Security Technologies Go Phishing

David Geer

Necessity is the mother of invention. In the computer industry, that usually means that when a problem arises, somebody figures out how to solve it and make money in the process.

One of the latest computer-related problems to arise is *phishing*, in which e-mails lure unsuspecting victims into giving up user names, passwords, Social Security numbers, and account information after linking to counterfeit bank, credit card, and e-commerce Web sites.

Organized crime frequently uses phishing, noted Ken Dunham, director of malicious-code intelligence for iDefense, an online-security company. In addition, he said, there is a black market for stolen credit card and Social Security numbers.

"All fraudsters operate according to three elements: How hard is it to perpetrate? What is the risk of getting caught? What is the reward? It is really easy to do phishing, there is a very small chance of getting caught, and the reward is very high," explained Naftali Bennett, CEO of Cyota, which provides online security for financial institutions.

For the 12 months ending April 2004, said analyst Avivah Litan with Gartner Inc., a market research firm, "there were 1.8 million phishing attack victims, and the fraud incurred by phishing victims totaled $1.2 billion."

Additional institutional costs, such as installing antiphishing technology and educating users, totaled about $100 million, according to George Tubin, senior analyst with the Delivery Channels Research Service at the TowerGroup, a financial-services research and consulting firm. Tubin predicted that phishing-related fraud could double this year.

The Anti-Phishing Working Group (www.antiphishing.org)—a global consortium of businesses, technology firms, and law enforcement organizations—reports that the number of phishing-related e-mails is growing rapidly, increasing 28 percent from July 2004 through March 2005.

So far, phishers have hit only a small percentage of financial institutions—150 of 9,000 in the US—but the number is rising and attackers are targeting other industries, such as e-commerce, said APWG secretary general Peter Cassidy. Nonetheless, major phishing incidents have already eroded consumer confidence in online banking, noted Dunham.

Banks and many other affected organizations are fighting phishing via public education. Some companies are using litigation. For example, Microsoft recently filed 117 lawsuits against people who allegedly used the company's trademarked images to create phishing sites.

However, the focus for numerous companies is on antiphishing technology.

ANTIPHISHING GROWING PAINS

Like phishing itself, antiphishing technology is new, with many companies starting to offer services only a year ago. Most of the companies focus on only one or two antiphishing techniques. Fighting phishing frequently requires more complex approaches, though.

With this in mind, Corillian, Internet Identity, NameProtect, PassMark Security, and Symantec recently formed the Anti-Fraud Alliance to offer a comprehensive set of strategies.

The antiphishing market hasn't been around long enough yet to coalesce around a few approaches. "Thus, many companies have delayed adopting antiphishing measures until the market matures or they decide that further investments in traditional fraud control measures are more cost-effective," said Chuck Wade, a principal with the Interisle Consulting Group, a network-technology consultancy.

Regulators want to encourage potential victims to use antiphishing systems. For example, the US Federal Deposit Insurance Corp. (FDIC), which insures bank deposits and investigates compliance with banking regulations, has recommended that financial institutions use such technologies.

In addition, the Financial Services Technology Consortium (www.fstc.org)—a group of North American financial institutions, technology vendors, independent research organizations, and government agencies—recently completed a six-month survey

of antiphishing approaches. The group has recommended technical and operating requirements for financial institutions' antiphishing measures.

FIGHTING PHISHING

Several antiphishing approaches are becoming popular. One key to many of these approaches is having Internet service providers (ISPs) close phishing Web sites. However, this can be time-consuming and expensive. And it can be useless to even try closing sites in countries that lack or don't enforce antihacking laws.

Meanwhile, companies whose Web sites are targeted by phishers must battle public perception that they can't protect their customers.

Retaliatory services. Several antiphishing companies offer retaliatory services. "Some security companies respond by sending phishing sites so much fake financial information that the sites can't accept information from would-be victims," explained Mark Goines, chief marketing officer of vendor PassMark Security.

Most phishing sites run off of Web servers installed on hijacked home computers and can't handle much traffic. However, retaliatory services generally don't shut down phishing sites by overwhelming them with traffic, as occurs in a denial-of-service attack. They just send the sites as much traffic as they can handle and dilute their database with largely false information, a process known as *poisoning*.

Two-factor authentication. Banks can blunt phishing attacks by requiring online customers to use two-factor authentication, said Goines. One factor is a user ID and password, and the other is an authenticating image and phrase that the participant preselects with a bank or online vendor.

