

INVESTOR'S BUSINESS DAILY

TUESDAY, AUGUST 3, 2004

INTERNET & TECHNOLOGY

E-Mail Phishing Expeditions Find Many Unwary Prey

Studies find these scam e-mails hooking victims by better masking intent

BY DONNA HOWELL

INVESTOR'S BUSINESS DAILY

When Molly Seitel received an e-mail offer for a new credit card from what seemed to be a partner of her bank, she bit. In responding to the offer, the 38-year-old San Franciscan provided some personal information — including her checking account number.

She quickly discovered that \$250 had been debited from her Washington Mutual account.

It could've been much worse for Seitel, and it has been for many.

Phishing e-mails — scam messages that pretend to come from PayPal, Citibank or other well-known companies — are getting tougher to peg as fraud. A recent survey found that one in four people couldn't tell phishing e-mails from real ones.

"Now I'm really careful," said Seitel, who these days checks incoming messages for signs of fraud. "That e-mail sounded so official. But Washington Mutual had never heard of the company."

Lucky for her, Washington Mutual reversed the charges and helped her quickly close her compromised checking account with no further ado. It's not always that easy.

Just one in four people are familiar with phishing scams, says a 300-person survey released Thursday by security firm Symantec^{SMC}.

"Phishing is a relatively new term — the first real attacks

only started to be tracked last October," said Bill Rosenkrantz, a group product manager at Symantec. "People don't necessarily know when they're being propositioned by a fraudulent e-mail or Web site."

While most people haven't been completely duped by phish, the Symantec survey found that almost one in five are sure they've visited a fraudulent Web site. Another 44% said they might well have done so, but aren't sure. And nearly 46% said they don't know how to protect themselves from online fraud or identity theft.

One problem is that phish are getting more sophisticated. They're harder to spot.

"A year ago, phishing was: 'Please enter all your credit card numbers,' and we'd sort of chuckle perversely" at the obviously fraudulent pitch, said Anne Bonaparte, chief executive of MailFrontier, a privately held maker of anti-phishing and anti-spam software. "Now these guys are using real e-mail templates and are including really good links."

Phishers are copying logos and other graphics from banks and e-commerce sites. Their e-mails for the most part look legitimate.

"They're understanding the psyche of those more discerning e-mail users and holes in the Internet infrastructure, and they're taking advantage of it," Bonaparte said.

Her firm recently hired a research company to test 1,000 Internet users: Could they tell the difference between real e-mails from companies and

Phishing Limits?

One research firm expects the number of e-mail scams aimed at stealing personal data will more than double in the next year

Year	Avg. number of unique phishes sent per day	% increase from previous year
'04	51	n.a.
'05	110	115%
'06	190	72%
'07	295	55%
'08	404	37%

Source: Radicati Group

fake ones meant to steal personal data? "Twenty-eight percent were duped," Bonaparte said. "It was surprising."

MailFrontier then put a little "can you spot the phish" test on its mailfrontier.com Web site. In just its first four days, about 65,000 people took the test. Again, more than one in four "failed" the test.

An e-mail supposedly from online payment company PayPal was the most surprising question that people in the big test answered wrong, Bonaparte says. It's an old phishing ruse that demands the recipient update billing information or face account suspension. A link in the e-mail leads to a PayPal look-alike site. Such fake sites, often registered overseas, automate identity theft.

How are people supposed to tell the difference between real and fake e-mails? Of 10 tips at MailFrontier's site, Bonaparte says the most basic is: You never, ever give your financial information away in the form of an e-mail.

Ex-victim Seitel suggests looking for dashes or underscores in addresses. Many scam sites try to look like legitimate big-name e-commerce sites, but they have a dash or other mark in e-mail or Web site addresses.

Security specialists say people can also look for misspellings and bad grammar as a tip-off that an e-mail is really a phishing attempt. Try to be logical. Look for incongruities.

Research firm Radicati Group says the rate of phishing will rise by 115% in the next year, to an average of 110 such unique attacks per day.

Technology firm VeriSign^{VRSN}, which provides security services and runs a domain name registry, last week released a study showing most phishing attacks happen after-hours, when IT managers are out.

Most online payment transactions are processed on Mondays and Tuesdays, just after weekend buying, says Mark Griffiths, vice president of security services at VeriSign. But increases in such traffic on other days can signal trouble.

"That could be that someone out there has managed to get hold of a database of credit card information or has succeeded in a phishing scam," he said. "We'll see transaction traffic rising."

Fighting the tide of phishing e-mail these days takes awareness, education and technology, say people in the security field.

"The issue around phishing," said Bonaparte, "is that if one person is duped, it's worth a lot of money" for the sender of the phish.

Investor's Business Daily www.investors.com © Copyright 2004



MailFrontier™

Email is good again.™