Avoiding Phishing Scams

If you receive e-mails with the following messages: “Important information regarding your account” or “Your Account is disabled: Please Re-Verify Your Account,” it may be a scam, called “phishing,” and it involves Internet fraudsters who send e-mail spam or pop-up messages to lure personal information (e.g., credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information) from unsuspecting victims. Some phishing (pronounced “fishing”) e-mails threaten a “dire” consequence if you do not respond. The messages provide a link that directs you to a website that may look legitimate. But it is not – it is a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The Federal Trade Commission suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And do not click on the link in the message, either.**

Legitimate companies do not ask for this information via e-mail. If you are concerned about your account, contact the organization mentioned in the e-mail using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct web address yourself. In any case, do not cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but actually send you to a different site.

- **Area codes can mislead.**

Some scammers send an e-mail that appears to be from a legitimate business and ask you to call a phone number to update your account or access a “refund.” Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers are physically located. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random e-mails that ask you to confirm or divulge your financial information.

- **Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.**

Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge. Antivirus software and a firewall can protect you from inadvertently accepting such unwanted files. Antivirus software scans incoming communications for troublesome files. Look for antivirus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It’s especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software “patches” to close holes in the system that hackers or phishers could exploit.

- **Do not e-mail personal or financial information. E-mail is not a secure method of transmitting personal information.**

If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons. You can also double-click the lock to guarantee the third-party SSL certificate that provides the https service. Many types of attacks are not encrypted but mimic an encrypted page. Always look to make sure the web page is truly encrypted.

- **Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.**

If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- **Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.**

These files can contain viruses or other software that can weaken your computer's security.

- **Forward spam that is phishing for information to spam@uce.gov and to the company impersonated in the phishing e-mail.**

Most organizations have information on their websites about where to report problems.

- **If you believe you've been scammed, forward phishing emails to spam@uce.gov – and to the company, bank, or organization impersonated in the email. You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a group of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.**

Victims of phishing can become victims of identity theft. While you cannot entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

Contact

AIG Programs Loss Control
T 800 611 3994
F 888 659 9047
programslc@aig.com

AIG Bring on tomorrow