Chapter 7

Securing Web Browsers and E-mail

Identity theft is the fastest-growing crime in the world. According to the Federal Trade Commission (FTC), identity theft is the top concern of people contacting the agency, and has now passed drug trafficking as the number-one crime in the world, affecting up to 10 million victims a year, costing the United States 50 billion dollars a year on average. Much of this can be reduced by leveraging some very practical security with regards to our Internet browsers.

One of the biggest battlegrounds in the fight against identity theft is your computer. We commonly use computers to communicate with the outside world using cell phones, web browsers, instant messaging software, and e-mail; all technologies that rely on the Internet. Identity thieves know this, and use the Internet as their tool for stealing identities through the acquisition of credit card numbers and online banking information, as well as gaining access to e-mail and social networking web sites to masquerade as someone else online. Therefore, securing our messaging systems has become a high priority to protect us from identity theft.

For the purposes of this chapter, we will concentrate on the web browser and e-mail clients as common messaging and communications systems. As we explain each of the security features of these systems and what they do, you can apply the information to other browsers, chat programs, and mail programs that you may be using, and configure them for the same level of security. Although the actual terminology may change, the concepts remain constant across applications (and platforms, for that matter).

When discussing how to secure your web browser, we will be covering Safari (Version 4) and Firefox (Version 3.6). There are other browsers out there, such as Opera and Google Chrome, but because these currently comprise a minority of browsers in use, we’re going to concentrate on securing Safari or Firefox. Likewise, there are a variety of e-mail clients out there. The two most common mail applications for the Mac are Microsoft Entourage (version 2008) and Apple Mail (version 4.2), so we will discuss these throughout the chapter as well.
CHAPTER 7: Securing Web Browsers and E-mail

**NOTE:** We spend much of this chapter discussing how to fine-tune your browser for security purposes, but we should mention that downloading and installing software from questionable sources, such as BitTorrent web sites, for example, is dangerous, and could damage your computer. It’s very hard to determine the origin of the software, and there is no guarantee the software won’t perform nefarious tasks on your machine. Keep this in mind when downloading software from these unknown sources.

A Quick Note About Passwords

We’ve mentioned it before and we’ll mention it again: if you take only one tip away from this book, take this one: use good, complex passwords! This is a mantra that we will use repeatedly throughout this book. We cannot overstate its importance.

**TIP:** When we refer to complex passwords, we are referring to passwords that consist of eight or more characters, contain a special character, and contain both letters and numbers where possible.

Your e-mail and online accounts are only as secure as the password you use to access them. And believe it or not, your e-mail account is quite valuable to a spammer. A resourceful spammer can make a small fortune by using insecure e-mail accounts to send spam. Because most web servers are fairly locked down with strong passwords, the spammer needs your e-mail account’s password to use it. And even if they don’t read your messages, they might end up getting your e-mail account disabled by your provider because of the high level of spam coming from your account. It can also be used to impersonate you to your friends and family, which can be very dangerous, especially when they ask for cash or private information. When this is used against high-profile individuals such as CEOs and celebrities, it’s called spear phishing.

Encrypting the e-mail transport, as many e-mail servers claim to do, is good, but without a hard-to-guess password, encrypted e-mail transport is not enough. No matter how heavily you encrypt the password and its transport between client and server, if the password is too easy to guess, then you may as well have not encrypted it in the first place. A weak password can be quickly guessed, encrypted or not.

**NOTE:** Not all providers allow the use of special characters in passwords. The characters that provide the most problems tend to be those that Unix reserves, such as ,, /, ?, and so on.