Recognizing phishing scams and fraudulent e-mails

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

Con artists might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank, credit card company or employer and request that you provide personal information.

What does a phishing scam look like?

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites.

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site. These copycat sites are also called "spoofed" Web sites. Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists.

How to tell if an e-mail message is fraudulent

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

"If you don't respond within 48 hours, your account will be closed."

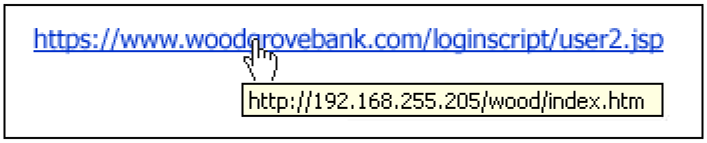
These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishing e-mail might even claim that your response is required because your account might have been compromised.

"Dear Valued Customer."

Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site. Notice in the following example that resting the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm