

Working Online: Hazards Ahead

Save to myBoK

by Jill Burrington-Brown, MS, RHIA

HIM professionals know that as we move from paper to an electronic environment, our mission of privacy and security remains the same. As the medium changes, however, we must evaluate new threats to information.

The growth of the Internet has been proportionate to the growth of its attendant privacy and security hazards. If you own a business, telecommute to work through your home computer, or use your home computer online, you must be responsible for keeping up with the latest threats and implement preventive remedies.

These dangers include phishers, spyware, hackers, crackers, and script kiddies. But what are they and how can we guard against them?

Phishers

Phishers typically send urgent e-mails impersonating a financial institution or a company you trust.¹ The e-mail requests private information such as your credit card or bank card number and PIN and may even link to a site that mimics the authentic institution's Web site.

Phishers can take your information and use it to ruin your credit or take on your identity in other ways. Recent phishers have mimicked eBay and its subsidiary PayPal, as well as CitiBank. The phisher impersonating eBay sent urgent notices claiming members' status as eBay members was in jeopardy unless they confirmed their credit card accounts. The CitiBank phisher sent a similar notice. The best way to guard against a phisher is to never give out your private information to a requesting e-mail. If you haven't initiated the contact, it probably isn't legitimate.

Spyware

Spyware is software that gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.² Some spyware is covertly installed along with freeware or shareware. Pop-up windows also can install spyware deceptively if you click on an option within the window. A study conducted by AOL in May 2003 found that 91 percent of Americans with broadband access had some kind of spyware on their computers.³ Spyware has the capacity to track the Web sites you visit, take control of your browser's home page, and redirect you from selected Web sites to their competitors.⁴ It can also consume your computer resources, slowing down your system and sometimes causing system crashes.

There are various ways you can safeguard your system from software that downloads spyware. Be wary of free programs, such as free music software and other file-sharing software. Maintaining higher security settings on your browser will also help prevent spyware from finding a place to roost. Finally, a number of spyware detector and removal programs are available to help keep your system spyware-free.

Hackers and Crackers

In the professional programmer world, a hacker is a computer enthusiast looking to gain knowledge about computer systems and perhaps use that knowledge for pranks. Hackers usually do not break into systems for the purpose of stealing data or with other malicious intent. They do it to show off their skills.

A cracker is an individual who breaks into a secure system with malicious intent to steal or corrupt data.⁵ Crackers come in various skill levels. At the low end of the scale are script kiddies, inexperienced programmers looking to break into any

system.⁶ Script kiddies look for free programs written by experienced programmers and seek tips from hacker sites. Generally, they do not understand how code works or the logic behind it. While bothersome, generally script kiddies are not very harmful.

Next are technicians. They have programming skill and the ability to break into and use targeted systems as gateways to attack other systems. The most dangerous type of cracker is the industrial spy, who has specific plans to steal specific data.⁷ These kinds of crackers are usually highly skilled programmers.

Preventing attacks requires us to be aware of common security measures and to keep current with evolving threats. Update your computer's system often with the security tools offered by the manufacturer of your operating system and at the direction of your organization's information technology department if you have one. Finally, be vigilant about the type of e-mail you open and the programs you download.

Notes

1. "Protect Yourself Online." *Consumer Reports* 69, no. 9 (2004): 14.
2. Webopedia. "Spyware." Available online at www.Webopedia.com/TERM/s/spyware.html.
3. "Protect Yourself Online," 15.
4. Ibid, 16.
5. Webopedia. "Crack." Available online at www.webopedia.com/TERM/c/crack.html.
6. Hiner, Jason. "Securing Your Network from Hackers: Get to Know the Enemy." TechRepublic, December 11, 2000. Available at <http://techrepublic.com.com/5100-6264-1031154.html>.
7. Ibid.

Jill Burrington-Brown (jill.burrington-brown@ahima.org) is an HIM practice manager at AHIMA.

Article citation:

Burrington-Brown, Jill. "Working Online: Hazards Ahead." *Journal of AHIMA* 76, no.1 (January 2005): 58.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.