

## FRAUD

# Fraudsters sharpening sights on social network, mobile users

Since phishing (also known as spoofing) began in the mid 1990s, the majority of the fake e-mails tended to look as if they had come from financial institutions and credit card companies. Although fraudsters are still using this old bait to try to get recipients to divulge personal or financial information, the rise in consumer awareness has forced them to find new variations on one of the oldest online scams.

“Phishing still occurs in our industry, but I don’t think it’s a major problem any more,” says Rick Rennie, vice president of risk services for MasterCard Canada. “People have become educated over the years, and most know how to spot a fake e-mail. They

see that it’s addressed to ‘dear valued customer,’ or some other impersonal wording, and realize this is not from a legitimate company such as ours.”

Not surprisingly, phishers have turned to the booming world of social media sites in search of new victims.

“I think we will see an increasing rise in phishing or spoofing messages being sent to mobile phones,” says Kevin Lo, a managing director of Froese Forensic Partners in Toronto, where he specializes in computer forensics. “One reason is their growing popularity. But another is that people – especially young people – tend to let their guard down when they use the phone.”

This is backed up by a recent study by the security firm Trusteer, which found that mobile users are “three times more vulnerable to phishing attacks than desktop users.”

A more relaxed attitude to security also often occurs on social media sites. It’s not uncommon for fraudsters to send out multiple friend requests to Facebook users, for example, in hope that some will accept the request without question. “Once they’re your friend, they can start to profile you and create a ‘dictionary’ of information on you based on your birthday, names of pets, your partner’s name, and other critical data that can then be used to guess your banking, work

log-in and other passwords,” said Mr. Lo.

Another new scam is called spear phishing. Unlike the old method that sent out generic e-mails to masses of recipients, spearing targets specific companies. Using information often obtained through social media sites, the fraudsters create messages that seem to come from within an organization. Typically, they spin a tale of some internal problem that, for example, requires the recipients to resend their direct-deposit banking information.

While MasterCard’s Rick Rennie has seen the old-time phishing gambit lose its effectiveness, he still urges consum-

ers to be vigilant in protecting against being defrauded. “We are constantly preaching the need for everyone to practise effective security procedures on their computers,” he says. “They should have the latest virus protection software and spyware software, including e-mail filters and e-mail scanning.”

Does he foresee a day when phishing will no longer work? “It’s possible we will reach a point where users will only accept communications from existing, trusted senders. But until that happens, if they do get victimized, at least they are protected by MasterCard’s zero liability program against fraudulent purchases.”

**“I think we will see an increasing rise in phishing or spoofing messages being sent to mobile phones. People – especially young people – tend to let their guard down when they use the phone.”** Kevin Lo, managing director, Froese Forensic Partners