E-mail fraud protection

How to spot e-mail fraud, and what to do about it **Interviewed by Chelan David**

Anyone with an e-mail address is at risk of being scammed by a practice called phishing. For the perpetrators, it's simply a numbers game. They send out millions of deceitful e-mails with the hope that even a few recipients will act on them, and in the process, unwittingly provide personal and financial information.

The objective behind phishing e-mails is a sinister one, says Hormazd Dalal, president of Castellan Inc. "Underground organizations do it to access bank accounts and glean the information they need to make online charges or to make wire transfers from banks."

Smart Business spoke with Dalal about how to spot phishing scams, the manner in which phishing has evolved and what type of protection is available.

What is phishing?

Phishing is the process of duping Internet users, by e-mail, to go to a fake site that poses as their bank. Once a target visits the phony site, they are requested to type in private, confidential information like bank account numbers, PIN numbers, Social Security numbers and so on. This information then enables the 'phisher' to access banking information for illegal purposes, such as withdrawing funds, making fraudulent purchases and stealing identities.

How can a person spot a phishing scam?

Typically, valid banks send notices in their statements to customers saying that they never request information via e-mail. Any e-mail that requests this information should be treated with skepticism.

If you're an advanced computer user, you can usually determine whether an e-mail is fraudulent or not by verifying the link to the Web page that has been pulled up. In many cases, you will notice that it is not actually at your bank home page and that it has a different IP address. The Web page, however, looks very professional and it looks like it could be the bank's. Sometimes it is possible that the Web site could be secure, so you can't judge whether it is legitimate by the lock in the corner of the page.

Hormazd Dalal
President
Castellan Inc.

The best way to avoid phishing is to know that you should never be typing your information into a Web site that you have arrived at from a link in an e-mail.

What are some common elements of phishing e-mails?

The major characteristic is that they have a clickable link to another Web site. A valid e-mail from a bank would instruct the user to log onto their site and will give no further information. It would not contain a link, but rather would direct the user to authenticate the transaction by using his or her specific password.

How have phishing scams, such as spear phishing, evolved in an effort by perpetrators to elude detection?

As the Internet populace becomes savvier and more aware about identity theft, phishers try and pose as though the e-mail is coming from a known person rather than from a bank. This is part of the technique that spammers use to spoof an e-mail address.

Spear phishing is when a scammer attempts to make the e-mail appear as though it's coming from someone you know within your company or department. Essentially, they're targeting you with the expectation that you're more likely to click on a link from such an e-mail because it appears to have more credibility.

What technologies are available for protection?

There are several databases of known phishing schemes. Starting later this year, Microsoft will be releasing IE7, its new browser, which will check against these phishing databases and alert you if it is indeed a known phishing site. Although these technologies will mature and the databases will be updated more regularly, there is always the latest phishing scam that will slide through.

The nature of phishing is that it can't be identified by patterns. An e-mail is sent to a user, who's asked to go to a specific site, and if that site is a brand new phishing site that is unknown to the databases, then that user is vulnerable. No technology can stop a person from going to a specific site and typing in their private information. The best defense is to never go from an e-mail to a link to a Web site.

In the future, how do you anticipate people being able to protect themselves against phishing schemes?

As technology evolves, users will become readily protected. Protecting against phishing is in its infancy. By the end of next year, there will be far more efficient systems in place to diagnose and recognize phishing scams. The FBI is also actively involved in tracking down phishing schemes.

HORMAZD DALAL is president of Castellan Inc. Reach him at (818) 789-0088 ext. 202 or hormazd@castellan.net.

Insights Technology is brought to you by Castellan Inc.