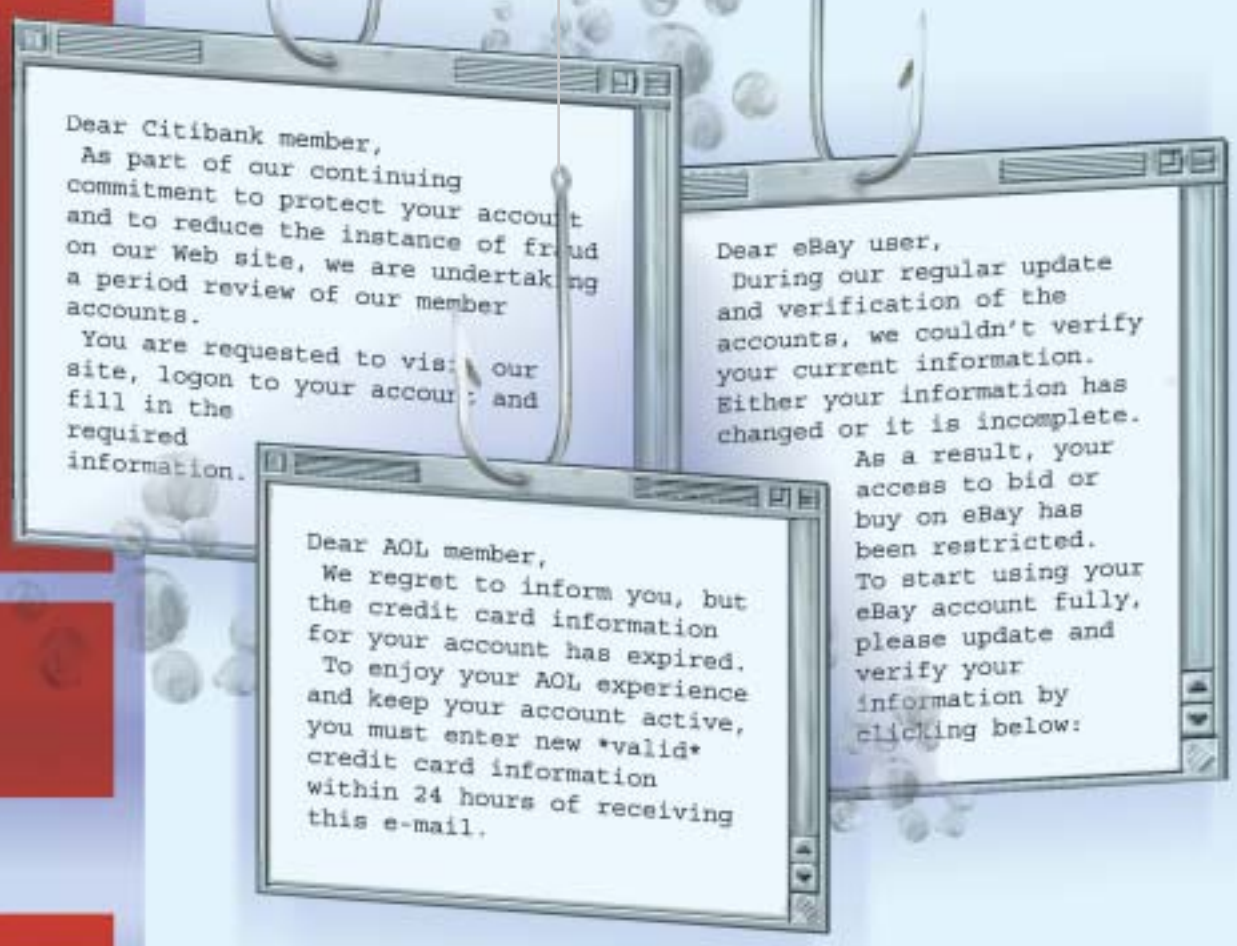
Sophisticated e-mail scams are a potential disaster for Internet commerce.

FEAR of PHISHING

BY DEBORAH RADCLIFF



These e-mails are fakes, frauds, phonies. They are examples of phishing, a growing scourge that strikes at the very heart of Internet commerce by undermining the trust between e-commerce sites and their customers.

"What's at stake is all of e-commerce and our online way of life," says Fred Felman, vice president of marketing with Zone Labs.

DK Matai, executive chairman of mi2g, an electronic banking and security vendor in the U.K., puts it this way: "Brand protection is the key issue in the 21st century because it's the flip side of identity theft. Even if phishing's not their fault, online brands should be powerful and calculating enough to prevent consumers from making mistakes that cost them their identities."

In this phish, if you click on the link in the scam e-mail, you are taken to a real Citibank site; it's the pop-up box that's fake. If you enter your information, it goes to the phisher.

