



Beware of “Phishing”

From the Office of Minnesota Attorney General Lori Swanson

The Minnesota Attorney General’s Office warns consumers to be on guard against fraudulent operators “phishing” for consumers’ personal information. Phishing occurs when fraudulent operators send e-mail impersonating financial institutions, government entities, internet service providers, national chain retailers, internet auction companies, or other companies, requesting that consumers “verify” their personal information. In this scam, fraudulent operators contact a consumer through e-mail, asking the consumer to disclose their credit card number, ATM PIN number, social security number, or other personal information. The consumer’s information is then used to commit the crime of identity theft. Identity theft occurs when a fraudulent operator has obtained a consumer’s information, and uses the information to withdraw money from the consumer’s accounts, or to obtain credit in his/her name.

Phishing scams may be particularly hard to spot, since the e-mails frequently have an official-looking appearance. Phishing scam e-mails frequently copy the logo of the company they are impersonating in an effort to trick consumers. Such e-mails often include a link to a website, which may appear identical to the standard website for the impersonated company, but is actually a fake website, mimicking the real thing. Fraudulent operators use sophisticated tactics to cloak the Universal Resource Locator (“URL”) of their fake websites. The URL is the address of the webpage that appears at the top of most internet browsers. Although the false URL may indicate the page belongs to a particular company, it actual belongs to a scam artist, who is often located outside of the United States. Such tactics are designed to trick a consumer into believing that he/she is dealing with a company or government entity that he/she trusts.

According to an alert released by the Federal Trade Commission (“FTC”), some consumers have fallen prey to e-mail requests asking them to disclose their financial

information to the “federal government” in accordance with federal law. In fact, there is no federal law requiring consumers to register such information with the federal government, and the senders of these e-mails are actually fraudulent operators phishing for information to commit identity theft. In another variation of this scam, a consumer may receive a fraudulent e-mail that appears to originate from a company the consumer does business with, such as a bank, an online auction company, or retailer, claiming that the company’s security has been jeopardized, and that the consumer must “confirm” their personal account information or the account will be frozen.

In another variation on the phishing scam, fraudulent operators use “spyware” software to track the websites that a consumer accesses from his/her computer. Fraudulent operators use this information to create “pop-up” windows, which appear on the screen when a consumer accesses the website of a given company. The “pop-up” message then asks the consumer to “verify” their personal information. Consumers may believe that the “pop-up” window is associated with the company’s website and agree to disclose their information to the fraudulent operators.

The Minnesota Attorney General’s Office provides the following tips to help consumers protect their personal information from scam artists phishing for their information:

- 1) Beware of e-mail requests to “verify” your personal information online. Companies you do business with already know your account number and do not need to verify it. Furthermore, in the event of a security breach or computer problem, most companies contact their customers in writing or by telephone to discuss the matter.
- 2) Contact companies through trusted channels. If you are concerned about receiving such an e-mail, call the company immediately at the publicly-listed phone number.

3) Don't be rushed by suspicious e-mails. Since many individuals, businesses and non-profits rely on the financial viability of their account in a given day, the prospect of a temporarily frozen account and lost business that could result can be particularly worrisome. Remember, however that the amount of money lost to such a scam is typically a much larger problem. Take your time to think logically and contact your financial institution directly.

4) Do not access links or "cut and paste" from questionable e-mail messages. By doing so you may be redirected to an official-looking website maintained by fraudulent operators.

5) Use a URL-checker. Computer users may wish to access software which allows them to check the accuracy of a given URL. This will help you know who you are dealing with online.

6) Do not disclose your personal information to "pop-up" messages. Consumers may protect their computer systems against spyware based pop-ups by purchasing anti-spyware software.

Consumers should report internet fraud to the Federal Bureau of Investigation's Internet Fraud Complaint Center online at: www.ifccfbi.gov/. Consumers with concerns about internet scams may contact the following agencies:

**Federal Bureau of Investigation
Minneapolis Office**

111 Washington Avenue South, Suite 1100
Minneapolis, MN 55401
(612) 376-3200

**Federal Trade Commission
Consumer Response Center**

600 Pennsylvania Avenue, NW
Washington, D.C. 20580
1-877-382-4357
www.ftc.gov

**United States Secret Service
Minneapolis Field Office**
300 S. 4th St., Suite 750
Minneapolis, MN 55415
(612) 348-1800

For more information on identity theft, or other consumer issues, consumers may contact the Minnesota Attorney General's Office as follows:

Office of Minnesota Attorney General

Lori Swanson

1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101
(651) 296-3353
1-800-657-3787
TTY: (651) 297-7206
TTY: 1-800-366-4812

