Phishing:
Be suspicious of unsolicited e-mails you receive

In February 2007, The Washington Post reported about 109 million U.S. adults received phishing e-mail attacks in 2006, compared with 57 million in 2004. The average loss per victim in 2006 was $1,244, nearly five times the $257 average loss reported in 2004.
Understanding the ups and downs of the Internet and online transactions is one of the best ways to start practicing "safe computing." Armed with a good understanding of common threats and a few practical tips to help you and your information stay secure, you can click to your heart's content.

One of the biggest threats to safe computing is phishing.

Phishing — also known as carding or brand-spoofing — is a type of deception designed to steal your identity. In a phishing scam, a thief tries to get information like credit card numbers, passwords, account information, or other personal information from you by convincing you to provide it under false pretenses. Phishing schemes usually come via spam e-mails or pop-up windows, and often pose as legitimate businesses with which consumers may do business.
In a phishing scam, the messages often look very authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. And because these e-mails look so official, up to 20 percent of unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them.
Con artists will continue to develop new and more creative ways to take advantage of consumers online. But following these five steps can help you reel in phishing scams, and to protect yourself, your identity and your assets:
1. Never respond to requests for personal information via e-mail. Legitimate businesses and financial institutions never ask for personal information like passwords, credit card numbers, or other personal information in an e-mail. If you do receive an e-mail requesting this kind of information, don't respond. If you think the e-mail is legitimate, contact the company by phone or through their Web site to confirm.
2. Don't click on links you receive in unsolicited e-mails, rather type Web addresses directly into your browser. Be suspicious of unsolicited e-mails you receive from any business. Look for misspellings and bad grammar in e-mails you receive. While an occasional typo can slip by any organization, more than one is a tip-off to beware. If you suspect that an e-mail from your credit card company, bank, online payment service, or other Web site you do business with is not legitimate, don't follow the links to the Web site from an e-mail message. Those links may take you to a spoofed site that might send all the information you enter to the scam artist who created the site. Sophisticated hackers can even display a fake URL in the address bar of your browser.
3. Check to make sure the Web site is using encryption. Before you enter any personal information, check to see if the Web site uses encryption to transmit your personal information. In Internet Explorer you can do this by checking the yellow lock icon on the status bar. If the lock is closed, then the site uses encryption to help protect any sensitive personal information — such as credit card numbers, Social Security numbers, or payment details - that you enter. Double-click the lock icon to display the security certificate for the site. The name should match the site you think you're on. If the name differs, you may be on a spoofed site.
4. Routinely review your credit card and bank statements for suspicious charges. Review your bank statement and credit card statements at least monthly for fraudulent charges.

5. Report suspected abuses to the proper authorities, including the Office of the Indiana Attorney General's Consumer Protection Division. Also report the scam to the company that's being spoofed. Visit the companies website rect contact information. The company may have a special e-mail address to report such abuse.

Resources

The Consumer Protection Division of the Indiana Attorney General's Office works to safeguard the rights of Indiana citizens every day. If you have questions or complaints regarding phishing, or other appropriate consumer issues, contact the Attorney General's Consumer Protection Division using the web address and phone number listed below, or visit www.in.gov/attorneygeneral for more information.