NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Fall 2004 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

It's Phishing Season

"Phishing" (pronounced: fishing) may lend itself to corny headlines, but it describes a serious, sophisticated practice in which Internet con artists—using bogus e-mails and websites designed to look like those of legitimate companies, banks, or government agencies—trick unwitting customers into divulging sensitive financial and personal information.

Staff at the CyberScience Laboratory (CSL) in Rome, New York, have been gathering information on this phishing epidemic for many months to share with law enforcement agencies throughout the United States. Funded by the National Institute of Justice to be a national resource center in the fight against cybercrime, CSL has begun to get requests for training, assistance, and outreach on this proliferating online crime.

In a typical phishing scam, the perpetrator copies the webpage code from a well-known site (such as eBay®, Citibank, or AOL®) and uses it to set up a replica page, complete with company logo, fonts, styles, and links to mimic the real company webpages. He or she then uses spamming techniques to send a million or more e-mails with a single click. The e-mails advise Internet users that their billing information needs to be confirmed or updated because of a technical or security problem and directs them to click on a hyperlink to reach the official corporate or institutional website.

In actuality, the link sends them to the scammer's look-alike page. Once there, the user is asked to provide credit card information, password, personal identification number, Social Security number, mother's maiden name, and other closely guarded data. Armed with this information, the scammer can proceed to run up charges in the user's name, empty bank accounts, apply for loans or new credit cards, and commit many other types of identity theft.

According to the Anti-Phishing Working Group (APWG), an industry watchdog organization, consumer phishing attacks are on the rise. In April 2004, 1,125 unique new attacks were reported—an increase of 180 percent over the previous month. (The number of attacks may even be higher, because APWG can only report the number of scams they hear about.) The group estimates that about 5 percent of phishing e-mail recipients "take the bait," but if 1 million e-mails are sent out, 50,000 people will be victims.

Gartner, Inc. (http://www4.gartner.com/Init), an information technology research firm, estimates that—

- More than 57 million Internet users in the United States have received some sort of e-mail related to a phishing scam.

If You Get Hooked . . .

If you receive a possible phishing e-mail, **do not** respond to it. Send copies of the e-mail to the Federal Trade Commission (FTC) at uce@ftc.gov and to the Anti-Phishing Working Group at reportphishing@antiphishing.org. Also send a copy of the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g., spoof@ebay.com).

If you have already disclosed your personal information to a possible phishing e-mail or website, immediately file an online complaint with the Internet Crime Complaint Center (a joint project of the FBI and the National White Collar Crime Center) at http://www.ic3.gov. Also go to the FTC's identity theft website at http:www.consumer.gov/idtheft and follow the directions there for reporting information to credit bureaus, credit card companies, and law enforcement.

In addition, an article titled "Protect Yourself Online" in the September 2004 edition (Vol. 69, No. 9) of *Consumer Reports* offers information and resources regarding phishing scams, computer viruses, junk e-mail (spam), and spyware.

- Close to 2 million checking accounts have been exploited.
- Annual losses associated with phishing exceed $2 billion.

In July 2004, CSL's Jeffrey Isherwood discussed phishing scams at a meeting of the U.S. Secret Service's Electronic Crimes Task Force during a cybercrime seminar in Charlotte, North Carolina. Isherwood covered such topics as how to spot phishing e-mails, tools for analyzing e-mail headers and tracking phishing e-mail to its source, and the need for law enforcement agencies to educate the public about phishing.

"Public awareness is the key, as it is in [fighting] all types of crime," says Isherwood. "People need to be suspicious of any e-mail that solicits credit card or other confidential information; that is not how legitimate companies work." And he cautions that those receiving a phishing e-mail should not click on the hyperlink and should not send a hard copy to report the incident; rather, they should forward the e-mail as an attachment to an appropriate resource (see "If You Get Hooked . . ."). To trace a bogus e-mail, investigators need to "look under the hood" at the code beneath the headers to figure out its source—not a simple task. Phishing e-mails are often relayed through dozens of servers in an attempt to hide the sender's true location.

Law enforcement agencies interested in learning about the methods of phishing scammers and the resources available to thwart them can contact the CyberScience Laboratory at 888–338–0584 or register at www.cybersciencelab.com

This article was reprinted from the Fall 2004 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.