Recognize phishing scams and fraudulent e-mail

Published: September 14, 2006 | Updated: October 15, 2008

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

You might see a phishing scam:

- In e-mail messages, even if they appear to be from a coworker or someone you know.
- On your social networking Web site.
- On a fake Web site that accepts donations for charity.
- On Web sites that spoof your familiar sites using slightly different Web addresses, hoping you won't notice.
- In your instant message program.
- On your cell phone or other mobile device.

Often phishing scams rely on placing links in e-mail messages, on Web sites, or in instant messages that seem to come from a service that you trust, like your bank, credit card company, or social networking site.

Related Links

- Get Internet Explorer 7
- 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.

Top of page

What does a phishing scam look like?

Phishing e-mail messages take a number of forms. They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.

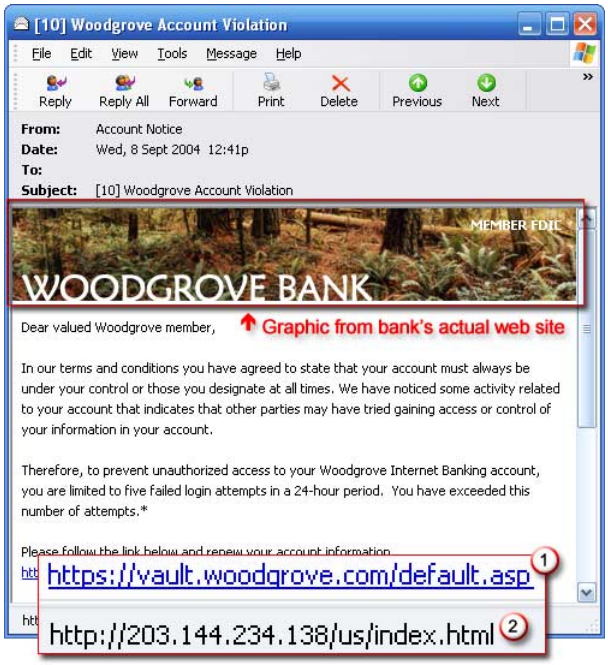
In the United States, recent bank mergers have created new opportunities for scammers. For more information, read FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A "Phish-erman's Special."

Spear phishing is a targeted form of phishing in which an e-mail message might look like it comes from your employer, or from a colleague who might send an e-mail message to everyone in the company, such as the head of human resources or IT. For details, see Spear phishing: highly targeted scams.

Phishing mail often includes official-looking logos and other identifying information taken directly from legitimate Web sites, and it may include convincing details about your personal information that scammers found on your social networking pages.

The main thing phishing e-mail messages have in common is that they ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data.

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



Example of a phishing e-mail message, which includes a deceptive Web 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 actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

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 message 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.

"You have won the lottery."

The lottery scam is a common phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to big companies, such as Microsoft. There is no Microsoft lottery.

"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. A phishing e-mail message might even claim that your response is required because your account might have been compromised.

Top of page

What does a phishing Web site or link look like?

Fake, copycat Web sites are also called *spoofed* Web sites. They are designed to look like the legitimate site, sometimes using graphics or fonts from the legitimate site. They might even have a Web address that's very similar to the legitimate site you are used to visiting. (For details, see Typos can cost you.

Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists. If you enter your login name, password, or other sensitive information, a criminal could use it to steal your identity.

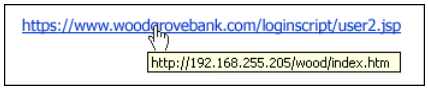
Here's an example of the kind of phrase you might see in an e-mail message that directs you to a phishing Web site:

"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.

Phishing links that you are urged to click in e-mail messages, on Web sites, or even in instant messages 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 an illegitimate 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 a masked Web address

Con artists also use Web addresses that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the address "www.microsoft.com" could appear instead as:
www.mi**c**osoft.com
www.mi**rc**osoft.com
www.**verify**-microsoft.com

Top of page

How can I protect myself from phishing scams?

Keep your operating system up to date, and install up-to-date antivirus and antispyware software.

Your first level of defense against phishing scams and other malicious humans or software is to secure your computer.

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 such as Windows Live OneCare. To help prevent spyware or other unwanted software, use Windows Defender. Windows Defender comes with Windows Vista and is available at no charge for Windows XP SP2.

For more information, see Protect your computer in 4 steps.

Learning how to spot social engineering techniques is the next step in protecting your computer, and Windows Vista makes that easier to do:

- Internet Explorer 7 is available for Windows Vista and has a Phishing Filter built in that scans Web sites and alerts users to phishing sites.
- Windows Vista Parental Controls offer parental controls for children to help prevent kids from downloading unwanted software.
- Windows Defender helps you avoid spyware and other malicious software that can be part of a social engineering scam. Windows Defender comes with Windows Vista. If you use Windows XP SP2, you can download Windows Defender for no charge.
- User Account Control built into Windows Vista requires your consent before allowing potentially dangerous programs to run. This helps reduce the impact of viruses, spyware, and other threats you might encounter through social engineering.

Top of page

Internet Explorer 7 and the Microsoft Phishing Filter

Even if you don't use Windows Vista, you should use Internet Explorer 7, which includes the Microsoft Phishing Filter to help protect you from Web fraud and the risks of personal data theft by warning or blocking you from reported phishing Web sites. See How to get Phishing Filter for more details.

With Internet Explorer 7 you get another layer of protection when you visit sites that use Extended Validation (EV) SSL Certificates. The Internet Explorer address bar turns green to alert you that there is more information available about Web sites. The identity of the Web site owner is also displayed on the address bar.

An EV SSL certificate not only helps ensure that the communication with a Web site is secure, but the certificate also includes information about the owner of the Web site, which has been identified by the Certification Authority (CA) issuing the SSL Certificate. For more information, see Internet Explorer and Extended Validation SSL certificates.

Get Internet Explorer 7

Top of page

Was This Information Useful?

Yes No