Security At Home

Security Updates

Latest Security Updates

Products and Services

From Microsoft

Learn how to:

Protect Your Computer

Protect Yourself

Protect Your Family

Resources

Get Our Newsletter

Read Our Blog

Sign Up for RSS

Talk to Our Newsgroup

Get Support

Video Tutorials

Quizzes

Worldwide Sites

Countries & Regions

Security At Home

Recognize phishing scams and fraudulent e-mails

Published: July 14, 2006 | Updated: September 14, 2006

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 or credit card company, and request that you provide personal information.

Top of page

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.

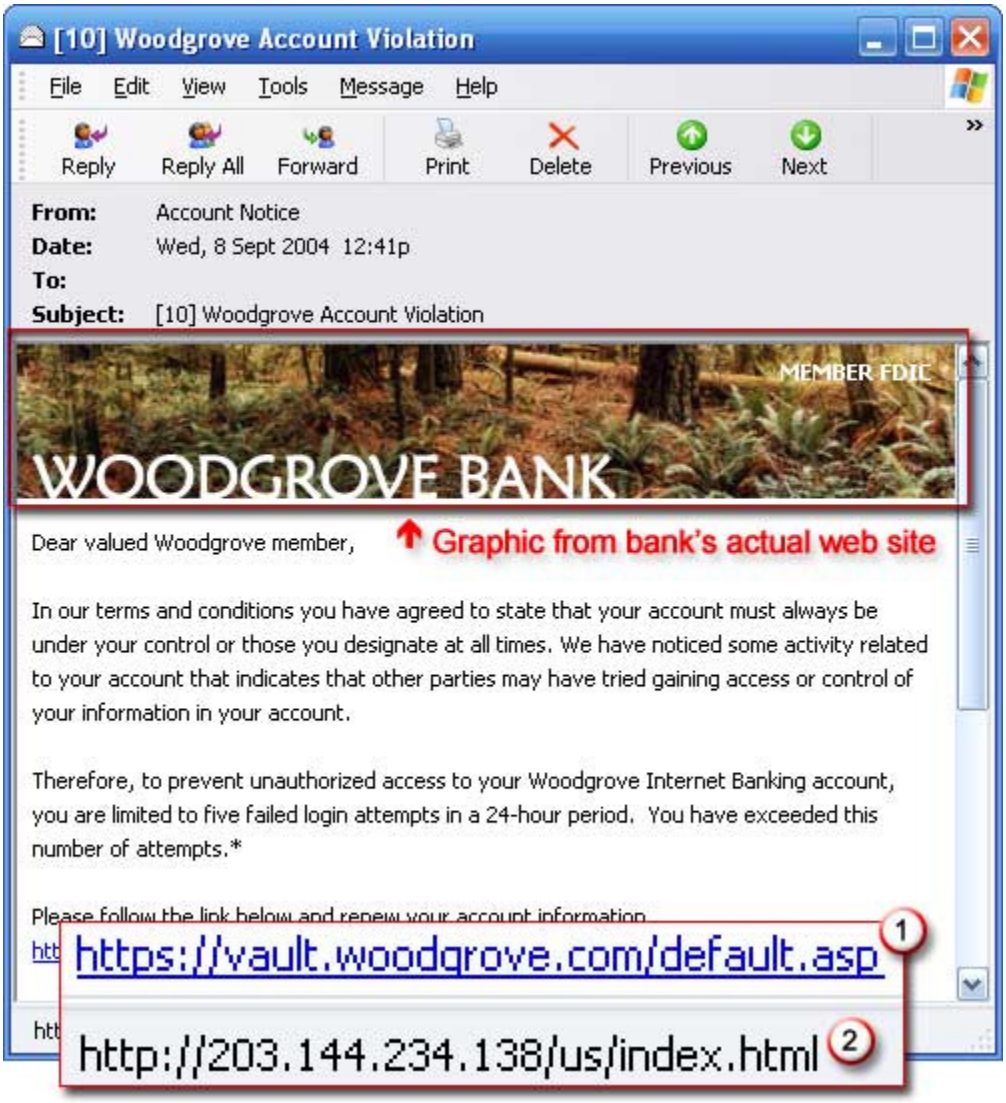
The following is an example of what a phishing scam e-mail message might look like.

Related Links

- Phishing Filter: Help protect yourself from online scams
- How to handle suspicious e-mail
- What to do if you've responded to a phishing scam

Tip

To see updated examples of popular phishing scams or to report a possible phishing scam, visit the Anti-Phishing Working Group Archive.



Example of a phishing e-mail message, including a deceptive URL address linking 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 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.

Top of page

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 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 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.

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.mi**c**osoft.com
www.mi**rc**osoft.com
www.**verify**-microsoft.com

Top of page

Use the latest products and services to help warn and protect you from online scams

- **Install the Microsoft Phishing Filter** using Internet Explorer 7 or Windows Live Toolbar . Phishing Filter helps protect you from Web fraud and the risks of personal data theft by warning or blocking you from reported phishing Web sites. Learn more about how to get Phishing Filter .
- **Install up-to-date antivirus and antispyware software** . Some phishing e-mail contains malicious or unwanted software that can track your activities or simply slow your computer. Try new antivirus and comprehensive computer health services like Windows Live OneCare. To help prevent spyware or other unwanted software, download Windows Defender (Beta 2)

To learn more, read How to handle suspicious e-mail. If you believe you may have already provided personal or financial information in response to an e-mail message, read What to do if you've responded to a phishing scam.

Top of page

Was This Information Useful?

Yes No