GONE PHISHING: THE INTERNET AND IDENTITY THEFT

Phishing Defined

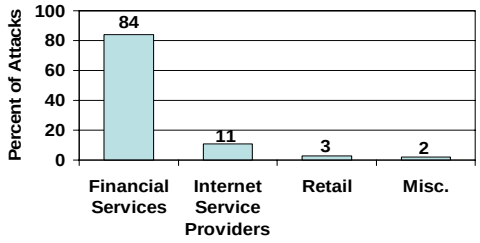
Phishing is a form of Internet fraud that involves sending an email message to an Internet user falsely claiming to represent a legitimate enterprise. This is done in an attempt to trick the user into visiting a fraudulent website and disclosing sensitive personal information that would then be used to commit identity theft. Phishing is a play on the word, "fishing," since the phisher is putting out bait in the hope that at least some people will be enticed to respond to the message.[1]

The Anti-Phishing Working Group (APWG), an industry-sponsored association, estimates that 75 million to 150 million phishing emails are sent daily.[2] Despite the fact that many of these messages are blocked by spam filters and never reach Internet users, it is estimated that a well-designed phishing email campaign can have response rates of up to 5 percent.[3]

Phishers often choose to target large financial institutions known to have a significant online customer base. This is done with the knowledge that a certain percentage of the email message recipients will be actual customers of the institution and likely to believe that the message is legitimate. Typically, the message attempts to spur the user to act before some adverse consequence occurs, such as having one's account cancelled or blocked.

Also targeted are websites belonging to Internet service providers, retailers, and even government agencies. Chart 1 illustrates the breakdown of industry sectors that were targeted most frequently by phishing attacks during April 2005.

Chart 1
Industry Sector Most Targeted by Phishing Attacks
April 2005



Prepared by AARP Public Policy Institute
Source: Anti-Phishing Working Group Phishing Activity Trend Report, June 2, 2005.

Once users have contacted the fraudulent website, they are asked to provide or update personal information, such as credit card or bank account number, account username, password, security code, Social Security number, or other sensitive personal information that is already held by the legitimate organization.

After collecting the information, the phisher will often sell the victim's personal information via the Internet to others who intend to use the information to commit fraud.[4] With their personal information compromised, the victim is at risk of a number of possible frauds:

- The information can be used to access existing financial accounts.
- The information can be used to apply for credit and open new accounts in the victim's name.
- The information can be used to hijack the victim's computer and use it as a platform to disseminate phishing and spam email messages to others.

The Increase in Phishing Attacks

Phishing frauds have become increasingly easy to perpetrate, with ready-made phishing toolkits and

---

[1] Another form of phishing, called "pharming," involves using computer program tricks to redirect Internet users from a legitimate site to a fraudulent site operated by criminals.

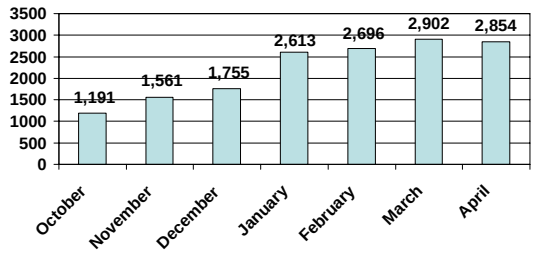
[2] APWG. "Commentary to FDIC 'Putting an End to Account-Hijacking Identity Theft,'" Feb. 4, 2005, http://www.antiphishing.org/APWG-FDICCommentaryLetter.doc.

[3] B. Sullivan. *Your Evil Twin: Behind the Identity Theft Epidemic*. John Wiley & Sons, Inc., 2004.

[4] Federal Deposit Insurance Corporation (FDIC). "*Putting an End to Account-Hijacking Identity Theft,*" December 14, 2004, http://www.fdic.gov/consumers/consumer/idtheftstudy.

email address lists available for purchase on the Internet.[5] The APWG, which regularly tracks phishing activity trends,[6] reports that 14,411 new, unique phishing email messages were reported in the month of April 2005. The number of active phishing (fraudulent) websites reported by the group in April 2005 was 2,854 (Chart 2).

Chart 2
Active Phishing Sites by Month
October 2004–April 2005



Prepared by AARP Public Policy Institute
Source: Anti-Phishing Working Group Phishing Activity Trend Report, June 2, 2005

Typically, the fraudulent websites are only active for a short period. According to the APWG report, the average time a phishing site remained active during April 2005 was 5.8 days. While a total of 68 countries hosted phishing sites in April 2005,[7] the United States was the most common geographic location with 26 percent of the active phishing sites being hosted in the United States, followed by China (22 percent), Korea (10 percent), and Japan (3 percent).

Defending Against Phishing

A U.S. Department of Justice special report[8] recommends a number of actions Internet users can take to protect themselves against phishing. For example, Internet users should not respond immediately to email messages requiring a quick response without first verifying the legitimacy of the message. Also, Internet users should examine claims made in email messages and evaluate whether they make sense (e.g., a bank would not ask its customers to provide their account numbers since it already has this information).

Allowing individuals to place a "security freeze" on their credit files can help phishing victims protect against the fraud typically associated with the theft of sensitive personal information. The security freeze prevents credit file information from being disclosed for the purpose of opening a new account without the explicit consent, through the use of a password, of the individual. Currently, four states have laws that permit residents to place a security freeze on their credit files,[9] and 20 other states proposed similar legislation during the 2005 legislative session.[10]

Summary

With an estimated 10 million consumers being victimized by identity theft each year,[11] phishing represents a rapidly growing problem, putting the personal information of Internet users at risk for identity theft. While Internet users can limit their chances of being victimized by not responding to suspicious email messages, phishers will continue to use new strategies, such as Instant Messaging and spyware, to lure additional victims into disclosing sensitive personal information. Therefore, consumers need additional defenses against these frauds, such as the option to impose a security freeze on credit file information.

Written by Neal Walters
AARP Public Policy Institute
601 E St., NW
Washington, DC 20049
202-434-3910; E-Mail ppi@aarp.org
June, 2005

[5] Krebs, B. "Despite Efforts to Contain Them, 'Phishing' Scams Spread." *Washington Post*, Jan. 19, 2005.
[6] APWG. "Phishing Activity Trends Report," April 29, 2005, http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf
[7] A host country is defined by the geographic location of the Web server maintaining the fraudulent site.
[8] U.S. Department of Justice. "Special Report on 'Phishing,'" March 2004, http://www.usdoj.gov/criminal/fraud/Phishing.pdf.
[9] California and Louisiana law allows individuals to proactively place a security freeze on their credit files**,** while Texas and Vermont law allows only individuals who are victims of identity theft to place a security freeze on their credit files.
[10] Krim, J. "States Scramble to Protect Data," *Washington Post*, April 9, 2005.
[11] Federal Trade Commission (FTC). *Identity Theft Survey Report*, Sept. 2003, http://www.ftc.gov/os/2003/09/synovatereport.pdf.

FACT SHEET