personal rant, and I’ll leave my soapbox in the closet where it belongs.

---

## SUMMARY

As of the writing of this book in the summer of 2013, we don’t know much about these data collection systems. We have to make a lot of assumptions about them and how we should be protecting ourselves from gathering up data that we don’t want the government knowing about. There is a theory that if you have nothing to hide, you shouldn’t mind the government knowing what you are doing. However, your information is yours and you shouldn’t be forced to hand over the information without having the option to keep it to yourself. With much on this information, it is easy to control who gains access to it. If we don’t give up the information to a company, then we don’t have to worry about a government gaining access to that information. We make this decision by simply not using some services that are out there. When we use some of these services, we need to understand that information is being collected by these companies that we are using and that these companies can be handing this information over to government agencies.

With encryption systems like we learned about in [Chapter 6](#), we can do our best to prevent the government from viewing or tracking what we are doing online. However, this only works when these monitoring systems are capturing data during transmission, not when they are capturing data at the source or destination servers.

The worst part about these systems is that the information about them is often highly classified, which means that we won’t get to know anything about these systems until long after changes to the systems.

# Index

Note: Page numbers followed by *f* indicate figures.

## A

- Amazon Appstore, 74–76
- Android market, 74
- Anonymouse website, 114, 114*f*, 115–116, 115*f*
- Apple OSX
  - app store, 74
  - decryption key, 65
  - FileVault tab, 64, 66*f*
  - MAC address filtering, 51–52
  - password, 64
  - recovery key, 65
- Application programming interface (API), 98

## B

- BitLocker, 59, 62, 62*f*
- Brute-force method, 22
- BuzzFeed, 81–82

## C

- Cable News Network (CNN), 81–82
- Cookies
  - EULA, 8
- Firefox
  - exceptions page, 13–14, 13*f*
  - privacy settings, 11, 12*f*
  - third-party cookies, 12–13
- Google AdWords, 7–8
- Google Chrome, 14–15
- InPrivate Browsing, 8
- internet explorer
  - accept, reject/prompt, 9–10
  - advanced configuration, 9, 10*f*
  - Per Site Privacy Actions screen, 10, 11*f*
  - privacy settings, 8, 9*f*
- Safari, 15–17
- CyberGhost, 116

## D

- Data encryption
  - Apple OSX
    - decryption key, 65
    - FileVault tab, 64, 66*f*
    - password, 64
    - recovery key, 65
  - BitLocker, 59
  - gain access, 58–59
  - internet games/downloads

- application stores, 72
- cell phones, 74–76
- flash game, 71
- Mac, 73–74
- random websites, 71
- tablets, 74–76
- windows antivirus software, 72–73

- laptops, 57–58
- technical support, 69–71
- website security logos
  - McAfee logos, 68, 69*f*
  - Norton, 67, 67*f*, 68
  - online privacy, 68
  - requirements, 66–67
  - risks, 67
  - secure environment, 66
  - Symantec, 67–68
  - Troy's post, 67, 68*f*

## Windows

- BitLocker, 62, 62*f*
- C/D drive, 62
- control panel, 60, 60*f*, 61*f*
- disk space, 64
- password policy, 63
- recovery key window, 62–63, 63*f*
- recovery password, 63–64
- start button, 60, 60*f*
- Start Encryption button, 64, 65*f*
- system and security link, 60, 61*f*
- D-Link routers, 35, 36*f*, 40–42

## E

- E-mail
  - access, 99–100
  - antivirus software, 98
  - API, 98
  - network protocol, 98
  - network traffic, 98, 99*f*
  - prevention
    - encrypt options, 111
    - PGP setup, 106–111
    - public key, 112–113
    - SSL protocol, 106
  - sample e-mail headers, 100, 100*f*, 101
  - sender/receiver, 101
  - server encryption, 99
- End user license agreement (EULA), 8, 78–79, 79*f*

