Money Matters

How To Spot A Phishing Scam And Avoid Getting Hooked

(NAPSA)—It could happen to you: You open your e-mail and see a message that seems to come from your bank asking you to reconfirm your online banking profile because of “some unusual activity on your account.” Reading it, you notice a couple of things, however. The e-mail begins with a simple “Hello,” not a personal greeting. A couple of words are misspelled and the grammar is a little off. Next, you roll your mouse over the link you’re asked to connect to and you notice it’s clearly not from your bank, because the link misspells the bank’s name.

Nice work. You’ve just avoided being hooked by a phishing scam, where online thieves use false website links and other schemes to gain access to people’s private information or install harmful software on their computers.

“This is what comes to mind when you hear ‘phishing’ and these low-skill attacks definitely still exist,” says Peleus Uhley, lead security strategist at Adobe. “However, phishing attacks have improved and have become more sophisticated over the years. In order to be less obvious, they will often illegally include corporate logos and messaging. They will even use recent events to make the e-mail seem more legitimate,” he adds.

For example, at least 2 million people received an e-mail notifying them that an order they had placed on a large U.S. retailer’s website was being processed, though none of them had actually done so. Still, thousands of people clicked on the link in the e-mail, and they downloaded malware that infected their computers, putting them in the control of the hackers.

Some phishing scams purport to offer the latest updates to popular software such as Adobe Reader and Adobe Flash Player. “These scams can mislead some users to install malware that harms their computers and attempts to capture their sensitive personal information,” says Uhley. In truth, updates to Adobe products are available only on its website. The company never makes software updates available through third parties.

Never give away a password or any personal information to an unsolicited e-mail, even if it seems to come from your bank or other legitimate company.

“If you think you have been a victim of a phishing e-mail claiming to be from Adobe, then send a copy of the offending e-mail to our customer support team so that we can investigate,” Uhley advises.

Recognizing Phishing E-mail

- **A request for personal information.** No legitimate company will ask for personal or account information via e-mail. For example, a recent phishing scam, this time supposedly from a major bank’s customer service group, warned recipients that someone tried to log into their accounts and they must now “confirm” their account info. The phishing spam took recipients to a very convincing copy of the bank’s log-in page, including a Web address that looked like it ended with the bank’s website link, but in fact went to a website in Russia.
- **Urgency.** Don’t ever feel pressured into divulging personal information. While there are legitimate reasons for a company to ask you to do something right away—there’s been a security breach, for example—phishers often use scare tactics to fool you into updating certain information. Contact the company directly to confirm the authenticity of the request.
- **Incorrect spelling and bad grammar.** Phishers often use misspelled words on purpose to get around spam filters that check for the legitimate spelling of a brand name, for example. Another reason is that many scams are run from overseas, where English isn’t the first language.
- **Impersonal greetings.** Legitimate companies will use customer names or user names in the e-mail and banks will often include part of an account number. Phishing e-mails typically offer generic greetings.
- **Your e-mail is the “From” address.** This is a sign of a fake e-mail message. Similarly, if the “To” field is a long list of recipients, you should also be cautious. Legitimate e-mails will most likely be sent directly to you and you only.

Be Smartphone Smart

You should be just as wary on your smartphone as you would be on your desktop. Never give away a password or any personal information. If you’re unsure, go to the site directly or e-mail customer support directly. Never use the links or contacts within the e-mail itself.

Learn More

For further facts and tips on phishing and how to protect yourself, visit www.adobe.com/security/prevent-phishing.html.