



Fact Sheet on PHISHING

Phishing is a technique used by con artists to gain your personal information in order to steal your identity. In this scam, con artists pose as a financial institution, an electronic retailer, a credit card provider or even a government agency and send spam electronic mail or pop-up messages designed to trick you into revealing your account information, credit card numbers, or other information that could be used to steal your identity. Phishing has become more sophisticated and dangerous.

The e-mails and pop-up messages often look authentic, and they usually direct you to Web sites that look just like the sites of the legitimate businesses. Once you get to the site, you are asked for sensitive account information to "update" or "validate" your account information.

If you receive an email from anyone asking for your personal information, no matter how legitimate it may seem, follow these tips:

- If you receive an e-mail or pop-up message asking for sensitive information, do not reply to the message and do not click on any links inside it. Legitimate entities will not contact you and ask you to send them personal or financial information via e-mail.
- If you are concerned about your account, you should contact your bank or credit card provider using a phone number or Web site that you know is legitimate.
- Use anti-virus software to protect your computer from potential viruses in accidentally opened files or attachments. Do not open an attachment if you do not know who sent it to you or why it was sent.

As these scams become more sophisticated, consumers might be fooled into responding. If you think you may have been tricked by a phishing scam, you should take the following steps:

- If you have given someone your bank account information, report this to your bank immediately and close your account.
- If you have given out credit card information, report this to your card issuer immediately. Also review your credit card statement regularly for unexplained charges.
- If you have given any other account information such as personal identification numbers (PINs) or passwords, report this to the card issuer or bank immediately.
- In any case where you have disclosed your account information, passwords, Social Security Number or other identifying information, contact one of the three credit reporting agencies (Equifax, Experian and Trans Union), request an initial fraud alert be placed on your account and request a free copy of your credit report. Review your credit report for any unauthorized charges or credit accounts.

If you have given out account information for an electronic retailer (ebay, paypal, AOL) contact that company immediately to cancel the account and report the incident.

Please visit

www.IllinoisAttorneyGeneral.gov

Chicago
(800) 386-5438
TTY: (800) 964-3013

Springfield
(800) 243-0618
TTY: (877) 844-5461

Carbondale
(800) 243-0607
TTY: (877) 675-9339