How to avoid being phished

If you've received an unexpected e-mail from a financial insitution or online seller that you may have dealt with, inviting you to update your files, you may have been "phished."

Phishing is a term used to describe the action of assuming the identity of a legitimate organization, or Web site, using forged e-mail and/or Web pages. These e-mails and sites are used to trick users into submitting personal information, including passwords, credit card numbers, and bank account information – even social insurance numbers, in some cases. The e-mails and the sites involved are designed to appear official enough – incorporating company logos and "real" links to other parts of the legitimate site – to deceive people into submitting their personal information.

While the practice has been around since the mid-nineties (when the term was first coined, as a reference that identity thieves on the Internet are luring people by "fishing" for passwords), it has become much higher profile over the last several months with a number of high profile organizations being "spoofed."

The risks are real. A Gartner Group study released in May 2004, showed at least 1.8 million consumers had been tricked into divulging personal information in phishing attacks, most within the past year. And dozens of additional scams have been launched throughout the Internet over the summer. Notable targets include eBay, Citibank, Suntrust Financial, and even Visa. One U.K. site documented more than 150 widespread and authentic-looking phishing scams from July to September 2004 alone.

In eBay's case, a variety of chillingly authentic-looking e-mails were sent out, requesting information to confirm online users' profiles and financial information. When a link on the e-mail was clicked, however, the user was taken to a fraudster's site, where the information was gathered and used for fraudulent purposes. Because of the popularity and perceived trust that eBay enjoys, they've been a frequent target. Several Citibank e-mails were sent out over the summer, with MailFrontier.com reporting that an estimated 40 per cent of recipients were taken in by the initial scam e-mail!

Even checking for an "SSL connection" – the little lock in your Internet browser indicating a secure connection – isn't a guarantee that you're safe. In some cases, fraudsters have registered a fake Web site that sounds authentic – in Visa's case, the site "visasecurity.com" was registered by a fraud artist, and the site collected information from users who had been "phished" for about 2-3 days before the site was abandoned. Site names such as "www.ebays.com" (note the extra "s") and www.yahoo-billing.com both sound legitimate, but both are fraudulent, and were used in recent scams.

Tips to avoid being phished

1. Don't respond to requests for personal information via e-mail
Many companies have now adopted a policy that they will not use unprompted e-mails to request personal information updates. If you receive an e-mail requesting personal information and you are suspicious in any way, contact the originating company – by phone, using a number from a bill or statement (not from the e-mail!) – and check it out.

Red flags should be raised if:

- the e-mail contains spelling or grammatical errors
- the tone seems unprofessional or out of character with the actual organization
- the e-mail request is marked urgent or overly time-sensitive
- the e-mail message itself contains a form asking for persoal or financial information

Remember that the sender or the reply-to e-mail address is not an indication of the validity of the e-mail either. These addresses can easily be spoofed to appear to come from legitimate sources when they do not.

2. Report incidents of actual or suspected abuse
If everyone is vigilant and contributes to helping police the issue, we all get the benefit of having phishing scams shut down promptly. Most responsible customer service desks will welcome reports of phishing scams targeting their organizations, and will provide more information and background to concerned consumers.

3. Avoid using links provided in e-mail messages
E-mail links can "appear" to take you to one site, but really direct you to another by hiding information in the e-mail message itself. You can reduce the risk by re-typing the name of the site in a new Web browser window. If possible, go to a trusted "home page" of the organization you're dealing with, and move around the site from there. This is a particularly good approach to use if you receive an e-mail seeking your password or other credentials – use the actual site itself, not a link from the e-mail.

4. Check to make sure the Web site is secure
While some sophisticated scam artists will set up SSL security to their fake sites, using extra diligence in checking for site security will help you avoid getting caught by "casual" fraudsters.

Ensure that any Web site that is collecting personal information has an "https" entry at the beginning of its address as it appears in your browser (e.g., https://www.lawpro.ca/file_online/login.asp), and ensure that you can see a closed padlock at the bottom of your browser screen. In Internet Explorer or Netscape, ensure that a small lock appears at the bottom of your screen to indicate a secure connection.

5. Be sure to audit your bank accounts and credit card statements
While many credit card companies are now taking the initiative to contact clients if large and/or out-of-country purchases are being made, it's a good idea to thoroughly review and double-check your statements to ensure that your accounts haven't been compromised.

6. Keep your software up to date
Some phishing scams are combined with the delivery of viruses or other malware – make sure to keep your computer system's operating system and software up-to-date with appropriate security patches, and ensure that your anti-virus, spyware and spyware software is current and running properly.

What if you've been phished?

Unfortunately, despite taking precautions, people can still be taken in by these fraudulent e-mails. If you suspect that you've been caught, here are some tips on what to do next:

1. **Keep a copy of the fraudulent e-mail as a record**.
2. **Contact your credit card company or financial institution immediately**, and advise them of the situation. Depending on the nature of the situation, file a police report as well. Some police stations may be reluctant to take a report, but this could be an important step in case you need to make insurance recoveries later on.
3. **Cancel your accounts or change your password on any Web site that may be compromised.** Make sure you do this from a different browser or computer from the original system that was compromised. Also contact the Customer Service department – by phone – of any organization involved. Take names, dates, and times of all contacts.
4. **Change your password on your e-mail account.** You will likely want to consider setting up a new e-mail account altogether, and cancelling the old account. Don't be too quick to take this step, as you may need e-mail access to validate information.

For more information on phishing, the following sites are recommended as good references: www.antiphishing.org and www.millersmiles.co.uk

Be alert – To paraphrase a character in the film "Matchstick Men" – "Con artists don't steal things from you – you give things to them."

David Reid is Director of Information Systems with LawPRO.