Keeping Your Data Secure - 1

by Vanessa Kier

Every couple of weeks I hear a story about how the computers or the website of this financial institution or that governmental organization suffered an attack from hackers. Or had data stolen from a supposedly secure location. How, then, are we supposed to keep our data secure?

Let's face it, if someone really wants the financial data stored on your computer, or that copy of your latest manuscript, they can get it with enough money and enough skilled resources. The only totally safe computer is the one that hasn't been built yet, because with each hardware and software component added there's also added the risk of malfunction or compromise. The best we can do is take reasonable steps to secure our computer. And, hopefully, we won't become the target of those willing to go to the extra lengths needed to break through our precautions.

The topic of computer and internet security is a huge one, going far beyond the space limitations of this column. So I'll hit upon some of the most basic elements and point you in the direction of great resources for learning more.

Passwords

1. Put a password on your computer's startup screen. Essential if you work on a laptop and take the laptop into public.
2. Put a password on your cell phone, particularly if it's a smartphone. At the very least, an unprotected phone exposes you to unauthorized users running up your phone bill.
3. Make the password complex. Yes, a cell phone might have a limit of four characters for the password, but don't use your birthday or any other piece of data easily tied to you. The strongest passwords contain numbers, letters (caps and lowercase) and symbols, making it hard for someone to guess. Afraid of not remembering your passwords? Use a mnemonic phrase, such as We love SFA for Ever!, then only use some of the letters. So this phrase might translate into a password of WlSFA4ev!
4. Don't overuse your passwords and usernames. If you use the same password on all your online banking and financial data websites and someone discovers that password in regards to one site, they've got access to all the other websites, too.
5. If you're logging into a site that offers a private or security key option, usually an image and/or phrase you need to validate in addition to your password before login, activate this feature.

Firewall

1. Turn it on. Most operating systems come with a firewall. This protects against hackers looking for an easy opening into your computer. Think of the firewall as the moat and wall guarding your castle aka computer. If your machine is older and doesn't have a firewall bundled with the operating system, install a commercial firewall program.
2. If your wireless router has a firewall, turn that on as well.

Keeping Your Data Secure - 2

Security Programs

1. Use antivirus software. Critical if you're using a Windows machine. Viruses can degrade your computer's performance and in some situations even crash your computer. Check to see if your internet provider offers a security suite for your computer that includes antivirus software. If not, there are very good programs available for free, or you can buy a program. A good resource for comparing the performance of antivirus software is: www.av-comparatives.org. Warning: Some commercial antivirus programs are known to be resource hogs, which means that once installed your computer may run slower, particularly when starting up or staring individual programs.
2. Install an anti-spyware/anti-malware program. This software scans your computer for programs that are installed on your computer without your knowledge. They may be marketing programs collecting data about your internet search habits so a marketer can target advertising to you, or they may try to collect personal data, such as passwords. Again, there are free options. Make certain that these programs are compatible with your antivirus software. Or install a comprehensive security suite that combines all of these features.
3. Research any security program before you install it, and if you're thinking of purchasing a program, see if you can run a trial version.

Safe Habits

1. Don't open e-mail attachments from unknown sources.
2. Don't click on links to unfamiliar websites/photos/videos/games that are sent via e-mail or social media. Viruses and malware can be embedded in these files. Be suspicious of links sent from friends via e-mails with no subject or with a subject line that makes no sense.
3. Never give out sensitive personal information, such as your social security number, your bank account number, etc. via e-mail. Banks and the government will never ask for this information in an e-mail.
4. Make sure you have security software scanning any files you do download from the internet. Many security software programs are set up to recognize suspicious patterns, even if the particular virus/malware isn't yet on its list of known threats.
5. Any time you're entering credit card or other sensitive data on the internet check for the secure website symbol. This is usually represented by a closed padlock.
6. Activate your e-mail provider's spam protection.
7. Disable pop-up windows. Don't click on the Close button or the X on unwanted pop-up windows, as this could trigger the installation of malware. Open a new tab in your browser. Then, if the pop-up is still present on the old tab, click Ctrl-W for Windows or Command-W for Mac OS. This will close that tab, taking the unwanted pop-up with it.
8. Be careful what machines you put your flash drive or other removable media into. If the other machine is infected, you could carry that back to your computer.
9. If you use a wireless router, take a look at this article which suggests ways to make your network secure. www.practicallynetworked.com/support/wireless_secure.htm At the very least, change the default password.
10. Disable third party cookies in your internet browser to stop many of the advertising cookies, or go to aboutads.info/choice and networkadvertising.org to opt out of specific marketing cookies.
11. Keep all your software updated. Many updates address security weaknesses, so this is critical to

ensure the protection of your machine.

12. Disconnect your computer from the internet when you're not actively online. Shut your computer off at night.

Below are some additional resources for keeping your computer and your data secure. Remember, as the old saying goes "An ounce of prevention is worth a pound of cure."

www.fbi.gov/scams-safety/computer_protect
www.microsoft.com/security/pc-security/botnet.aspx (Windows machines)
www.pcmag.com/article2/0,2817,2385673,00.asp (Mac OS X security)

This article first appeared in the *Tech Talk* column in the July 2011 issue of *Heart of the Bay*, the San Francisco RWA newsletter.