Tackling Phishing

Rebecca Wetzel

It's a never-ending struggle, but the anti-fraud arsenal continues to grow.

"Technology is," as security expert Chuck Wade of Interisle Group said, "the rising tide that lifts all ships—including pirate ships," and in this case phishing boats. Phishing is here to stay.

This 21st century fraud combines deception (aka social engineering), impersonation, and automation to steal authentication credentials such as passwords and account numbers from individuals over the Internet, and uses this information for ill gain. You've doubtless seen emails purporting to be from a credit card company or bank, which actually are ploys to steal account information. Initially these emails were easy to spot because they contained typos and other telltale signs, but now even savvy users can be duped, and fraudsters are expanding beyond email, to pounce via the Web, instant messaging, chat rooms, interactive games and malware like keyboard logging programs that capture passwords entered into legitimate sites. Although fending off phishing is a challenge, countermeasures are available, with more on the way.

The Rising Cost Of Phishing

Phishing costs victims and financial institutions money and time. Victims must correct credit records and repair other phishing-related damage, while financial institutions must absorb customer losses, as well as costs from issuing new credit cards, answering calls and shutting down fraudulent websites.

For financial institutions, of even graver concern than direct costs is the erosion of trust in online communications and transactions. Suspicion of legitimate online interactions between customers and their financial institutions is driving consumers from online banking to more expensive and labor-intensive channels such as telephone call centers or "bricks and mortar" branch offices.

An April 2004 survey of 650 U.S. banking customers by software vendor Cyota shows that phishing is diminishing customer's trust in online interactions with their banks. In the study, 65 percent of account holders were less likely to use their bank's online services due to phishing, and 75 percent were less likely to respond to email from their bank because of phishing.

Estimated losses due to phishing vary. Gartner puts total U.S. phishing-related losses during 2003 at some $1.2 billion, whereas a study by the Ponemon Institute estimates total consumer losses as of September 2004 at $500 million per year, and a study by Financial Insights expects 2004 losses to tally as high as $400 million.

Whatever the actual losses, the problem is serious and worsening. Seven out of 10 Internet users surveyed by the Ponemon Institute reported that they had unintentionally visited a spoofed website, and more than 15 percent admitted to providing sensitive private information including credit card numbers, checking account information and social security numbers. Of those, about 2 percent believed they lost money as a result of phishing.

Anatomy Of Phishing

To help dissect the problem of phishing and provide a common language to describe attacks and countermeasures, the Financial Services Technology Consortium (FSTC) recently developed a taxonomy of phishing attacks (Figure 1). This taxonomy helps make sense of the complex nature of the problem by mapping out a common attack life cycle, and a predictable set of activities attackers engage in within each life cycle phase.

It is important to note that phishing does not include credential theft from databases or via non-electronic means, so those activities are not included in the taxonomy, even though they may result in similar patterns of financial fraud.

During the initial planning phase, the attacker decides whom to attack, what to steal, how to steal it, and what ruse to use. During the setup phase, the attacker creates attack mechanisms, and in the attack phase makes contact with prospective victims. This contact aims to lure people into taking actions that allow the attacker to steal credentials during the collection phase.

Next, during the fraud phase, the attacker sells, trades or directly uses the stolen credentials for

Rebecca Wetzel is an Internet industry analyst, consultant and writer. She is president of Wetzel Consulting LLC, and she is an associate with NetForecast, an Internet technology and market analysis firm, as well as technology consulting firm Interisle Group. She can be reached at rwetzel@rwetzel.com

FIGURE 1 Phishing Attack Taxonomy

Planning	Setup	Attack	Collection	Fraud	Post-Attack
Determine Target Firm	Create Materials	Attack via website	Collect via Web Form	Phisher Uses Credentials	Shut Down Attack Machinery
Determine Target Victim	Set Up Destinations	Attack via email	Collect via email Response	Credential Trafficking	Destroy Evidence
Determine Target Credentials	Obtain Contact Info	Attack via IM	Collect via IM Response	Credentials Used In Second-Stage Attack	Track Hunters
Determine Ruse	Set Up Attack Machinery	Attack via Phone Auto Dialer	Collect via Phone Response	Money Laundering	Assess Effectiveness
Determine Attack Method		Attack via Chat Room	Malware Sends Credentials	False Registrations	Launder Proceeds
Determine Fraud Objective		Attack via Bulletin Board			
		Attack via Newsgroup			
		Attack via Malware			

Source: Financial Industry Technology Consortium

fraudulent purposes. Following that, in the post attack phase, attackers deactivate the attack mechanisms, cover their tracks, assess the attack's "success," monitor attack responses and apply lessons learned to planning the next attack.

A sample attack might unfold like this: An attacker sets out to steal credit card information from customers of Bank "Y" by sending email containing the ruse that the customer's credit card has been compromised and will be cancelled unless he or she acts immediately to correct the situation. Concerned customers click on a link in the email which takes them to a spoofed website, where they enter their credit card number, PIN and other information. The attacker collects and sells this information to a third party, then dismantles the website, destroys evidence, monitors efforts to catch him, assesses the attack's effectiveness, and applies lessons learned to subsequent attacks.

