

# NYS Consumer Protection Board's SPOTLIGHT on PHISHING SCAMS

**Phishing** (also called *pharming* or *whaling*) e-mails trick people into sending money or providing personal information such as usernames, passwords, credit card details, and Social Security numbers to unauthorized individuals who hijack their information.



***Some more prevalent and troublesome Phishing scams involve:***

## ***Business / Retail Establishments***

With technology at their fingertips, scammers are recreating and using official logos, company information, disclaimers and more to lure consumers into responding to their offers, queries, surveys or payment alerts. In 2008, scams perpetrated against McDonalds and Walgreens, as well as i-Tunes, Wal-Mart, and even the Better Business Bureau were publicized by the CPB.

## ***Banks and Financial Institutions***

Scammers continue to hack into websites of banks and financial institutions and e-mail unwitting consumers requesting personal and financial information. Compounding this problem, are the many changes in corporate structure which are prompting modifications in brands, names, letterheads and statements. Phishers are capitalizing on the confusion, sending e-mails that look like they're from a financial institution to collect personal information such as credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. These Phishing messages typically ask consumers to "update," "validate," or "confirm" account information. They may also ask consumers to protect account information, stating, for example, that the bank or financial institution has had to "block some accounts connected with money laundering, credit card fraud, terrorism and check fraud activity." Recipients are asked to log in using a link provided to check and verify their financial accounts. Banks and financial institutions do not ask for information to confirm that which they already maintain.

## ***Couriers***

A Phishing scam from alleged couriers such as Federal Express, DHL International and UPS tells consumers that a package is ready to be delivered (the box for which may actually be pictured in the e-mail) containing a check, money order, or bank draft representing a large sum. The scam usually requires that security fees be provided from consumers. The fees end up in the hands of scammers rather than legitimate business, robbing the perspective recipient of their money and providing no package in return. All the couriers listed above have assured users that they have been alerted to the unauthorized use of their business names, service marks and logos by persons or companies fraudulently representing themselves as representatives of their companies. Legitimate couriers do not require recipients to provide payment or personal information in return for delivery of goods.

## ***Social Networking Sites***

Phishing and downloadable virus scams emerged on social networking sites such as Facebook.com, and are exploiting the lack of caution people may exhibit online. The technique tricks people into visiting fake websites designed to look like the login page of a popular website for the purpose of stealing their personal information. Criminals target personal information disclosed by users on Facebook, for example, sending a message that appears to be from a friend to network users. The message may tell the user that a friend is changing their online profile, mentioned them in a blog posting, or alert them to an exciting new online picture or video. It may use slang or even include the user's name to a link that appears legitimate. The link will direct them to a URL such as view-facebookprofiles.com or facelibook.com that looks identical to the real Facebook login page. Users who submit their e-mail and Facebook password then have their profiles hijacked, giving the scammers access to all their personal information. Their friends may then also receive a similar message, thus continuing the cycle.

## Phishing scams, continued

### **Job Searches**

As a result of the large number of layoffs, a relatively new Phishing scam is targeting people who have listed their resumes on job search sites. Scammers pretend to be potential employers and request Social Security numbers and other personal information, which is then used to commit fraud.

### **Internal Revenue Service (IRS)**

Spam messages promising an unexpected tax refund continue to be sent to computers across the country. The spam message, which is "signed" by the IRS, may read as follows: "After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of \$109.30. Please submit the tax refund request and allow us 6-9 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access the form for your tax refund, please click here." In March 2008, the IRS reported that taxpayers had brought more than 33,000 of these scam e-mails, reflecting more than 1,500 different schemes, to their attention. The IRS never uses e-mail to contact taxpayers about their tax issues.

### **The Federal Bureau of Investigations (FBI)**

The FBI has been targeted by scammers who are sending e-mails from alleged high-level organization officials with "official orders" from the FBI's Anti-Terrorist and Monetary Crimes Division to target consumers. The FBI or other "official" seals, letter head, photographs and/or banners presented in the e-mails look authentic. Recipients are told they have been named the beneficiary of millions of dollars; however, the e-mail claims the FBI has stopped the transfer of these funds due to suspicion that they are related to terrorism. To further "substantiate" the claim, recipients are then provided with directions on how to obtain a "Diplomatic Immunity Seal of Transfer" which the scammer contends must be provided so that the claimant can avoid prosecution. To collect the large sum, recipients are instructed to furnish personal information including, the recipient's name, banking information, telephone number, a copy of their passport and sometimes a fee.

### **US Courts**

E-mail messages purporting to be subpoenas and commanding recipients to appear before a grand jury in a U.S. District Court represent a Phishing scheme targeting business executives (a tactic known as "whaling") and attempting to lure recipients into downloading and installing software that records their keystrokes and allows computers to be controlled remotely. The U.S. Court system became aware of this scheme and posted an advisory alert on its website, alerting consumers that it had received bogus e-mail grand jury subpoenas, purportedly sent by a United States District Court. The Court issued a statement saying "The e-mails are not a valid communication from a federal court and may contain harmful links. Recipients are warned not to open any links or download any information relating to this e-mail notice." The federal Judiciary's e-mail address is [uscourts.gov](mailto:uscourts.gov). The e-mails in question appear to be sent from a similar address that is not owned and operated by the federal courts. Law enforcement authorities have been notified."

Consumers should report suspected Phishing scams to the FTC at **[spam@uce.gov](mailto:spam@uce.gov)**, to the CPB at **[www.nysconsumer.gov](http://www.nysconsumer.gov)**, and to the institution or company targeted in the Phishing e-mail. They may also be reported to the Anti-Phishing Working Group at **[reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org)**.

For further information, please refer to the CPB's Consumer Guide to Preventing and Responding to Identity Theft, available at [http://www.consumer.state.ny.us/pdf/id\\_theft\\_online\\_version.pdf](http://www.consumer.state.ny.us/pdf/id_theft_online_version.pdf) or refer to the many resources available through the CPB's homepage at [www.nysconsumer.gov](http://www.nysconsumer.gov).

