Maintaining Cyber Safety

BY DEBORAH H. WEINSTEN

The key to keeping your information secure online used to be simple: Ignore spam. As long as you remained vigilant to avoid online entreaties offering cheap watches, prescription drugs, or well-publicized scams and used automatic filters to root out the majority of online cons, you could trust that you weren’t making personal information available.

But, today, cyber attackers are more sophisticated and targeted. "Phishing schemes — in which a dummy Web site mimics a commonly used Web site, such as online banks or e-mail — have gained notoriety, as have less detectable spyware, worms, Trojan horses, and viruses that tend to work with personal information.

So, how do you protect your family, your business and yourself from online attacks?

ONLINE SECURITY AT HOME

In addition to installing and consistently updating antivirus, anti-spam, and security software, you can make great strides to improve security by setting ground rules for everyone under your roof.

First, ensure that your children know to delete e-mails when they don’t know the source or the sender. Often, cyber-scammers will simply try to "go through the front door" by sending an e-mail with an attractive offer. While you are likely able to recognize when an e-mail simply got past the spam filter, your children may not be as savvy — so stamping out any e-mails, instant messages, or texts from strangers is an easy rule to implement.

Second, avoid downloading free software, which often includes spyware and other programs designed to slow your home network or gather personal information. Often, scammers will offer useful-sounding "freeware" that actually installs a dangerous program onto your hard drive.

Third, never provide credit card information to a less-established company. This can be a problem for senior citizens in your household, as they are often targeted by scammers.

Finally, when simply surfing the Web, ignore e-mails or pop-up messages that ask you to update your account information. One scam simply directed the user to "type your credit card information here to see if it’s been compromised." Far more clever methods of gathering financial information are out there, so remain alert.

AT THE OFFICE

For small businesses, complicated cyber attacks can be more difficult to prevent and eradicate. By the time symptoms arise — suggesting your network or your data has been compromised, it can be too late — you already may have lost account data or other key information without even knowing your network was vulnerable. But, just as at home, you can take several proactive actions to keep your business virus-free.

Start by developing a strict code-of-conduct for employees’ online usage to help avoid dangerous activities. For example, peer-to-peer file-sharing Web sites and BitTorrent downloads can include applications that draw on hard-drive information. Any downloaded application can include a security threat.

In addition, consider installing systems that regularly scan for worms and update virus algorithms for signs of dangerous traffic, thereby helping prevent attacks and subsequent system failures.

With nearly every business dependent upon 24/7 communications and reliable networks, it is more important than ever to diagnose vulnerabilities and plug holes — long before symptoms of any security breach appear on your network. This can include assessing the effectiveness of network firewalls, ensuring safe, automated backups of information are occurring regularly, and password and authentication management.

Remaining aware is the key to protecting your business, your data, and your personal information from being compromised by cyber attackers.

A small business owner can take several simple steps to secure sensitive data. First, have a good password process that requires unique and random passwords that are changed regularly. Secondly, invest in software that will encrypt sensitive data.

Knowing the signs — and solutions — to a cyber attack will ensure your business communications and productivity remain consistent and uninterrupted.

IDENTITY THEFT

Identity theft is now the nation’s fastest growing crime, costing Americans an estimated $12 billion every year. As many as nine million Americans are victims of identity theft annually, and it can be difficult to restore their good credit fully, even after the security breach has been detected.

Adopting good online habits at home and work will go a long way toward protecting your identity. But, to go one step further, you can adopt a series of measures to detect whether your personal and financial information has been compromised.

If you have not reviewed your credit report within the past year, it may be worth contacting a credit reporting agency to see if anything unusual has arisen. But, do note that a great number of online scams are under the guise of offering you a credit report — seeking key personal information online in order to finalize the transaction. Thus, be certain you are contracting directly with one of the three credit reporting bureaus: Experian, Equifax and TransUnion.

In addition, simply maintaining your monthly accounting and bill-paying routines can alert you to potential problems. Good financial habits will alert you more quickly if you don’t receive your regular bills or if you receive credit cards you did not request — or even worse, communication from unknown creditors.

So, go ahead. Take advantage of the myriad of opportunities to gather data and shop online. But, be sure to implement regimented habits that will protect yourself and your company and ensure that your private information remains safe.

DEBORAH S. WEINSTEN, CISSP-ISSAP, GIAC-GSEC, is senior technology security manager for AT&T, Inc. (www.att.com). She can be contacted at 703-691-6101 (e-mail: dslevine@att.com). ©