

Phishing is a reality on Internet life that simply will not go away. New types of threats are emerging on a regular basis. One of these – known as ‘pharming’ – is an attack in which Internet routing servers are taken over and traffic is redirected from legitimate web sites to bogus sites. Once there, unsuspecting surfers are tricked into entering sensitive personal information that is used to impersonate that individual at the real web site.

Being ‘net smart’ has never been more important. Smart consumers need to be able to identify and avoid Internet fraud and identity theft.

‘Phishing’ for Your Dollars

Phishing, also call brand spoofing, is a form of Internet fraud in which e-mail messages are used to lure the unsuspecting to web sites that are replicas of sites used by legitimate businesses. These web sites are used to trick users into divulging credit card numbers, bank account information, and passwords that will be used to commit fraud.

Phishing attacks normally are initiated through an e-mail. It will come disguised as a message from your financial institution or an Internet merchant you recognize. Even though the message looks legitimate, it may not be.

How can tell the real thing from the fake? Here are some things to look for:

- **WARNING SIGN #1: Soliciting Personal Information by E-Mail**

Financial institutions and reputable on-line retailers do not send e-mails asking for personal information. Period. Any e-mail that claims to be from a reputable source but asks for such data is probably a phishing expedition.

- **WARNING SIGN #2: Badly Written E-Mail**

Read the message closely. A professional company such as e-Bay or Amazon will not issue any communication containing basic grammatical and spelling errors. A high proportion of phishing e-mails contain such fundamental errors. For example,

From: support@citibank.com *spelling!*
To:
Subject: Verify Your E-mail with Citibank
Date: Wed, 31 March 2004 10:12:49 -0800 *grammar!*
Dear Citibank Member,
This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that use ATM.
This is done for your protection – because some of our members no longer have access to their e-mail address and we must verify it.
To verify your E-mail address and access your bank account, click on the link below.
<http://web.da-us.bank.com/signin/citifi/scripts/email.verify.jsp>
should be a secure web site (https)

- **WARNING SIGN #3: Hidden Addresses & Sources**

Phishing attacks will take you somewhere other than where they claim to be going. Check to see whether the web site you reach by clicking on the address in the e-mail is the same as the one shown in the e-mail. If it isn't, leave the site immediately. Look at the name of the web site shown in the e-mail. Reputable on-line businesses ensure that all their customer accessible web sites contain the company's name in the address. If you don't see that, you probably haven't reached the real web site.

- **WARNING SIGN #5: Asking for Personal Data**

Receiving an e-mail from your financial institution asking you to go to their web site should set the alarm bells ringing. That is not normal business practice for any credit union or bank. Don't click on the web address in the e-mail. Call your financial institution and ask whether they sent you a message.

- **WARNING SIGN #6: Threatening Legal Sounding Messages**

Consider the source. Would you expect your favourite on-line retailer to send you a threatening notice? Not likely. If you receive a threatening e-mail, it probably isn't legitimate. If you think it may be, call the company instead of responding to the e-mail.

Take Action

The simplest way to protect yourself from phishers is to avoid clicking on any unexpected link in an e-mail message. DO NOT reply to e-mails soliciting personal information. Having safely ignored the suspicious e-mail, report it.

A significant proportion of on-line fraud goes unreported. Some people are too embarrassed to admit they've been taken in. Others simply don't know what to do.

If you do spot something suspicious, go to the company's real web site – the one that looks like www.companyname.com. Most sites have an option on their home page labeled "Contact Us" or something similar. Use that to report the phishing attempt. If you have gone so far as to provide sensitive personal information before realizing you may be a phishing victim, report the matter to your local police and keep a copy of the police report. You may need that documentation to resolve any fraudulent transactions.

Go on-line to www.recol.ca, the web site for Reporting Economic Crime On-Line. This site is administered by the National White Collar Crime Centre of Canada and is supported by the RCMP and other law enforcement agencies. You can also call, toll-free to PhoneBusters, the Canadian Anti-Fraud Call Center at 1-800-495-8501.

Put Your Knowledge To The Test

Think you're ready to avoid the phishers trying to separate you from your money? Take the anti-phishing challenge by going to http://survey.mailfrontier.com/survey/Phishing_uk.html

Protect your identity!