As Figure 1 shows, an e-mail that a bank or online business sends to a consumer contains something the phisher couldn't have, such as the unique image and phrase that the user chose when setting up the account, explained Goines. This proves to the user that the e-mail

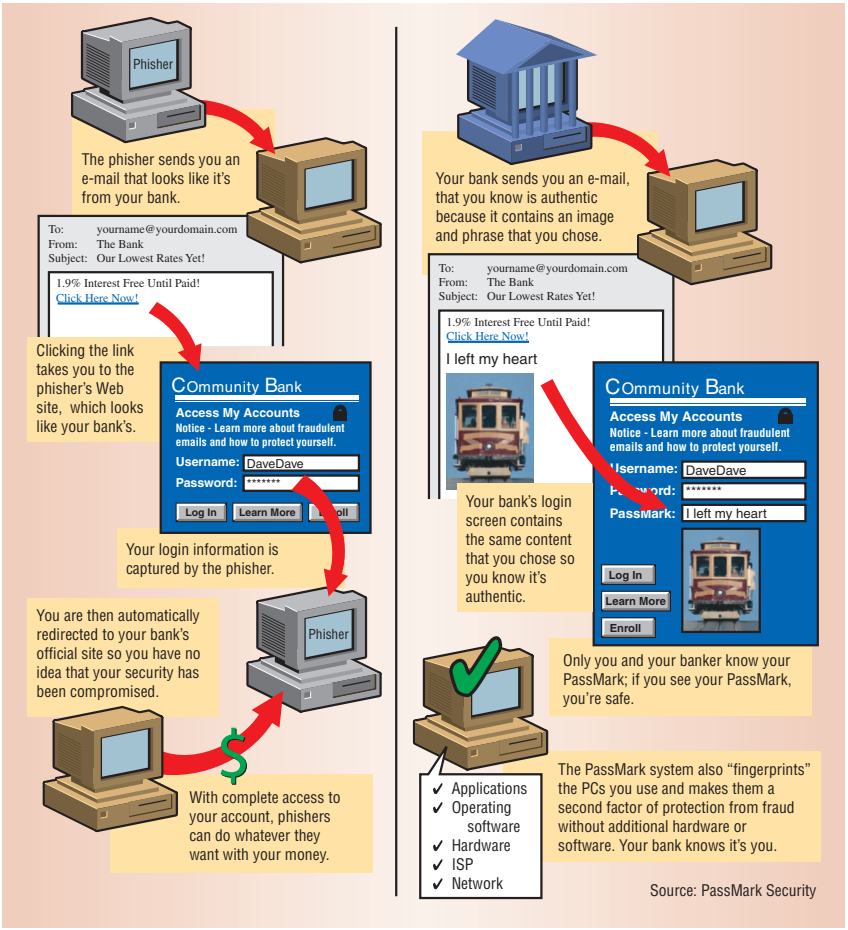

Figure 1. PassMark Security offers a two-factor authentication system to fight phishing.

came from the bank or business, not a phisher, and that it is safe to use the provided link.

Businesses can implement the system inside either their Web site's or PassMark's data center. If implemented on PassMark's data center, the application provides additional protection by asking participants, before they link to a Web site from an e-mail note, for their user IDs for the site and by identifying their computer's IP address. The system verifies that both are correct.

The application then presents customers with their preselected image and phrase along with a request for their logon password. After receiving the correct password, the system lets the customer access the Web site.

The FDIC recommends that US banks adopt two-factor authentication. However, said the TowerGroup's Tubin, few banks have required such measures out of concern that the additional effort could cause customers to avoid Internet banking.

Catching phishers during their preparation. Phishers spend considerable time visiting targeted sites, or they use automated tools to download copies of Web pages. This lets them more accurately counterfeit a business's site.

Corillian, which also develops Web sites for financial institutions, monitors and evaluates suspicious traffic on customers' sites on weekends, when most phishers conduct reconnaissance. Corillian recognizes the signs of an impending phishing attack by understanding hackers' tools and techniques, explained Jim Maloney, Corillian's chief security executive.

"The Corillian Fraud Detection System (CFDS) analyzes Web logs to look for patterns of possible phishing-related behavior," he explained. "We have a set of rules for analyzing logs and producing suspicious-activity reports."

For example, to look more authentic, many phishing sites link to images on a targeted business's site, presenting them along with bogus information the hackers provide on their counterfeit site. The CFDS can check entries in a bank or other business's Web logs and identify phishers who are downloading and saving images, which is unusual behavior for a legitimate transaction.

The CFDS then identifies counterfeit sites using customers' images without authorization. At that point, Maloney said, "Corillian can notify the account holder and law enforcement."

Phishers frequently verify stolen information before selling it. When CFDS identifies a single Internet address trying to access many of a business's online accounts, which is what would occur during the verification process, it notifies the company that the accounts may have been compromised.

Registering deceptive domain names. NameProtect watches for phishers by monitoring spam from many sources, including e-mail accounts set up to bait spammers and spam feeds from ISPs. The product also checks domain-name registration records and searches the Internet for counterfeit bank sites under construction, as located by its Web crawlers.

If the company's ActiveIP tool finds a Web site that includes all or part of a customer's trademarked name, an analyst reviews it to determine if illegal activity is taking place, explained James Blystone, NameProtect's senior director of marketing.

"We work with the client, the ISP, and the registrar to immediately close phishing sites. We can take sites down as quickly as an hour or two but typically within 24 hours," noted Blystone.

NameProtect shares phishing-related information with the US Secret Service and FBI, said Robert Caldwell, the company's director of business development.