**F**

- Facebook, 3, 79–80, 79*f*
  - custom privacy option, 84, 84*f*, 85, 85*f*, 86*f*
  - drop-down menu, 83, 84*f*
  - post dialog, 83, 83*f*, 85, 86*f*
  - privacy settings
    - future posts, 87, 88*f*
    - limit past posts, 87*f*, 88
    - menu option, 86, 87*f*
    - picture security, 88
    - sample post, 88, 88*f*
    - settings icon, 85–86, 86*f*
    - tools, 87, 87*f*
  - screenshot, 84*f*, 85
- FileVault tab, 64, 66*f*
- Firefox
  - exceptions page, 13–14, 13*f*
  - privacy settings, 11, 12*f*
  - third-party cookies, 12–13
- Flickr
  - avatar, 89
  - EXIF data, 92, 92*f*
  - personal data privacy, 92
  - pop-up menu, 89
  - privacy and permissions tab, 90, 90*f*
  - profile setting, 92–93, 93*f*
  - settings option, 90–91, 90*f*, 91*f*
- Fob-based system, 27

**G**

- Google, 123–124
- Google AdWords, 7–8
- Google Chrome, 14–15
- Government scrutiny, 120
- Gpg4win, 112

**H**

- Health Information Patient Protection Act (HIPPA), 5
- Home network security
  - description, 33–34
  - network firewalls, 53–55
  - router
    - AT&T U-verse service, 35
    - cable internet services, 34, 34*f*
    - components, 35
    - D-Link firmware, 35, 36*f*
    - DSL services, 34, 34*f*
    - NAT, 35–37
    - NetGear router, 35, 37*f*
    - network firewalls, 37
  - Wi-Fi network

- AT&T U-Verse router, 38–39
- D-Link routers, 40–42
- friends, 52
- guest network, 52, 53*f*
- NetGear routers (*see* NetGear Wi-Fi routers)
- pocket network, 52
- WEP, 38
- WPA, 38

- Home Wi-Fi network security
  - AT&T U-Verse router, 38–39
  - D-Link routers, 40–42
  - friends, 52
  - guest network, 52, 53*f*
  - NetGear routers (*see* NetGear Wi-Fi routers)
  - pocket network, 52
  - WEP, 38
  - WPA, 38

**I**

- Information online
  - cookies/websites (*see* Cookies)
  - customer loyalty cards, 1–2
  - data protection policies, 5–6
  - Facebook, 3
  - product selling, 2
  - risks of sharing
    - attackers, 3–4
    - social networking sites, 4–5
  - target store, 1–2
  - zip code, 2
- InPrivate Browsing, 8
- Internet explorer
  - accept, reject/prompt, 9–10
  - advanced configuration, 9, 10*f*
  - Per Site Privacy Actions screen, 10, 11*f*
  - privacy settings, 8, 9*f*

**K**

- KeePass
  - Add Entry screen, 24, 25*f*
  - creation, 23–24
  - home screen, 24
  - profile generation drop-down menu, 25, 25*f*
  - URL field, 26
  - web browsers, 26
- Kleopatra, 112, 112*f*

**L**

- Laws and internet privacy
  - legal issues, 126
  - morals, 127
  - PRISM
    - AIVD agents, 123



- Canadian version, 125–126
- data communication, 122–123
- Google, Microsoft, and Verizon, 123–124
- internet backbones, 123
- NSA, 124–125
- TechCrunch article, 124, 125f

## M

- McAfee, 68, 69f
- Media access control (MAC) address filtering
  - Apple OSX, 51–52
  - definition, 49–50
  - in Windows, 50–51
- Microsoft, 123–124
- Microsoft store, 74
- MySpace, 93–94

## N

- NAT. *See* Network address translation (NAT)
- National Security Agency (NSA), 124–125
- NetGear Wi-Fi routers
  - connections window, 44, 45f
  - details window, 46, 47f
  - hidden network, 48–49
  - IPv4 Default Gateway, 47, 47f
  - MAC address filtering
    - Apple OS X, 51–52
    - definition, 49–50
    - in Windows, 50–51
  - network icon, 44, 44f
  - network/sharing center, 44, 45f
  - properties, 44–46, 46f
  - settings page, 42–44, 43f
  - Windows XP, 44
- Network address translation (NAT), 35–37
- Network firewalls, 37
- Norton, 67, 67f, 68
- NSA. *See* National Security Agency (NSA)

