Gone Phishing

Fraudsters troll for member IDs.

Roy W. Urrico

This isn't about Opie and Andy angling at the local pond in Mayberry. No, this phishing isn't even spelled the same way. But its objective is the same: Bait a line and tempt unwary victims. Here the lure is e-mail that tries to convince recipients to reveal vital personal information.

More than 75% of the 300-plus (and growing) phishing e-mails sent out weekly target financial institution customers.

Why is there concern? Compromised credit unions face operational and legal liabilities as well as intangible costs, such as reputation damage, arising from any fraudulent use of member information.

Focus

- **From March through June,** the number of reported phishing attacks on financial institutions grew from 256 to 1,099.
- **Ninety-five percent** of phishing expeditions use spoofing, in which e-mail recipients receive bogus messages from familiar companies.
- **Eight CUs** were among five pages of spoofed financial institution sites linked to a bogus Russian Web site.

While there are many types of fraudulent e-mail schemes, phishing is the most prevalent today and a catchphrase for all. "These types of attacks are from a small amount of very motivated people looking to steal money," says Vincent Weafer, senior director of Symantec Security Response, Cupertino, Calif.

"Financial institutions are the No. 1 target because that's where the money is," points out Mark Rasch, chief security counsel for managed security services provider Solutionary, Omaha, Neb.

According to the Cambridge, Mass., Anti-Phishing Working Group—an industry consortium of financial institutions and vendors formed by Tumbleweed Communications, Redwood City, Calif.—the number of unique phishing attacks in June 2004 was 1,422 (most recent data available). The business sector most targeted: financial services. From March through June, the number of reported phishing attacks on financial institutions increased from 256 to 1,099.

Mark Rasch

Most of the fraudulent messages end up in the trash. Unfortunately, however, an estimated 5% of recipients respond, reports the working group. Gartner, Stamford, Conn., says about 1.78 million adults report giving phishers their financial or personal information. The research firm estimates the resulting identity theft cost U.S. financial institutions and credit card issuers about $1.2 billion last year.

"Phishing is a big concern for all types of financial institutions, especially those offering credit cards," says Brian Warfel, senior vice president/sales and service for Power 1 Credit Union, Pembroke Pines, Fla. He's also secretary/treasurer of the CUNA Technology Council and a member of Washington, D.C.-based BITS Internet Working Group. BITS is the technology group of the Financial Services Roundtable, and the Credit Union National Association is the only credit union trade group represented on it.

Warfel says e-mail fraud has been a major topic of discussion for the BITS Internet Fraud Task Force and its e-scams subcommittee.

Phishing for sitting ducks

"Phishing is the perfect crime. It's easy to deploy, the risk is very low, and there are high rewards," says Naftali Bennett, CEO of Cyota, New York.

Naftali Bennett

Fraudsters employ many different tactics, but the Anti-Phishing Working Group says 92% of phishing expeditions use spoofing, in which e-mail recipients receive bogus messages from familiar companies. The messages ask recipients to update personal information at a Web site that's conveniently hyperlinked. "It looks like, smells like, feels like a real e-mail," says Jahan Moreh, chief security architect, Sigaba, San Mateo, Calif. In reality, the Web site is just a facsimile.

Jahan Moreh

The phony Web site is set up to collect either the log-on information or enough personal information to perpetrate identity theft. The schemes try to dupe recipients into divulging anything—account and/or Social Security numbers, usernames, and passwords—that would allow the phishers to misrepresent themselves as the conned addressee. "Most of these play on greed or fear," maintains Bill Calpin, CEO of Digital Envoy, Atlanta.

Bill Calpin

Some phishing attacks are more obvious because they contain substandard graphics or spelling and grammatical mistakes. But, Bennett warns, "phishing is growing in quantity and quality."

Many phishing attacks occur from nomadic Web sites abroad, so catching the perpetrators is difficult. "They literally can bring up and take down the site within 24 to 48 hours," says Moreh.

There are other e-mail fraud variations, though fewer in number, that try to take advantage of people by using social engineering, explains Barry Thompson, financial institution security expert and trainer, the Thompson Group, Oswego, N.Y.

Barry Thompson

These social-engineered e-mail frauds mimic variations of proven fax, phone, and direct mail ruses. They try to sucker individuals into giving out information by earning their trust. These sometimes involve sweepstakes winnings that the addressee will "receive" once they have supplied their Social Security and/or financial institution account number. Some even involve paying an up-front fee. "No one is going to charge you a fee if you've won," advises Thompson.

"We continue to educate credit unions on the types of attacks we're seeing," says Ann Davidson, credit union protection product expert for CUNA Mutual Group, Madison, Wis.

However, fraud variations continue to evolve. "In time, phishing will expand. These attacks are getting very sophisticated," says Weafer.

Some hackers already surreptitiously install key logger programs on personal computers using popular Internet access and e-mail programs. The spyware then monitors every keystroke to learn personal identification numbers, passwords, and account information.

