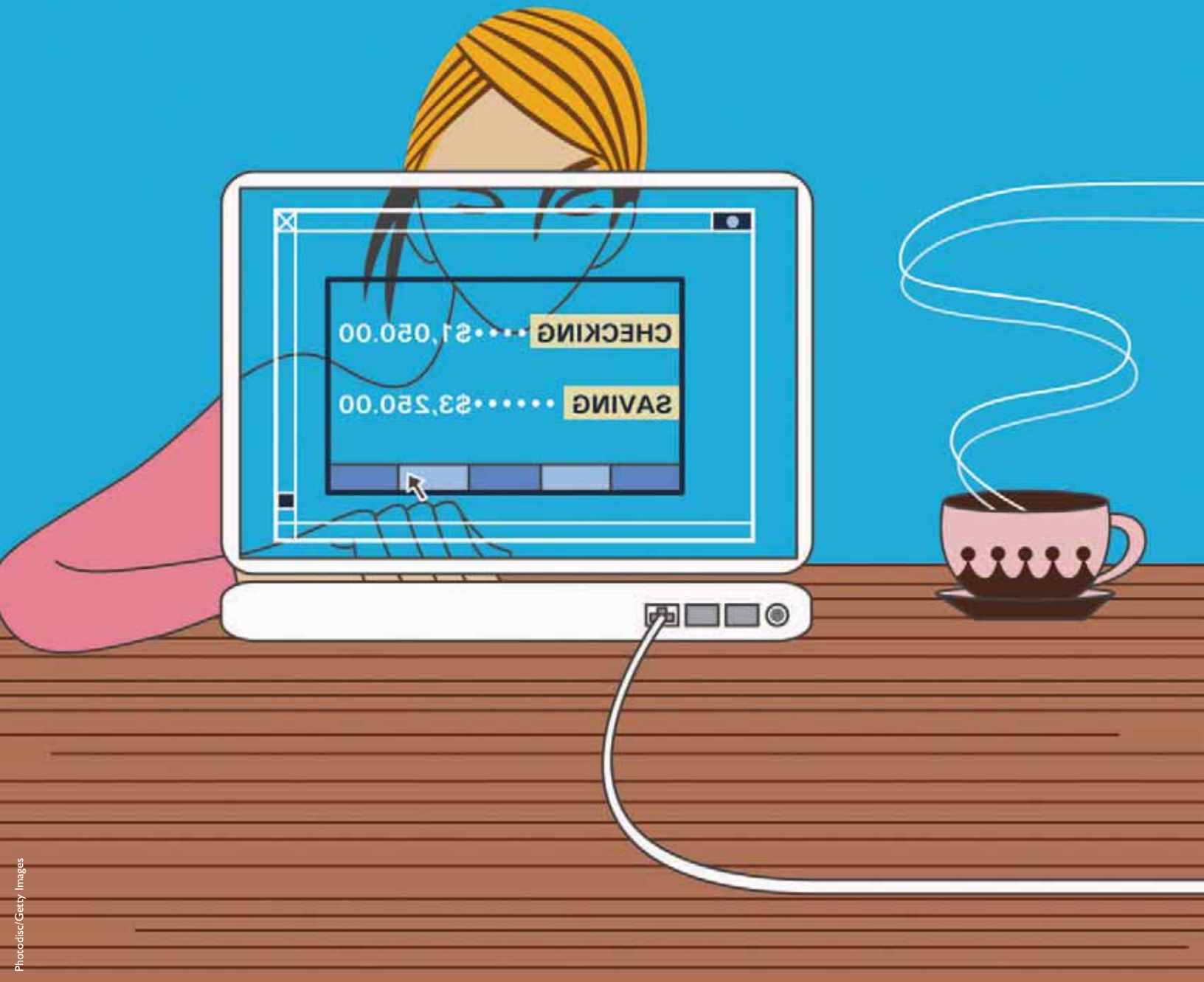
Phishing and Pharming:
Helping Consumers Avoid Internet Fraud

by Dawn Hicks
Federal Reserve Bank of Boston



Photodisc/Getty Images

Gone are the days when consumers had to step outside to purchase groceries, book flights and vacations, rent or purchase cars, or just transfer money between bank accounts. Today, they can simply grab their checkbooks, debit cards, or credit cards, sit down at a computer in the comfort and safety of their homes and complete such transactions with passwords and personal identification numbers, or PINs. Thanks to advances in technology, the types of transactions they can now complete online are seemingly endless.

Unfortunately, the increase in online transactions has been accompanied by an increase in online identity theft. Moreover, fraudulent access to personal information over the Internet is increasingly sophisticated. Two forms of identity theft, *phishing* and *pharming*, are at the forefront of this Internet piracy.

