# Online fraud: protecting yourself

David De Lossy/Photodisc/Thinkstock

**In the age of the Internet, hackers around the world have developed a wide range of tools for invading computers, stealing confidential information, and accessing financial accounts.**

In this issue, we look at some of the most common types of online fraud – and offer suggestions on how you can keep your business safe.



## Phishing scams

You've seen the e-mails. They often look impressively authentic as they tell you that your bank requires you to submit your password, tax ID number, account number, or other confidential information. When you click on the link, you are taken to a "spoofed" Web site that features your bank's logo, some official-sounding language, and a log-in screen or form.

But in truth, these e-mails are distributed by "phishing" scams that are designed to capture your information so that criminals can access your accounts.

In 2008, there were 8,313 phishing sites reported — nearly double the number of the previous year. That trend is expected to continue well into the future.

Most anti-virus programs will help block phishing scams from your company's PCs. So make sure to install a reputable program and keep it up to date.

But the best defense against phishing is a skeptical eye — and the "delete" key. Alert your employees that virtually all legitimate financial institutions have policies against sending e-mail, phone, or mail requests for passwords, tokens, and other personal information. Therefore, any such requests should be immediately discarded.

And to ensure that you never enter a fake Web site, always enter your online banking service directly through its official sign-in page. Type the URL — such as www.citibusinessonline.com — directly into the address bar.

## Malware invasions

Hackers and criminals around the world are busy producing a wide range of malicious software programs — known as "malware" for short. These programs contain viruses, worms, spyware, and Trojan horses that can damage your company's computers, steal confidential information, and spy on your activities. Some are even designed to turn your PCs into "bots" that will silently participate in illegal online attacks.

*Continued*

citibank®

In 2007, the security software company McAfee reported receiving 370 new malware samples every day. And it expected that number to increase significantly over the next few years.

Malware programmers are extremely innovative, and have learned to embed their programs in Web pages, e-mails, and e-mail attachments. Once these programs take up residence on your computer or network, they can be very difficult to exterminate. Worse, you may not even know that they are there.

Again, the leading antivirus and firewall programs offer protection against many forms of malware. New forms are invented every day, making it imperative to keep your software up to date.

## Financial institutions fight back

Financial institutions are working around the clock to protect their customers against phishing, malware, and other online threats.

Citibank, for example, provides business customers with electronic security "token" devices that generate dynamic passwords that are virtually impossible for outsiders to imitate. Used in conjunction with a customer-selected password, tokens provide a very powerful two-dimensional method to ensure the security of online banking.

To help these methods work effectively, your customer-selected password should contain both letters and numbers, and should include upper-case and lower-case letters. Just as important, be sure to change your password at least every 90 days.

## Talk to Citibank®

Citibank is at the forefront of the financial services industry's efforts to combat online fraud. And your Citibank business specialist can explain the many ways in which we help protect your business. Call 877-528-0990 today, and learn how you can stay safe in a hazardous online world.

Be sure to consult with your own security experts to ensure the safety of your company's assets.