With access to this information, says Mark Goines, chief marketing officer of PassMark Security, Palo Alto, Calif., the swindlers could add themselves to a payee list, create an account un-

Phishing Facts*

No. of unique phishing attacks reported	1,422
Avg. monthly growth rate in attacks	52%
Organization most targeted	Citibank (492)
Percentage of attacks using spoofed e-mail addresses	92%
Country hosting the most phishing Web sites	U.S. (27%)
Avg. lifespan of a phishing site	2.25 days

*For June 2004

Source: Phishing Attacks Trends Report, June 2004, from the Anti-Phishing Working Group

der the identity theft victim's name, access information about a credit or debit card, request a new card, or go on a spending spree.

Discerning threats to CUs

"Many times phishing targets big money financial institutions [Citibank reportedly was besieged 492 times in June alone] because phishers need to fashion a wide—almost generic—net," explains Dan Maier, communications director for the Anti-Phishing Working Group and senior product manager at e-mail security company Tumbleweed. For the most part, he adds, only 50 or 60 financial institutions are really under fire—for now.

Although credit unions have remained under the radar of phishing attacks, that anonymity may be fleeting. "We are anticipating 'spear-phishing attacks' if scammers get ahold of targeted mailing lists," says Maier. He warns that credit unions need to maintain extra strong security about member information, or they will see scams directed at specific members.

Ann Davidson

"From the fraudster perspective, larger financial institutions make more sense. They buy a spam list, throw it against the wall, and see what sticks," observes Bennett. "However, what we've been seeing is that fraud goes to the weakest link," those without antifraud measures.

Credit unions may be experiencing the first onslaught:

▶ **Davidson reports** that in April CUNA Mutual learned eight credit unions were among five pages of spoofed financial institution sites linked to a bogus Russian Web site. None of the eight knew of the phony sites until CUNA Mutual notified them.

▶ **The Federal Bureau of Investigation's** Internet Fraud Complaint Center reports a steady increase in complaints involving unsolicited e-mails pointing members to false Web sites or directly asking for member information, according to the National Credit Union Administration (NCUA).

NCUA recently released two letters (letter Nos. 04-CU-05 and 04-CU-06) warning about the risks and possible fallout if credit union members fall victim to phishing schemes. It could result in membership decline, a loss in confidence, or costly litigation if members perceive that security breaches led to misappropriation of confidential information.

Mark Goines

Even if credit unions aren't obligated to reimburse defrauded members, "most institutions globally have been protecting their customers, regardless of whether they're liable," points out Goines.

Another danger lurks on a broader scale. It erodes the confidence of consumers in the online channel, indicates Calpin. "The defense mechanism is that everything must be fake, and that's a problem."

A Cyota survey shows that 75% of accountholders are less likely to respond to e-mail from their financial institutions—and more than 65% said they were less likely to sign up or continue to use their online financial institution services—due to phishing qualms.

If members distrust e-mail from credit unions, attempts to cross-promote products and services are lost, emphasizes Rasch. Losing the online channel could drive members back to the branches, thereby increasing operational costs, says Goines. Communicating to members what a legitimate message is, adds Weafer, could pre-empt any problems and prevent the online marketing channel from also becoming a fraud victim.

Protecting members

It's credit unions' responsibility to educate members about phishing and to respond to its threat, advises Davidson. (Educational Risk Alert is a value-added benefit provided to CUNA Mutual bond policyholders. It addresses what the issue is and what action the credit union can take to help minimize its exposure.)

"The credit union industry has done a pretty good job of keeping members educated," says Warfel. "We run a fine line between educating consumers and sending them into a panic." He explains that Power 1 tells its members "to *never* release any personal information to any party unless they're setting up a new account or updating their information in person with a known representative of the company." In addition to educating members, Power 1 also has extensive security protection devices in place for its data networks.

More education would help assuage consumer concerns, according to the Cyota survey, which indicated most accountholders (67%) hadn't received any communication about phishing. However, 91% of accountholders believe communication about phishing is helpful.

"All employees should be trained to recognize the various electronic fraud schemes so if one is reported, the situation can be elevated quickly to be resolved," explains Warfel. "An educated employee who catches a scheme in its infancy can save the organization a lot of time and trouble."

Power 1 conducts mandatory security training each year and updates employees about new schemes as soon as they break.

Identifying best practices

NCUA recommends credit unions:

▶ **Improve authentication** methods and procedures for members to identify themselves to the credit union as well as for the credit union to identify itself to members;

▶ **Review protections** of confidential credit union member data;

▶ **Describe to members** how they can authenticate the credit union's site by clicking on the Web site certificate logo (for example, the lock symbol at the bottom of a secured site's Web page) and viewing the name of the holder of the digital certificate;

▶ **Search the Internet** for variations of the credit union's Web site;

▶ **Monitor accounts** for unusual activity;

▶ **Encourage members** to report suspicious e-mails by establishing a toll-free telephone number; and

▶ **Train member service representatives** to refer member concerns to the security staff.

