



INVESTORS.com

November 22, 2006

INTERNET & TECHNOLOGY

Watch That Inbox: Some E-Greetings Bring Bad Tidings

By Donna Howell

First the turkey, now spam and phish and more.

A smorgasbord of online threats awaits holiday shoppers and it probably will grow over the next month, security trackers say.

Their advice: Beef up protections early, then employ caution. For example, don't even open an e-greeting unless it's from someone you know — it could be from an identity thief or some other cybergrinch.

"These guys are all experts in manipulating people," said Dave Jevans, chairman of the Anti-Phishing Working Group. "They're definitely getting smarter about working seasonal events."

Jevans says many e-mailed greeting cards are fraudulent. When someone clicks on a Web link to open the card, Trojan code downloads and infects the computer. The number of password-stealing malicious Web pages rose 83% from November to December last year, APWG data show.

More E-Mail, More Scams

Around the holidays, fraudsters try to capitalize on the increased commerce and communication that takes place online. This year, such a surge already is under way.

"We are currently in the middle of an unprecedented outbreak of attacks on e-mail," said Daniel Druker, executive vice president of marketing at message management firm Postini.

Of all e-mail today, 91% is spam, he says. Spam volumes rose 60%, from Sept. 1 through early November.

"I would anticipate as we get closer and closer to the holiday period . . . we'll start to see the flavor of spam and phishing attacks will change," said Mark Sunner, chief technology officer at MessageLabs.

Security analysts say pitches are likely to focus more on shopping and holiday themes. "Consumers may get unsolicited e-mails for a charity asking them to contribute," said Ron Teixeira, executive director of the National Cyber Security Alliance. "We're telling consumers not to respond . . . we suggest they go directly to their Web sites and contribute that way."

Much of the recent rise in spam is tied to a sophisticated Trojan called SpamThru, Sunner says. When it infects computers it turns them into spam-senders, part of a very resilient, so-called "botnet" army — an array of compromised machines that hackers control remotely.

Spyware has become more sophisticated, says Oliver Friedrichs, director of emerging technologies at security firm Symantec. (SYMC)

"In addition, we've seen attackers cross technology boundaries and use other technologies to propagate phishing attacks," he said.

Phishing typically starts with an e-mail appearing to be from a legitimate company. It asks the recipient to click on a link to a Web site to update account details or such. But the e-mail and the Web site are fakes meant to steal passwords and other personal data.

Beyond Phishing

And now, says Friedrichs, there's also "vishing": sending people an e-mail message asking them to call an 800 number. The v is for voice.

Then there is smishing, as phishing ruses arrive by SMS — short message service — text via cell phone.

Types of phishing to watch for include "things like, 'Hey, you purchased this gift for somebody and there's a shipping problem,'" Jevans said. "You see a lot of that this time of year when people do more e-commerce. That was a scam we saw last year around the holidays. Then it went away. We expect we'll see it pick up again."

Scams centered on security are likely too, he says — things like "Due to the holidays and an increased amount of e-commerce, please come here to verify your information."

To counter phishing and other threats, Jevans recommends using more than a plain-vanilla security approach.

"You've got to have more than anti-virus — you've got to have anti-spyware and update it every day," he said. Even then, he adds, the protection isn't 100%.

Security vendors have begun introducing software that helps keep people from visiting malicious Web sites.

Jevans says one of the easiest ways to try this approach is to use either Mozilla's new Firefox 2.0 Web browser or Microsoft's (MSFT) new Internet Explorer 7 browser. Both provide site warning and screening features. Check to make sure these are turned on before Web surfing.

Wi-Fi A No-No

All but the most experienced technology users should consider avoiding online shopping at public Wi-Fi hot spots, says Richard Rushing, chief security officer for wireless security technology vendor AirDefense. Several attacks unique to wireless Wi-Fi are possible.

"The likelihood that someone can mess with you is way too great," Rushing said.

Not all online shopping risks are security-related. Internet users risk ending up with counterfeit goods if they're not careful where they buy.

Jupiter Research forecasts about \$32 billion in U.S. online retail spending this holiday season, up 18% from last year.

About \$2 billion of the total is likely to be for goods that are fakes or sold through unauthorized distributors, says David Silver, vice president of corporate and product strategy at brand-protection firm MarkMonitor.

High-markup products tend to be more at risk of counterfeiting. Many knockoffs are made of luxury purses, video games, movies, software and gift cards.

"Products with low or thin (profit) margins are usually not worthwhile for counterfeiters to reproduce," Silver said.