What Can Be Done About Phishing?

The fact that the phishing attack life cycle consists of many phases, each encompassing a diverse and changeable set of activities, makes phishing a kaleidoscopic problem for which no single solution can suffice. Multiple solutions are called for, and the earlier in the life cycle an attack can be countered, the better the outcome for targeted victims and financial institutions.

It is good news, therefore, that a flurry of entrepreneurial activity is currently focused on developing a broad spectrum of nostrums to apply to the phishing problem early in the attack life cycle. Among the technologies promising some immediate relief are: better mutual authentication; spam filtering; detecting infringed domain names; and alerting consumers when they are being directed to fake websites.

■ **Better Mutual Authentication:** Because impersonation is a prerequisite to successful phishing attacks, better mutual authentication between a financial institution and its customers is an essential weapon. Effective authentication of a financial institution's identity helps prevent attackers from successfully impersonating a bank or credit card company in the attack and collection phases, and better customer authentication can keep attackers from successfully impersonating customers in the fraud phase.

Email sender authentication schemes help identify attempts by fraudsters to impersonate a financial institution in phishing emails during the

Spam filters can also catch phishing emails in their nets

attack phase. The idea behind authenticated email is to validate the source of the email, so a recipient can be assured that the email is from who it says it is and not a scam artist. Email authentication schemes take a number of forms. Two standards for email sending address authentication are in the works, the Sender Policy Framework (SPF) and the Microsoft-sponsored Caller-ID, but it will be some time before these or their counterparts are implemented.

In the meantime, proprietary solutions exist. For example, Goodmail provides an email stamping service that gives accredited volume senders premium delivery of legitimate mailings. Email stamped messages are allowed to bypass spam filters and are distinctly labeled in a user's inbox so a recipient can recognize them as from legitimate senders. SafeScrypt, on the other hand, provides tools that encrypt an email message as an attached file, and then the entire mail is digitally signed using a certificate issued by a valid certification authority. Recipients can verify the authenticity of the mail by verifying the signature.

A number of solutions are being applied to the problem of criminals impersonating customers during the fraud phase. In this phase, criminals routinely impersonate the customer of a financial institution to steal from the customer's account via the Web, or to open a new electronic account using the customer's identity. Countermeasures to this customer impersonation include physical factor authentication solutions from the likes of RSA, Entrust, ShareCube and Vasco Data Security; digital certificates from such firms as Verisign and GeoTrust; and biometric identification techniques like finger scanning, face geometry, hand/finger geometry, iris recognition, signature verification, voice verification and keystroke dynamics.

BioPassword uses keystroke dynamics to identify users by the way they type. The user types a user name and password. The user name, password, and the user's typing sample is compared to a sample already on file to authenticate the user.

In a rather unorthodox authentication approach, 41st Parameter performs dozens of verification checks on the customer's computer operating system (e.g. checks of local time, time zone and IP address) and compares the visitor's operating system “DNA” profile to a profile on file.

PassMark, Real User, and Bharosa offer authentication schemes using personalized images. These schemes can help customers to authenticate interactions with financial institutions, and can help financial institutions authenticate customers. PassMark users adopt a personal PassMark consisting of a picture and a text phrase. When asked for sensitive information, the user is first shown his or her unique PassMark to validate the communication. Similarly, Real User randomly assigns human faces to serve as a user's “Passfaces.” The user is presented decoy faces and Passfaces, and authentication succeeds when the user correctly identifies all Passfaces. Bharosa's users manipulate images in specific ways known only to the user and their financial insitution.

■ **Spam Filtering:** At least for now, email is the most common phishing attack vector, and spam filtering from the likes of Digital Envoy, Envisional, Ironport, McAfee, Postini, Symantec (formerly Brightmail), and Tumbleweed can prevent phishing emails from being delivered. Successful filtering of phishing emails can prevent fraudsters from making contact with target victims in the attack phase.

Most spam-filtering vendors detect phishing emails as a by-product of general spam filtering, but several specifically address phishing emails. Symantec, for example, uses its Brightmail probe network and decoy accounts to attract suspicious email, which Symantec then delivers to researchers who analyze the messages and identify fraud attacks. Symantec then creates and automatically deploys anti-fraud filters to block the phishing emails. Every four minutes, Symantec distributes (to ISPs) updated fraud filters which tag or block phishing emails, and when an email-borne phishing attack is detected, Symantec sends subscribing financial institutions an alert that the attack is under way and provides the attacker's source IP addresses.

Digital Envoy's email server software compares email headers and embedded URLs to information in a database containing information about country black lists, country “white lists,” etc. and assigns a score based on phishing suspicion level. If an email is scored as suspicious, it is moved to a quarantine folder and a descriptive message is added to the subject line, which is sent to the user.

In another approach, Envisional seeds email addresses in public locations such as newsgroups, guest books, bulletin boards and other sites, to be harvested by spammers. The emails received by these honeypot accounts are examined by Envisional's software to determine which ones are likely to be phishing attempts, and this information can then be used to filter phishing emails.