Thompson also suggests having member programs that cover identify theft, phishing, and spamming, and recommends placing security information and tips online.

Other beneficial practices, suggests Bennett, include preparing fraud contingency plans, creating a relationship with law enforcement prior to an incident, "defining ownership" of the phishing problem within the credit union, and creating an antifraud task force.

Getting help from technology

Authentication will be used to combat fraud and secure the growing phishing problem, forecasts Davidson.

Authentication also must be mutual. "All authentication schemes used to be one-way 'how do I know you're a member of the credit union?'" points out Rasch. Now it needs to be two ways because members also are asking the credit union for its ID.

Products and services can help:

▶ **Cyota FraudAction** is a modular service that provides real-time phishing detection, a risk assessment for each incident, technical countermeasures, post-mortem attack analysis, and a hosted Web-based application service provider module designed to educate accountholders.

▶ **PassMark Security** authenticates messages by using a personalized image called a PassMark. When members log on to a credit union's Web site, they see a personalized image they have preselected. Because a bogus Web site won't

RESOURCES

▶ Anti-Phishing Working Group, Cambridge, Mass.: e-mail *info@antiphishing.org* or visit *antiphishing.org.*

▶ Credit Union National Association:

1. ID theft resources: *cuna.org/initiatives/idtheft.html.*
2. "Spoofing, Spamming, and Phishing" cassette: *buy.cuna.org/detail.php? sku=25826*

▶ CUNA Mutual Group, Madison, Wis.: 800-637-2676.

▶ Cyota, New York: 212-977-5402 or *cyota.com.*

▶ Digital Envoy, Atlanta: 877-201-3593 or *digitalenvoy.net.*

▶ PassMark Security, Woodside, Calif.: 650-599-0350 or *www.passmarksecurity.com.*

▶ Sigaba, San Mateo, Calif.: 800-475-8226 or *sigaba.com.*

▶ Solutionary, Omaha, Neb.: 866-333-2133 or *solutionary.com.*

▶ Symantec Security Response, Symantec Corp., Cupertino, Calif.: 408-517-8000 or *securityresponse.symantec.com.*

▶ Thompson Consulting Group, Oswego, N.Y.: 315-342-5931 or *tgrouponline.com.*

know the PassMark, members will know whether it's safe to enter a password. The system also won't ask for a password if it doesn't recognize the member.

▶ **Digital Envoy's IP Inspector Fraud Analyst** reveals more than a dozen Internet-protocol data elements (including location, anonymous proxies, domain name, and other identifiable attributes) and analyzes the data to detect potential online fraud.

▶ **Sigaba Secure Email** uses a core gateway component allowing administrators to implement a configurable set of policies to manage e-mail encryption and decryption. It also performs content filtering, virus scanning, auditing, and message control.

▶ **Solutionary's offerings** use ActiveGuard software, the company's security system, which is designed to offer 24/7 monitoring of networks and systems for changes and vulnerabilities, and initiate protective actions when it detects security risks. It's critical to monitor and respond to threats because if phishers access the credit union's systems, they could obtain a legitimate e-mail list or user password list and target individuals.

▶ **Symantec Mail Security** integrates virus protection, spam prevention, and e-mail content enforcement in an around-the-clock monitoring system.

Obtaining other assistance

"Once consumers give their information, the game is over. They're conned," warns Moreh. There's no easy recourse for identity theft victims other than the painful, painstaking process of reporting the theft as quickly as possible to the credit union, credit bureaus, and credit card companies; reviewing their financial records; changing passwords; and closing accounts.

Hoping to ease the burden, BITS launched the Identity Theft Victim Assistance Center in October 2003 so fraud victims need only to notify their primary financial institution, which then sends details to the center. The center then contacts all other financial institutions and arranges to get credit reports.

Prevention, however, still is the best strategy. That's why the Financial Services Technology Consortium, New York, plans an initiative to address phishing. (The 11-year-old organization includes financial institutions, technology vendors, independent research organizations, and government agencies and exists to bring forward, test, prove, and validate new financial services technologies.) The consortium's focus includes investigating and defining counter-phishing technical solutions, and determining their infrastructure fit, requirements, and impact when deployed.

Phishing won't end e-mail as a medium. The key is to keep up with those phishing for your members.

Meanwhile, the Texas Credit Union League has joined with other statewide institutions and law enforcement agencies in the Loss Avoidance Alert System, a network that provides timely alerts and postings of fraudulent activities.

"The main reason we joined was to have a system so members could be aware of fraud," says John Walker, director of marketing for the Texas League, which represents more than 600 of the state's credit unions and 6.8 million members. "It's a benefit for members that doesn't cost anything besides their dues," explains Walker.

Thompson, for one, believes the industry is moving in the right direction. "Phishing won't end e-mail as a medium," he says, adding that better means of dealing with e-mail fraud will mitigate the problem. The key is to keep up with those phishing for your members. ●

For more information about phishing, visit
CREDITUNIONmagazine.com