

Biz Buzz



The Next Big Online Threat Is it Someone You Know?

Almost everyone knows about spam and viruses. Most understand that up-to-date Anti-Virus software is a necessity. But there is a new threat with the potential to cause much more serious damage: Phishing and Spoofing.

“Phishing” is a relatively new form of online fraud. Commonly associated with spam, the goal is to fool the victim into providing sensitive personal information (usually your username and password, online banking information, or PayPal/Ebay, or other online store account information. Sophisticated examples include a link to a website where you can login and update your account information. Many phishing attempts are from seemingly legitimate sources asking you to update your account information, respond to a recent security threat by changing your password, or threatening to cancel your account unless you reply.

“Spoofing” is pretending to be someone else. This can include using the logo and branding of another company. “Email spoofing” is when the email message appears to be from someone other than the person who actually sent it - these emails can even appear to be from your own domain, from a system administrator within your company, or even yourself! A quick online search will reveal that virtually every major corporation has been a victim of spoofing: Visa, Citibank, MSN, Amazon.com, AOL, Yahoo, even Disney and the FBI have all been targets.

The danger is when that email appears to come from a company that you know and trust and possibly have an account with. When combined, phishing and spoofing result in a very sophisticated, convincing, and dangerous threat to your security, your business, and to online business in general.

How You Can Protect Yourself:

- Educate yourself about Internet fraud. A recent study by Visa Canada revealed that only 16% of Canadian email users were aware of phishing.
- Treat all email from people and organizations that you do not know as suspicious. Watch for email messages – even from companies that you know - that ask for personal or financial information. Legitimate financial institutions will never ask for your account details via email.
- Do not reply to or click on any links inside a suspicious email. Instead go to the company’s website and login from there or call the company directly. Never open an attached file from any suspicious email.
- Consider the tone and language of the message. Is it consistent with what you would expect of the sender? Be alert for spelling or grammatical errors.
- Ensure that your anti-virus and browser software are up-to-date. Consider installing firewall, anti-spam, and anti-spyware software. Report incidents of phishing to your ISP, webhosting company and the Anti-Phishing Working Group at: reportphishing@antiphishing.org.
- If you unknowingly supplied personal/financial information in a phishing attempt, contact your bank and credit card company immediately.

The danger is when that email appears to come from a company that you know and trust

The best defense against phishing and spoofing is education. Learn more at: www.antiphishing.org.



Chris Cormier is the in-house designer at ideas company. ideas company helps new or small businesses effectively market themselves in print and on the web. www.ideascompany.ca

