

Phishing Scams

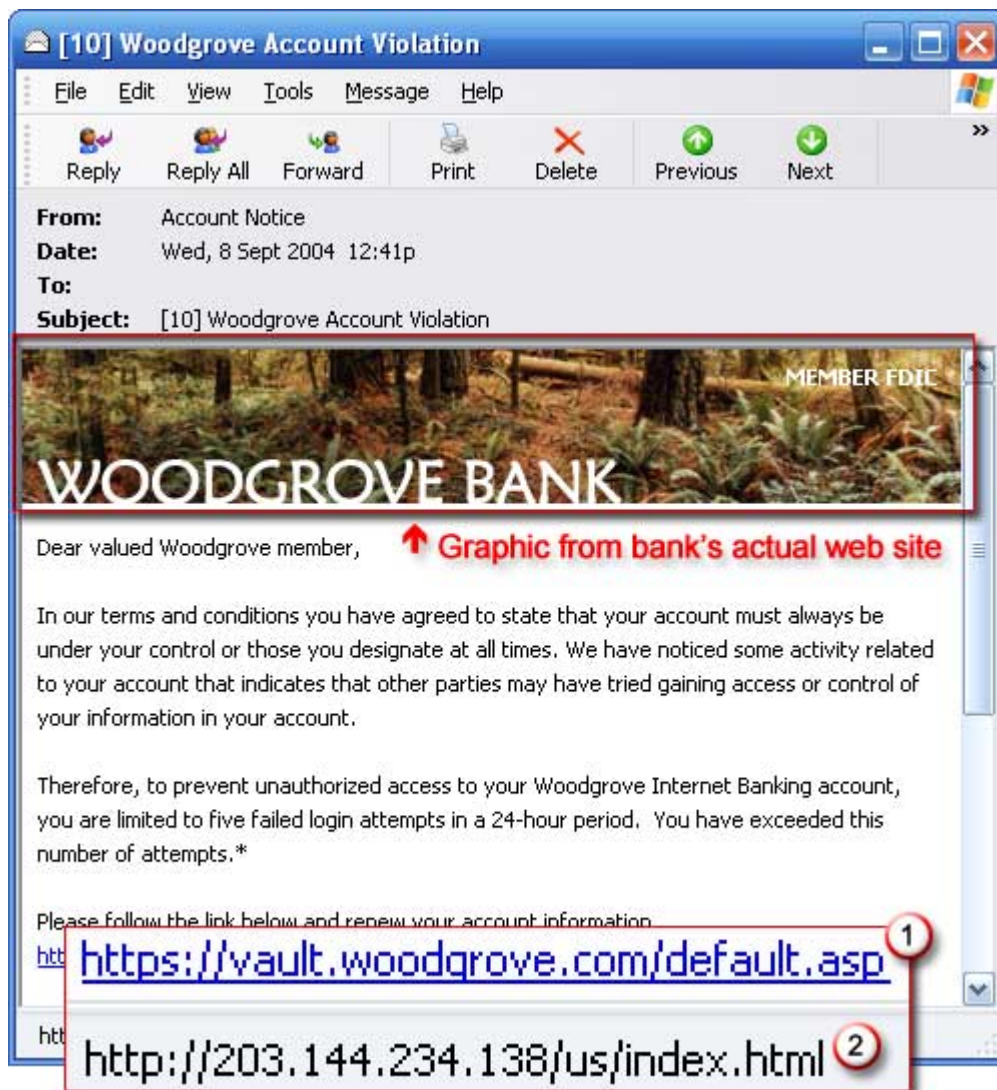
“**Phishing**” is the criminal act of deceiving computer users and luring them into divulging sensitive information such as social security numbers, usernames, passwords, bank account information, and credit card information through electronic communications such as email. The perpetrators of phishing schemes masquerade as legitimate online companies such as PayPal, eBay, Youtube, or online banks. They direct their victims into providing sensitive information under the guise of keeping their account up to date. Phishing is an example of a social engineering technique. Technology such as spam blockers and anti-virus programs can prevent many phishing communications. However, none of these technologies are foolproof. User training and awareness is necessary and probably the most effective means of combating this activity.

Excerpts from <http://www.microsoft.com/protect/yourself/phishing/identify.mspx>

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:



Example of a phishing e-mail message, which includes a deceptive URL address that links to a scam Web site

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

Phishing Scams

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 receive an e-mail from Microsoft asking you to update your credit card information, do not respond: this is a phishing scam. To learn more, read [Fraudulent e-mail that requests credit card information sent to Microsoft customers](#).

"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 message 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 (but not clicking) 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.



Example of masked URL address

Con artists also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as:

www.micosoft.com

www.mircosoft.com

www.verify-microsoft.com

For More Information Check Out These Helpful Sites:

- Short and informative video on phishing:
<http://www.microsoft.com/athome/security/videos/Phishing8.html>
- Article from the Federal Trade Commission:
<http://www.ftc.gov/opa/2003/07/phishing.shtm>
- Anti-Phishing Working Group
http://www.antiphishing.org/consumer_rec.html
- Anti-Phishing Phil – instructional game developed by Carnegie Mellon
http://cups.cs.cmu.edu/antiphishing_phil/quiz/index.html