Online merchants such as eBay offer free toolbars that will confirm that you are on the real eBay site and warn you when you are going to a phish site.

David Remick, manager of enterprise information security for EarthLink, adds, "Phishers are a serious problem to our consumers. EarthLink has been committed to fighting phishers since we started picking up on the activity against our brand three years ago." EarthLink currently is offering a free scam-blocking toolbar that alerts consumers when they are about to visit a site that's on EarthLink's list known scammers.

Clearly, phishing has become more sophisticated and more prolific. "We got a phish last week with the eBay brand, and it took us 25 minutes to be sure it was actually a spoof. If we can't tell the good from the bad, then how can the consumer?" asks Cayce Ullman, CTO of secure messaging company PostX.

The number of phishes is skyrocketing. In April, the Anti-Phishing Working Group (AWG) detected 1,125 unique new phishes. That's a 180% increase over March, when 402 new phishes were reported.

Phishing is starting to take its toll. Consumer confidence in e-mail is at an all-time low, according to Pew Internet Life. In its March survey of 1,371 Internet users, 63% said they are less trusting of e-mail. Last June, that number was 52%.

In a recent online survey of 650 U.S. respondents, 75% said they are less likely to respond to e-mails from their bank because of phishing. Online market researcher Infosurv conducted the survey on behalf of anti-fraud vendor Cyota.

Experts say that unless businesses can stop the fraudulent use of their brands, they could lose their online channels altogether.

Step 1: Educate

Ask any big online brand what they're doing about the problem and they'll point to user education.

Citibank, one of the earliest brands phishers exploited, has a prominent link at the bottom of its home page about e-mail fraud. The link takes you to all known e-mail phishes forging the Citi brand name, and tells readers how to identify and report fraudulent e-mails.

But education isn't enough, analysts say. For starters, some customers are learning not to trust anything, so they're deleting your legitimate communications without reading them, says Brian Murray, vice-president of client services of Cyveillance, an online brand protection service provider.

Step 2: Authenticate

Beyond education, online brands need a way to authenticate legitimate e-mail in a simple, easy-to-follow way, says Pete Lindstrom, research director at Spire Security.

"The missing piece is how does a bank or online business validate their authenticity without being complicated for the consumer?" says Phillip Hallam-Baker, principal scientist at VeriSign.

One way, he says, would be an extension to Secure Multi-purpose Internet Mail Extensions (S/MIME) that would show users a corporate logo instead of a digital signature chain to prove the mail's been signed by a valid certificate authority.

"We've issued a logo in our own certificates. And the technology and standards exist," he explains.

Tumbleweed Communications, a secure Internet messaging company, announced in March that it has a market-ready S/MIME solution that does just that. Its e-mail authentication engine applies in-bound and out-bound digital signatures at the gateway. The customer sees a red ribbon on the left side of the mail that, when clicked, says the message is signed and by whom. If a phisher tries to spoof a digital signature, the recipient will get a warning message.

"Outlook, Notes or Novell Groupwise are already configured to read our S/MIME certificates, so consumers wouldn't have to install any new software," says Dave Jevans, marketing vice president for Tumbleweed and chair of the AWG. "All businesses need to do is put this gateway between their mail sending servers and the Internet, import cer-

PHEAR OF PHISHING SPECIAL REPORT

What is Phishing?

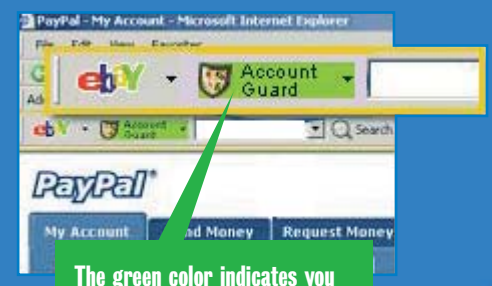
Phishing attacks use spoofed e-mails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames, passwords and Social Security numbers. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers convince up to 5% of recipients to respond to them.

User protection

Just as important as educating your consumers about phishing is giving them some tools to protect themselves, says David Remick, manager of enterprise information security for EarthLink. AOL, EarthLink and others offer links to a variety of protection tools that will go a long way in stopping phishes from making it to the desktop. These include:

Pop-up blockers, which protect against a new form of phish that sends users to a pop-up directly in front of a legitimate site. When they type in their credentials, the dialog box closes, sends an error message and delivers the browser to the legitimate site.

Anti-spam tools, which would block at least some of the spam-based phishes coming at them.



The green color indicates you are on a PayPal or eBay site.

Anti-spyware tools, which help protect consumers from spyware-embedded URL-redirects to phishing sites.

Anti-virus tools that protect against virus-born phishes.

