

# How to recognize phishing scams and fraudulent e-mail

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

## 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.

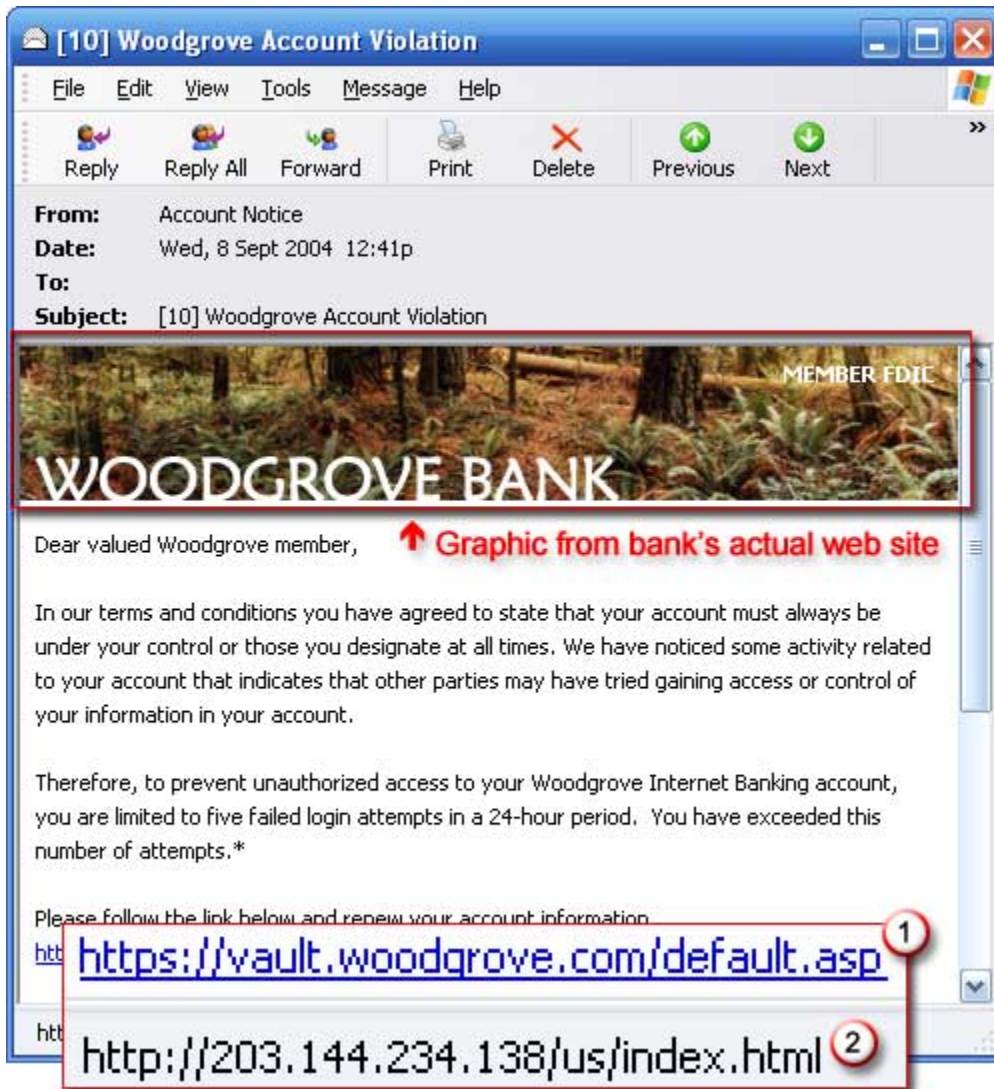
In the United States, recent bank mergers have created new opportunities for scammers.

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.

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.



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 a financial institution asking you to update your credit card information, do not respond: this is a phishing scam.

## **"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.

## **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.

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.



## **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.

Learning how to spot social engineering techniques is the next step in protecting your computer.

The final and perhaps the hardest step is to be aware! If it sounds too good to be true, or doesn't seem like something someone or some company should be asking, then it probably is a scam.

Most financial institutions, the National Bank included, do not request account or personal information from our clients via email or from our website.

Calling the institution that you received the email or website information from is not a bad thing. We are here to assist you, we will not think badly of you for asking. If the email or link is legitimate we will let you know and if it is a phishing email or link the institution that it is spoofing most definitely would like to know so the issue can be resolved before clients get their funds or identities stolen.