The Crimes

Phishing lures consumers into divulging their personal financial information to fraudulent web sites, also known as spoofed web sites. The phisher may send an unsuspecting victim an e-mail with a link to a fraudulent bank site. The e-mail instructs the recipient to click on the supposed bank's link to confirm personal account information. Often the message sounds plausible, describing a problem that feels serious to victims. To straighten out, say, a purported overdraft, trusting customers provide PIN numbers or passwords. The phisher can then use that personal data to clean out bank accounts or commit other identity theft

Pharming is more sophisticated. Pharmers also send e-mails. However, the consumer can be duped by the pharmer without clicking on a link or opening an attachment. Simply opening the e-mail message does the damage. The pharming e-mail message contains viruses, or Trojan horses, that install small software programs on the user's computer—a good reason to advise everyone to get antivirus software. The pharming e-mail installs the stealth application so that whenever the consumer tries to visit the official web site of an organization, the program redirects the browser to the pharmer's fake web site.[1] Thus, instead of going phishing for personal data by luring victims through a web link, the pharmer harvests information that the oblivious victim enters into the counterfeit web site.

And that's not all. The latest form of pharming doesn't even require e-mail. The Anti-Phishing Working Group (APWG) reports that password-stealing Trojan horses can attack through Microsoft Messenger using something called *keyloggers*. Keyloggers are viruses that track a user's keystrokes on

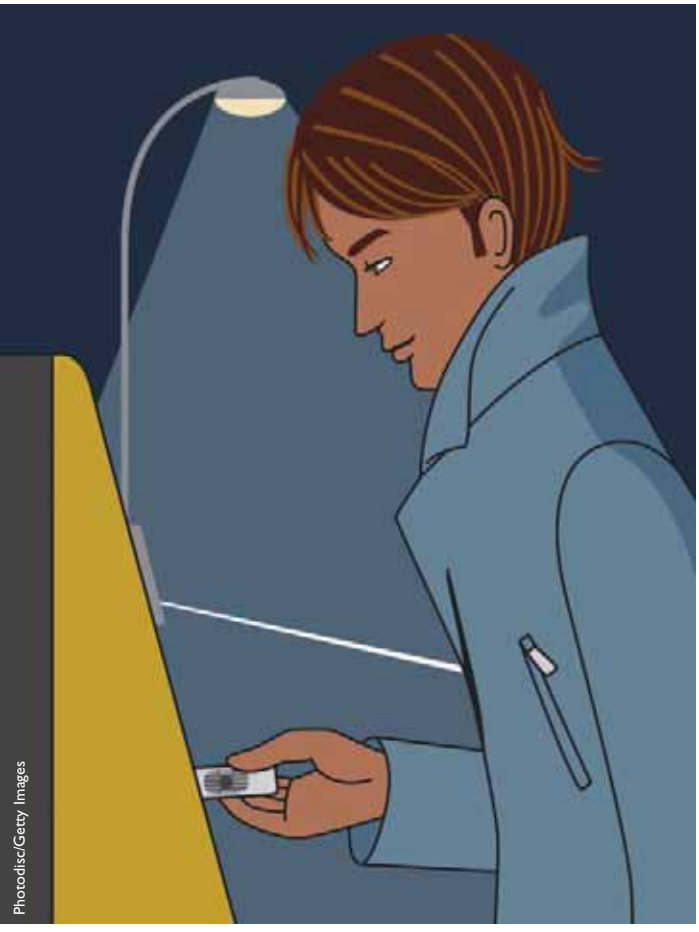
legitimate sites and steal passwords.[2] Victims who use the same password on many sites thus expose themselves to multiple frauds.

The Impact

The APWG estimates that phishing attacks grew by an average of 36 percent between July 2004 and October 2004. Between August 2004 and October 2004, the number of new and unique phishing e-mail messages more than tripled from 2,158 to 6,597.[3] The APWG also reports that the leading geographic location for phishers is the United States, with 32 percent of the world's phishing sites.[4]

As much as 81 percent of all phishing attempts made by January 2005 were targeted at customers of large financial institutions, although phishers prey on others as well.[5] Recent trends reveal that phishers also are targeting smaller financial institutions, such as community banks and credit unions. The smaller financial institutions tend to be more vulnerable to attacks because they have fewer resources to employ large security teams or implement effective security systems.