While EarthLink offers its own pop-up and spam-blocking tools, AOL links to other vendor products, including:

Pop-up Stopper Download — www.STOPzilla.com
Free Pop-up Blocker — www.Stop-Sign.com
Free Anti Spam tool — www.spamfighter.com
Spam — www.spambutcher.com
Fight Spam on the Internet — http://spam.abuse.net
WWW.SPAM.COM — www.spam.com
SpamCop — http://spamcop.net
Welcome to CAUCE — www.cauce.org
Spam Laws — www.spamlaws.com
SpamAssassin — www.spamassassin.org
A Plan for Spam — www.paulgraham.com/spam.html
Anti-Spam — www.hostedscripts.com/scripts/antispam.html
MailWasher — www.mailwasher.net
UXN Spam Combat — http://combat.uxn.com

tificates and the server signs outbound mails in accordance with policy."

Longer-term global authentication projects include the Sender Policy Framework, Yahoo DomainKeys proposal and Microsoft's Caller-ID. But these approaches take time and 100% buy-in from the online community, says Scott Olechowski, vice president of product strategy and development at PostX, a secure e-mail company.

Caller-ID would require all e-mail servers to perform forward DNS lookups to confirm the domain that claims to have sent the message. It also would require DNS servers to have an extra set of entries for every host name that can appear after the @ symbol in the e-mail, or at least one new entry that encompasses all host names.

At the RSA Security conference in February, PostX announced a similar concept to Tumbleweed's in which a simple pop-up panel under the URL box with green-, red- and yellow-light indicators tell consumers if the e-mail is bad, good or questionable. (In non-browser-based e-mail such as Eudora or Outlook, an icon button in the main screen and message screen lights up.)

But this requires consumers to load a little piece of free software that must be distributed by their online brands. Merchants aren't too keen on the yellow-light concept, says Julie Fergerson, co-chair of the 7,000-member Merchant Risk Council, a network of merchants doing business online.

"The problem with the PostX solution is the potential for false-positives," she says. "Merchants who don't sign up for the service will receive a yellow light, which would make a consumer hesitant."

Step 3: Validate

Web sites, too, need some sort of validation of their legitimacy. So CoreStreet, an identity management validation company, recently posted on its Web site a free browser helper called Spoofstick. Working on Mozilla Firefox and Internet Explorer browsers, Spoofstick validates the Web site by using the browser's internal read-only variables to display the top and second level domain name that the user is browsing.

So when a user is at a legitimate site such as http://signin.ebay.com/aw-cgi/ …, a prominent note just beneath the URL box will say, "You're on ebay.com." If a user is fooled into going to a spoofed site like http://signin.ebay.com@10.19.32.4, the note will say, "You're on 10.19.32.4."

This requires users to know where to go to download the browser helper. If something like this becomes ubiquitous, phishers likely will try to create a similar pop-up message of their own, says Phil Libin, president of CoreStreet. But, because the message style and font are user-specified, it'd be nearly impossible to make a spoofed validation message look the same.

Besides, he adds, "Users need to know information provided by Spoofstick much more than they need to know the full URL. So we think it should be included in all browsers by default."

E-commerce companies are tackling the problem by telling their consumers when they're at spoof sites. For example, eBay has added a new service to its toolbar called Account Guard (http://pages.ebay.com/ebay_tool bar/), which alerts users when they're at legitimate eBay and PayPal sites and spoofed eBay and PayPal sites. It does this by looking through its own domains and a database of spoofs the community has reported. Then, eBay goes one step further and warns users when they are entering their eBay password into an unverified site.

"With the tremendous volume of spoof reports, eBay Toolbar leverages the vigilance of our community to enable users to protect themselves," says Amanda Pires, an eBay spokeswoman.

Step 4: Block

Some ISPs are blocking users from going to bad Web sites altogether. For example, when AOL customers report spam, the links inside the spam are added to a list of blocked sites. When users click those links, they get an error page. But this technique also blocks legitimate links to offers from real businesses.

So EarthLink limits blocking only to phish sites claiming to be part of the EarthLink domain. Like eBay, EarthLink has an easy fraud-reporting mechanism on its "contact us" page, which it uses to feed the database of phish sites.