■ **Infringing Domain Name Detection:** Attackers often use domain names which mimic legitimate domain names. By detecting registration of infringing domain names, financial institutions can detect phishing websites during the setup phase of the phishing attack life cycle, and can work with law enforcement agencies and others to remove the sites from the network.

A VeriSign service scans websites, Usenet newsgroups and chat groups for brand infringement and traffic diversion. Another firm, Internet Identity, monitors brand names used in Internet domains, prioritizes and resolves domain-related problems, and continually monitors the domain space for unauthorized uses of a company's brand. A similar service from NameProtect monitors use of brand names in Internet domains, email, images, Usenet, IRC, auctions and search engines.

The service reports findings and provides tools for taking action against attackers.

■ **Phishing Website Detection:** Technologies from Billeo, EarthLink, Geotrust, Netcraft, PhishFree, Collective Trust, Webroot Software and WholeSecurity alert customers during the collection phase, when target victims are visiting a bogus website.

Billeo provides a browser plug-in with a "traffic light" in the toolbar that turns from green to yellow to red when a user visits a suspicious site. The plug-in compares the URL and Web page with a repository of known phishing sites, and applies a scoring mechanism to determine the site's alert level. Once a threshold alert level is reached, the traffic light turns red, and the tool prevents the user from entering information on that site. GeoTrust's browser-based tool notifies users when they are visiting a spoofed website, and rates a website's ability to allow users to provide confidential information securely.

WholeSecurity's browser-based tool detects phishing sites by examining URLs, content, text, layout and other aspects of a website; the tool then aims to determine whether a site is suspicious by combining the results of all tests.

■ **Phishing Solution Packages:** Some firms, including Corillian, Cyota, Cyveillance and MarkMonitor, offer comprehensive service packages that can combat phishing attacks at multiple points in the phishing attack life cycle.

Corillian searches for phishing sites under construction by analyzing bank Web servers' log activity using a complex set of parsing rules, and Corillian's software provides information to deactivate phishing sites before they go live. Setup activity is detectable because phishing sites are often built using legitimate site elements, which are retrieved from the bank's bona fide website. Should phishing sites slip through the cracks and go live, Corillian identifies visitors so financial institutions can identify compromised accounts and notify account holders, and it also collects evidence to find and prosecute attackers.

Cyota helps firms prepare for, respond to, and "clean up" after phishing attacks. Cyota detects phishing attacks using a probe network and other sources. Then, using statistical analysis, behavior models and other utilities, Cyota's staff evaluates each attack, estimates its severity, and works with ISPs and law enforcement on the bank's behalf to stop the attack and shut down phishing websites. Cyota then conducts forensic analysis to gather additional information, and works with law enforcement to catch attackers. Cyota also provides tools that help reduce attack risks, minimize impact, and deter future attacks.

Cyveillance checks domain registries for infringing domain names, and it detects and works to shut phishing sites. Cyveillance deploys Web crawling technology that takes 21 days to cycle through the entire Internet to detect illicit uses of its clients' brand names, and it monitors spam through its own trapping filters and through relationships with third-party spam filtering companies. Cyveillance also monitors for stolen credit card and/or personal information trafficking.

Lastly, the Internet Crime Prevention and Control Institute (ICPCI) is a private membership-based organization which takes preemptive actions against phishing attacks. The ICPCI operates an Internet Crime First Response Center which analyzes, coordinates and communicates with an array of third-party organizations to stop phishing attacks. It boasts a response time of five minutes from phishing attack detection to actions such as taking down a phishing website.

Counter-phishing will require ongoing innovation

What's Next?

Phishing is destined to become a never-ending cat-and-mouse game, in which today's solutions may not work as well tomorrow. Solution providers and financial institutions must pedal hard to keep up. Because so much is at stake, counter-phishing will continue to attract money and innovation, and vendors will increasingly be called upon to offer integrated solutions that address multiple facets of this complex problem□

Companies Mentioned In This Article

41st Parameter (www.41stparameter.com)
Bharosa (www.bharosa.com)
Billeo (www.billeo.com)
BioPassword (www.biopassword.com)
Collective Trust (no site found)
Corillian (www.corillian.com)
Cyota (www.cyota.com)
Cyveillance (www.cyveillance.com)
Digital Envoy (www.digitalenvoy.com)
EarthLink (www.earthlink.com)
Entrust (www.entrust.com)
Envisional (www.envisional.com)
GeoTrust (www.geotrust.com)
Goodmail (www.goodmail.com)
Ironport (www.ironport.com)
MarkMonitor (www.markmonitor.com)
McAfee (www.mcafee.com)
Microsoft (www.microsoft.com)
NameProtect (www.nameprotect.com)
Netcraft (www.netcraft.com)
PassMark (www.passmark.com)
PhishFree (www.phishfree.com)
Postini (www.postini.com)
Real User (www.realuser.com)
RSA (www.rsasecurity.com)
SafeScrypt (www.safescrypt.com)
ShareCube (www.sharecube.com)
Symantec (www.symantec.com)
Vasco Data Security (www.vasco.com)
VeriSign (www.verisign.com)
Webroot Software (www.webroot.com)
WholeSecurity (www.wholesecurity.com)