Monitoring chat rooms and domain-name registries. MarkMonitor's Brand Protection and Fraud Protection services track online chat rooms and Internet-address registries for information on possible phishing sites. Every day, the company tracks name registrations and name changes, said MarkMonitor CEO Mark Shull.

The company also has an Identity Tracker service that searches millions of Internet address records in its whois and reverse whois directories to identify the creators or owners of counterfeit sites, Shull noted.

It appears that phishing will be a war of attacks and counterattacks.

MarkMonitor uses its findings to try to convince domain-name registrars to transfer ownership of domains that include a company's name and that are used for phishing to the victimized businesses.

Antiphishing browsers. In the near future, Netscape plans to release a Web browser designed to resist phishing. Netscape is negotiating with security companies to supply the Netscape 8 beta with frequently updated blacklists of suspected phishing Web sites. "The browser also uses a whitelist of [trusted] sites," explained Netscape spokesperson Andrew Weinstein.

When a user follows an e-mail link and visits a trusted site, the browser automatically renders it. "The browser will block user access to known phishing sites," Weinstein noted. When a user visits a site not on a whitelist or blacklist, the browser renders it with enhanced security that disables ActiveX and JavaScript capabilities, which phishers could use to exploit vulnerabilities.

Deepnet Explorer 1.4, a browser shell that uses Internet Explorer to render Web pages, analyzes Web addresses and warns users about those on a blacklist of suspect sites. Users can then choose to either stop or continue trying to access a site.

"Our blacklist comes from sites collected internally, reported by our users, and aggregated from our affiliate companies," noted Deepnet marketing manager Anneli Ritari.

Tracking. Cyota monitors various accounts set up specifically to be tracked if phishers attack them. This enables companies to observe the phishing and fraud process and learn ways to fight back. Cyota tracks account activities outside a bank's network, such as on the Internet, while banks track them within their own systems.

FUTURE THREATS

Phishers are improving techniques for making counterfeit Web sites look more realistic and for convincing visitors to enter personal information on them.

In addition, phishing attacks are becoming more sophisticated. For example, phishers are increasingly using instant messaging instead of e-mail, according to the APWG's Cassidy. In one type of attack, phishers send IM users a message with a link to a fake Web site.

Cross-site scripting

"Online criminals are increasingly using cross-site scripting (XSS) flaws to inject their own code into legitimate Web pages and fool unsuspecting consumers into falling for phishing scams," said Paul Mutton, a developer with Netcraft, an Internet services company.

"Cross-site scripting vulnerabilities in Web server applications cause some pages to process JavaScript code incorrectly. This lets hackers push their own JavaScript programs, such as fake password login systems, onto legitimate Web pages," Mutton explained.

"The majority of phishing Web sites are only semi-believable, and users are

starting to see through them," he said. "But with cross-site scripting, people are more likely to fall for the scam."

XSS can also take advantage of the session cookies frequently used when customers log onto banking or e-commerce sites. A script injected onto a site could access a cookie and send it to the phisher, who could then replicate it and log onto a victim's account.

"Companies will see more XSS threats unless they review server applications and eliminate the flaw that enables the attacks," Mutton predicted.

Malicious code

The recent Crowt.D worm demonstrated how a virus author could write code that alters an operating system's hosts file, which contains mappings of IP addresses to host names, and redirect visitors to another site, noted Jaime Lyndon Yaneza, senior antivirus consultant with the Global Anti-Virus Research Group at Internet-security vendor Trend Micro. Attackers could use this technique to redirect users to a phishing site, according to Yaneza.

Attacking companies, not customers

Rather than targeting a victim's personal information, some phishing schemes attack individuals to gain access to valuable information in a company's database.

Phishers send an e-mail, purportedly from a company, to the firm's customers promising new application features if they link to and log into the business's Web site and enter their account name and password. However, the site they link to is counterfeit.

Attackers use the account name and password to enter the company's real site and hack their way to network drives and other network resources, administrative logon information, additional online accounts, and sensitive data such as credit card and e-commerce logon data, according to iDefense's Dunham.

Dunham said phishers use similar schemes to target a company's employees and steal corporate intranet logon information. This would let attackers enter a company's internal network, steal confidential material, and cause other problems.

According to the Tower Group's Tubin, antiphishing products, adopted primarily by larger nationwide or international banks, appear to be effective because phishers recently have started hitting smaller, regional financial institutions that are less likely to use the technology.

Despite the technology's early success, MarkMonitor's Shull stated, potential victims must remain vigilant. "The Internet benefits everyone," he explained. "It enables enterprises to reach new customers, and it enables criminals to do the same."

As for the future, the APWG's Cassidy said phishing will be a war of escalation, attacks, and counterattacks.

Concluded Bennett, "Phishing is evolving, so solutions need to evolve, too." ■

David Geer is a freelance technology writer based in Ashtabula, Ohio. Contact him at david@geercom.com.

Editor: Lee Garber, *Computer*, l.garber@computer.org