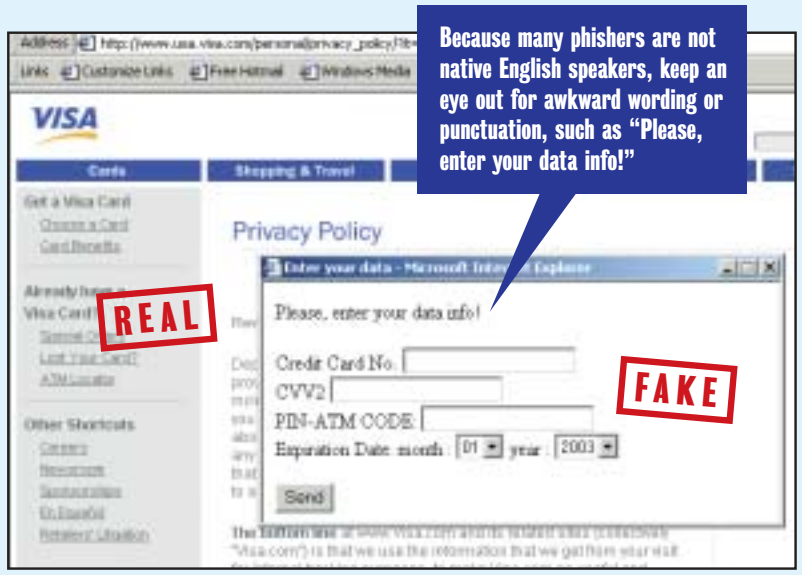
"We use a system known as IP null routing to block Web sites linked from spam pretending to be from EarthLink," EarthLink's Remick says. "If a customer clicks that link, it will not resolve."

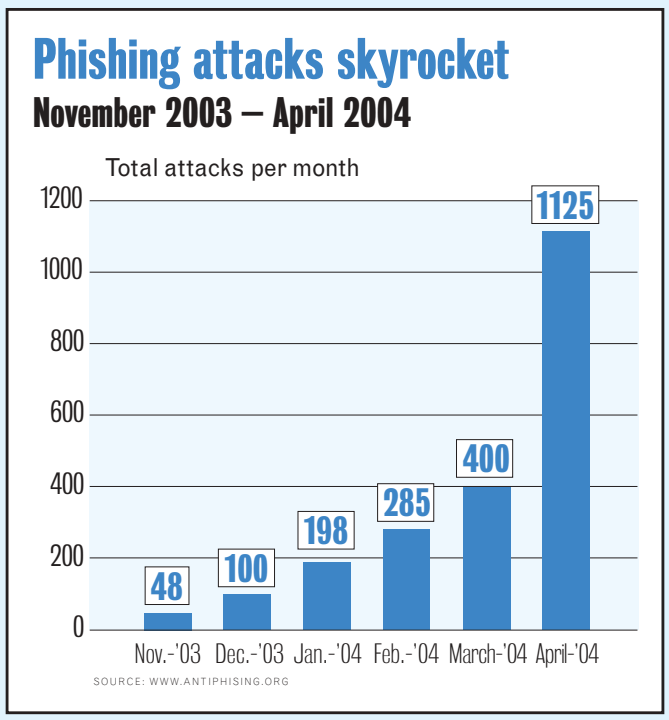
Step 5: Monitor

EarthLink also uses an outside service to alert the company when someone registers for a copycat brand. "Then we run through certain procedures to make sure that the Web site does not attempt to pose as a phisher site for EarthLink," Remick says.

Monitoring for brand misuse is the most effective method of protecting your brand from phishing, according to Fergerson of the Merchant Risk Council.

"Companies like Cyveillance now monitor the Web on behalf of large retailers looking for these types of scams. So the phishing sites and e-mail schemes are detected and shut down nearly within hours instead of days," she says. "That means there are fewer victims."





Cyveillance charges $1,000 per month and up to protect corporate brands from brand theft, trademark infringement, partner compliance and other brand-damaging problems.

For starters, it checks domain registries on behalf of its clients. If it sees a copycat Web site being registered, it notifies the client and works to prevent that site from being used as a phish site. Moreover, it uses a Web crawling technology that takes 21 days to cycle through the entire Internet to capture uses of its clients' brand names. The company also monitors spam through its own trapping filters and through relationships with third-party spam filtering companies.

When phishes are discovered, Cyveillance works closely with ISPs to get them shut down, Murray says. And, when possible, Cyveillance also works with law enforcement.

Step 6: Plan

Murray suggests that all online businesses have a checklist of who to call when their brand has been compromised.

"Most local FBI offices have Internet crime centers. And the Secret Service is opening more Electronic Crime Task Force offices all over the country," says Tom Grasso, a special agent at the FBI's National Cyber Forensics and Training Alliance in Pittsburgh.

Already, some cases are going to court. In March, Zachary Hill pleaded guilty to bilking 400 AOL and PayPal users out of $75,000 through phishing. He's awaiting sentencing in May. And, in January, Helen Carr of Akron, Ohio, was sentenced to four years in prison for phishing, while her partner in crime, George Patterson of Jeannette, Pa., was sentenced to three years last summer.

"Hopefully," Grasso says, "putting more phishers in jail will act as a deterrent."

Radcliff is a freelancer writer in California. She can be reached at deb@radcliff.com.

- Read details on convicted phisher Helen Carr's case.
- Find eight tips on avoiding phishing.

DocFinder: 2227