## O

- Online monitoring
  - consequences
    - ease of use, 118–120
    - government scrutiny, 120
  - e-mail (*see* E-mail)
  - governments
    - AT&T, 103–104
    - data encryption, 104
    - rouge monitoring code, 103
    - SSL vs. NSA, 104–105
  - IT professionals, 97
  - web browsing traffic (*see* Web browsing traffic)

## P

- Password
  - brute-force method, 22
  - character types, 21
  - KeePass
    - Add Entry screen, 24, 25f
    - creation, 23–24
    - home screen, 24
    - profile generation drop-down menu, 25, 25f
    - URL field, 26
    - web browsers, 26
  - OAuth service, 30–31
  - setting up, 23
  - two-factor authentication
    - application, 26
    - codes, 26
    - fob-based system, 27
    - random values, 27
    - software-based system, 27–28
    - text-messaging-based system, 28–30
- Porn Mode, 8
- Posting information online
  - BuzzFeed, 81–82
  - CNN, 81–82
  - EULA, 78–79, 79f
  - Eye-Fi card, 80
  - Facebook, 79–80, 79f
  - Flickr, 80
  - information security
    - Facebook (*see* Facebook)
    - Flickr (*see* Flickr)
    - MySpace, 93–94
    - Twitter, 82–83
  - personal embarrassment, 77–78
  - social media websites, 77
  - Twitter services, 80–81, 81f
  - Yahoo agreement, 80, 80f
- Pretty Good Privacy (PGP)
  - administrator option, 108, 110f
  - command prompt icon, 108, 110f
  - compose tab, 111
  - gen-key command, 110
  - GPG location dialog, 106–107, 107f
  - Gpg4win, 106–107
  - key expiration, 111
  - outlook privacy plugin, 106
  - public/private key pair, 107, 108f, 109f
  - RSA keys, 110, 110f
  - trade-off, 111
  - Windows 8 Start button, 108, 109f
  - Windows 8.1 Start button, 108, 109f

**PRISM**

- AIVD agents, 123
- Canadian version, 125–126
- data communication, 122–123
- Google, Microsoft, and Verizon, 123–124
- internet backbones, 123
- NSA, 124–125
- TechCrunch article, 124, 125*f*

**R**

- Router security
  - AT&T U-verse service, 35
  - cable internet services, 34, 34*f*
  - components, 35
  - D-Link firmware, 35, 36*f*
  - DSL services, 34, 34*f*
  - NAT, 35–37
  - NetGear router, 35, 37*f*
  - network firewalls, 37

**S**

- Safari, 15–17
- Secure Socket Layer (SSL) encryption, 103
- SecurityKISS, 116
- Software-based system, 27–28

**T**

- Text-messaging-based system, 28–30
- Tor website, 117
- Twitter, 82–83
- Twitter Terms of Services (TOS), 80
- Two-factor authentication system
  - application, 26
  - codes, 26
  - fob-based system, 27
  - random values, 27
  - software-based system, 27–28
  - text-messaging-based system, 28–30

**U**

- United Airlines website, 7
- Username
  - definition, 19
  - eHarmony account, 19–20
  - e-mail address, 20
  - internet websites, 19–20
  - OAuth service, 30–31
  - personal information, 20–21

**V**

- Verizon, 123–124

**W**

- Web browsing traffic
  - internet, 102–103
  - machine, 101–102
  - prevention
    - Anonymouse website, 114, 114*f*, 115–116, 115*f*
    - data tracking, 113–114
    - IP address, host, Browser/OS, 114, 115, 115*f*
    - Tor website, 117
    - VPN connections, 116, 117, 117*f*
- Wi-Fi Protected Access (WPA), 38
- Windows
  - BitLocker, 62, 62*f*
  - C/D drive, 62
  - control panel, 60, 60*f*, 61*f*
  - disk space, 64
  - password policy, 63
  - recovery key window, 62–63, 63*f*
  - recovery password, 63–64
  - start button, 60, 60*f*
  - Start Encryption button, 64, 65*f*
  - system and security link, 60, 61*f*
- Wired Equivalent Privacy (WEP), 38

**Z**

- Zip code, 2