The financial loss to consumers and institutions can be tremendous. Gartner, Inc., a Stamford, Connecticut-based research and advisory firm, conducted a survey on phishing and identity theft in May 2005. The study revealed that 1.2 million Americans lost a total of $929 million in the previous year because of phishing.[6] And in his study "Phishing: A Growing Threat to Financial Institutions and E-Commerce," Frederick W. Stakelbeck, Jr., of Philadelphia's Federal Reserve Bank determined that a typical phishing attack can cost a financial institution between $50 and $60 per account compromised, or $50,000 per attack.[7] Those figures do not even cover the cost of time spent disabling the phishing sites, resetting legitimate user passwords, and installing software patches.



Photodisc/Getty Images

In advising consumers, advocates should be careful that their warnings do not cause anyone to overreact and give up online transactions. Exaggerated perceptions of threats can undermine customer convenience, as well as being damaging to financial organizations. A Forrester Research study reveals, for example, that 26 percent of consumers have elected not to apply for a financial product online; 20 percent decided not to open e-mail from their financial providers; and 19 percent would not enroll in online banking or bill payment.[8]

The Solution

Institutions are taking steps to protect customers from phishers and pharmers. In June 2005, Bank of America, for example, initiated SiteKey, a web site authentication service. The software makes it easier for users to determine when they are on the authentic Bank of America site.[9] Bank of America also implemented a personal digital-image system. The customer chooses a "secret image" for logging on to the web site, and if the secret image does not appear when he or she goes to an apparently authentic Bank of America site, it is a fake site.

Frederick Stakelbeck of the Federal Reserve Bank of Philadelphia determined that a typical phishing attack can cost a financial institution between $50 and $60 per account compromised, or $50,000 per attack.

Software companies also are taking steps to prevent Internet piracy. Microsoft recently announced that it is creating an "antiphishing" feature for Windows Internet Explorer 7, the next version of its browser. Users will be interrupted and warned if they attempt to visit a known phishing site.[10] In addition, antiphishing developers have new software that can collect and encrypt personal data and store it safely on the user's hard drive. When the user enters personal information in response to an unknown e-mailer or a mysterious pop-up box, the software will display an alert.[11]

Netcraft, www.netcraft.com, offers an antiphishing toolbar that also works for pharming. The software alerts users to the geographical location of the site they are accessing. Then if users attempt to visit their U.S. bank's web site and the software reveals that the site is actually originating from Ukraine, for example, they know they should contact the institution through recognized channels before divulging personal financial information.[12]

The U.S. Congress also is taking steps to protect Internet users. In his February 2005 introduction to the Anti-Phishing Act of 2005, Vermont Senator

Patrick Leahy said that the act would add two new laws to the U.S. Code. The first law would "prohibit the creation or procurement of a web site that represents itself to be that of a legitimate business, and that attempts to induce the victim to divulge personal information, with the intent to commit a crime of fraud or identity theft."[13] The second would prohibit "the creation or procurement of an e-mail that represents itself to be that of a legitimate business, and that attempts to induce the victim to divulge personal information, with the intent to commit a crime of fraud or identity theft."

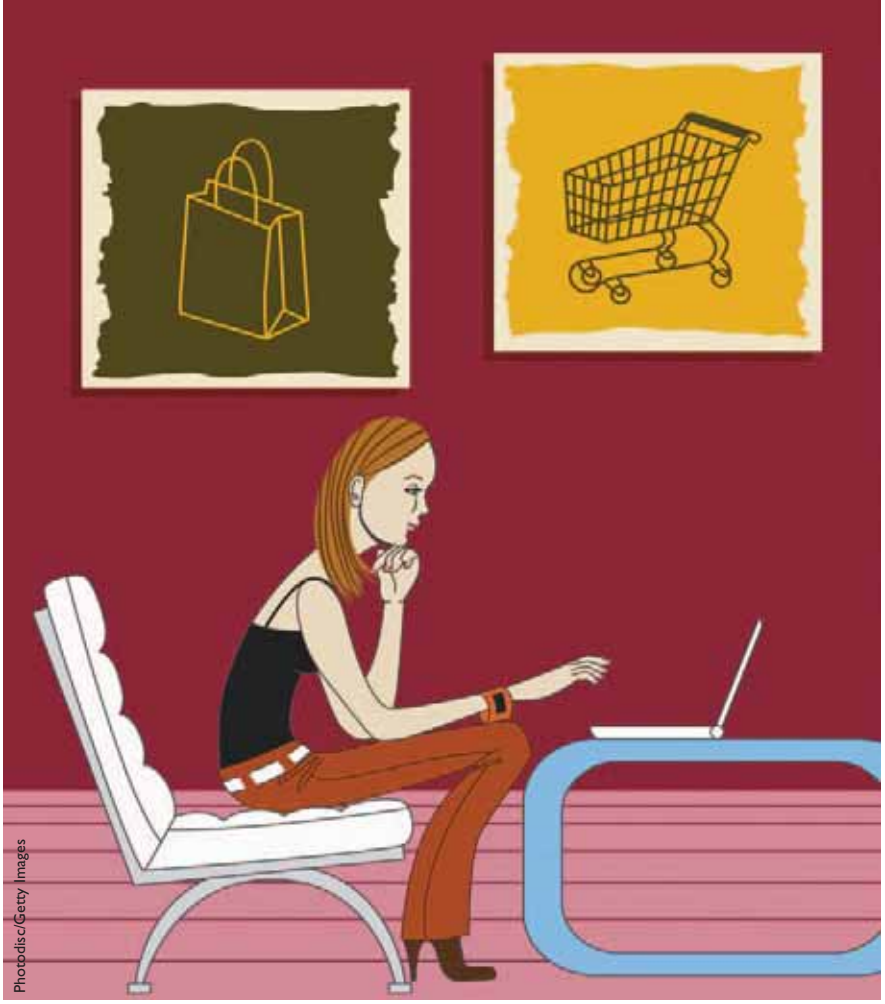
The fraudulent e-mail itself would be sufficient for prosecution, whereas under current law, phishers can be prosecuted only if the crime has taken place and been reported. Unfortunately, by that point, the thieves have already packed up their fake sites and moved on. The proposed legislation would help law enforcement entities to intervene sooner.

