

Phishing, Pharming, Spimming, and Spoofing

Online crooks are impersonating businesses and deluding consumers with e-mails, messages, and worms with the intent to steal identities and account information. Fifty percent of account holders have received at least one phishing e-mail—a 100% increase from last April, says the annual “Financial Institution Online Fraud Survey” by Cyota, New York.

February saw 2,625 phishing attacks—a 26% monthly growth rate since July, reports the Anti-Phishing Working Group, Redwood City, Calif., (antiphishing.org).

Other identity theft threats have joined phishing attacks. “Spimming” is instant message spam phishing for account information. “Pharming” employs technologies such as worms or Trojans to attack a browser’s address bar. When users type a valid Web address, they’re redirected to a “spoofed” site mimicking the original site, report *eWeek* magazine and the Anti-Phishing Working Group. Also, spyware secretly installs password-stealing Trojan horses on computers to capture and report passwords.

The growth of these threats is changing consumers’ financial behavior online. Forrester Research reports 26% of consumers have elected not to apply for a financial product online, 20% not to open e-mails from their financial providers, 19% not to enroll in online banking or bill pay, and 14% not to use online banking or bill pay.

You need a proactive plan for addressing these threats, countering them by educating members, routinely monitoring your Web site, and enhancing your security services. Among member education strategies:

- **Educate** members about the importance of verifying the security certificate associated with secure Web pages. They can find these by clicking on the security symbol (the small lock) located in the footer of the secured site page. Phishers won’t have legitimate certificates.

- **Ask** members to download a browser tool bar displaying information about the visited site—where it’s hosted, the Internet address, whether others have flagged it as a scam site. Netcraft, based in Bath, England, (news.netcraft.com) provides one such service.

Also, consider enhancing your log-on and authentication process and systems for online member service by using a

two-step or multifactor authentication system. That requires a password and some other identifying factor such as a biometric confirmation or a unique code. The Federal Deposit Insurance Corp. recommends this as part of its Financial Institution Advisory Letter (FIL-132-2004), issued Dec. 14, 2004.

Addressing e-mail fraud risks in Letter No. 04-CU-06, the National Credit Union Administration also suggests improving authentication measures.

Vendors are developing systems and programs to help credit unions accomplish this. Among these are SecurID from RSA Security, Bedford, Mass., a device generating a random set of numbers members would enter during the authentication process, or Identity Guard from Entrust, Addison, Texas, that provides consumers with a printed random numeric grid. When they log on to a site using this system, they’re asked to supply numbers from the grid to authenticate their accounts, reports *Business Week*.

Consider these strategies to manage risks associated with new threats:

- **Monitor** your Web logs for system intrusions that could indicate identity theft attempts—for example, requests for images stored on your servers.
- **Consider** working with an antiphishing service provider such as Corillian Corp., Hillsboro, Ore., or Cyota. Corillian serves about 20 financial institutions with its Fraud Detection System, reports the *Washington Post*. One of them is BECU (formerly Boeing Employees Credit Union), Tukwila, Wash. Cyota offers FraudAction to combat phishing.
- **Monitor** the work of the Anti-Phishing Working Group, the newly formed Anti-Fraud Alliance (antifraudalliance.com) and the Financial Services Information Sharing and Analysis Center (fsisac.com) for warnings and recommendations.
- **Consider** a service such as Name Protect (nameprotect.com) or MarkMonitor (markmonitor.com) to make sure you’re monitoring any possible spoofing or phishing of your credit union site.
- **Notify** the Anti-Phishing Working Group if your credit union experiences a phishing attack.

As you review your plans to protect members and reinforce your credit union’s strong brand, remember identity theft is pervasive and must be fought with a range of technology, education, and networking activities. ■

© 2005, Paul Gibler, principal consultant and e-marketing strategist, ConnectingDots, Madison, Wis. Reach him at 608-255-4092 or at pgibler@connectingdots.com.

