Phishing

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

We live in the land of 10,000 lakes, but not all fishing in Minnesota involves walleye or northern pike. Attorney General Keith Ellison warns consumers to be on guard against fraudulent operators "phishing" (not "fishing") for consumers' personal information. According to the FBI's Internet Crime Complaint Center, Internet fraud costs victims hundreds of millions of dollars each year, with phishing being the top form of Internet fraud. Increasingly, fraudulent operators are using throw-away email accounts and other advancements in technology to avoid detection and steal consumers' information, identity, and money.

Phishing generally occurs when fraudulent operators send email impersonating financial institutions, government entities, Internet service providers, national chain retailers, Internet auction companies, or other companies, requesting that consumers "verify" their personal information. Scam artists then use this information to commit identity theft. Phishing can also occur over the phone, through text messaging, through phony or hijacked websites, or social networking sites.

Email Phishing

In the most common variation of phishing, fraudulent operators contact a consumer through an email that appears to originate from a company that the consumer does business with, such as a bank, online auction company, or retailer. The fraudulent email asks the consumer to disclose their credit card number, ATM PIN number, Social Security number, or other personal information. Often, the message will indicate that the consumer's account has been frozen or their security has been jeopardized and urges the consumer to act immediately. Scam artists use fear and urgency to pressure consumers to act rashly in disclosing information that they otherwise would not share. The consumer's information is then used to commit the crime of identity theft by withdrawing money from the consumer's accounts, or obtaining credit in his/her name.

Phishing scams may be particularly hard to spot, since the emails frequently use an official-looking appearance. Phishing scam emails frequently copy the logo of the company they are impersonating in an effort to trick consumers. Such emails often include a link to a fraudulent website.

Website Phishing

Fraudulent operators create fake websites designed to look identical to the website of a well-known company. Scam artists then 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 actually belongs to a scam artist. Such tactics are designed to trick a consumer into believing that he/she is dealing with an entity that he/she trusts.

Scam artists may also hijack legitimate websites in order to re-direct the consumer to their own fraudulent website (sometimes called "pharming"). Fraudulent operators may also use "spyware" software to track the websites that a consumer accesses from his/her computer.

Fraudulent operators use a consumer's web history 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. Consumers may inadvertently download spyware to their system by clicking on a link on a fraudulent website that they believe to be legitimate. Fraudulent operators also set up fake websites within social networking websites, in order to phish for consumers' private information. Since some of these websites cater to young consumers, they may be especially vulnerable to phishing.

Phony Government Email Phishing

According to an alert released by the Federal Trade Commission (FTC), some consumers have fallen victim to email requests asking them to disclose their financial information to the "federal government" in accordance with federal law. The Internal Revenue Service (IRS) and the Federal Deposit Insurance Corporation (FDIC) have put out similar alerts. In fact, there is no federal law requiring consumers to register such information with the federal government, and the senders of these emails are actually fraudulent operators phishing for information to commit identity theft.

"Vishing" and "Smishing"

Vishing and smishing are variations of phishing that may be executed through the telephone or SMS (short message service). In a typical vishing scam, a consumer may receive an email indicating that the security of their account has been breached. The message may simultaneously warn the consumer about email phishing scams and request that the consumer contact a telephone number listed within the message. The phone number will redirect the consumer to a boiler room fraud operation where they will be asked to disclose their personal information, which will undoubtedly be used to commit identity theft. Vishing can also include traditional telemarketing fraud where a scam operator cold-calls a consumer and uses some pretext to request that they disclose their private information. In the case of smishing, a consumer receives similar communication through a text message, SMS, or hand held computer.

The Attorney General's Office provides the following tips to avoid phishing scams:

1. Beware of email 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 email, call the company immediately at the publicly–listed phone number. Don't trust the number or email in the message.

3. Don't be rushed by suspicious emails. 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.

4. Do not access links or "cut and paste" from questionable email messages or websites. 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 may help you know who you are dealing with online.

6. Consumers should avoid disclosing personal information over the Internet in general unless they are 100 percent certain that their computer and the website with which they are dealing is secure. 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 and/or using pop-up blockers. Update your antispyware, virus protection, and other software regularly. Report Internet fraud to the Federal Bureau of Investigation's Internet Crime Complaint Center online at *www.IC3.gov* and contact the following agencies:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580
(877) 382-4357
www.consumer.ftc.gov

United States Secret Service
300 South 4th Street, Suite 750
Minneapolis, MN 55415
(612) 348-1800
www.secretservice.gov