In the meantime, awareness is key. Consumer advocates might recommend the preventive measures listed on the APWG web site:

- Be suspicious of any e-mail with urgent requests for personal financial information;
- Do not use the links in an e-mail to get to any web page;
- Avoid completing forms in e-mail messages that ask for personal financial information;
- Be sure to use a secure web site when submitting credit card or other sensitive information via the web browser;
- Consider installing a web browser tool bar for protection from known phishing fraud web sites
- Regularly log on to online accounts;
- Regularly check bank, credit, and debit card statements to ensure all transactions are legitimate;
- Make sure the browser is up-to-date and security patches are applied.[14]

Advocates also might tell consumers that if they believe they are being targeted by phishing or pharming, they should notify the Internet Fraud Complaint Center of the FBI by filing a complaint at www.ifccfbi.gov. Alternatively, they may forward the entire suspect e-mail to one or more of these:

- reportphishing@antiphishing.com
- the Federal Trade Commission at spam@uce.gov
- the company that has been mis represented (for example, an e-mail purporting to be from eBay, should be forwarded to spoof@ebay.com)


Photodisc/Getty Images

Dawn Hicks *is a member of the Federal Reserve Bank of Boston's Consumer Regulation Outreach Group.*

Endnotes

[1] US Netizen, "A New Security Threat – Pharming" (2005), http://www.usnetizen.com/articles/pharming.html.

[2] Jane Larson, " 'Pharmers' hit online bank users with fraud scam," *The Arizona Republic*, April 26, 2005.

[3] John Leyden, "Phishers tapping botnets to automate attacks," *The Register*, November 2004, http://www.theregister.co.uk/2004/11/26/anti-phishing_report.

[4] Other top countries are China, 13 percent; Korea, 10 percent; Japan, 3.1 percent; Germany, 2.7 percent; Brazil, 2.7 percent; Romania, 2.2 percent; Canada, 2.1 percent; France, 2.7 percent; and Australia, 2.1 percent.

[5] See NW3C: National White Collar Crime Center, http://www.nw3c.org/.

[6] Gregg Keizer, "Phishing costs nearly $1 billion," *TechWeb News*, June 24, 2005.

[7] Frederick W. Stakelbeck, Jr., "Phishing: A growing threat to financial institutions and e-commerce," *SRC Insights*, fall 2004.

[8] Paul Gibler, "Phishing, pharming, spimming, and spoofing," *Credit Union Executive Newsletter*, April 18, 2005, p. 7.

[9] Cameron Sturdevant, "Spam tools take on anti-fraud chores," *eWeek*, June 20, 2005, http://www.eweek.com.

[10] Ina Fried, "Microsoft MSN offers scam-site detector," *ZDNet News*, August 25, 2005, http://news.zdnet.com/2100-1009_22-5843325.html.

[11] Paul L. Kerstein, "How can we stop phishing and pharming scams?" *CSO Update*, July 19, 2005, http://www.csoonline.com/talkback/071905.html.

[12] Amanda C. Kooser, "Pharm's way: Learn how to protect yourself from the latest Internet attack," *Entrepreneur*, July 2005, p. 22.

13 Patrick Leahy, "Statement of Senator Patrick Leahy: Introduction of the anti-phishing act of 2005," February 28, 2005.

14 For more information, visit www.antiphishing.org/consumer_recs.html.