Recognizing Spam

Spam messages are messages that are unwanted. If you have received an e-mail from the Internal Revenue Service or the Federal Deposit Insurance Corporation, chances are it was a phishing attempt. If you received e-mail from your bank, PayPal, or Facebook urging you to immediately verify information or risk having your account suspended, it was undoubtedly phishing.

Phishing email messages, websites, and phone calls are designed to steal money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer.

Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.
How to identify spam

Here is an example of what a phishing scam in an email message might look like.

Spelling and bad grammar:
Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. Some have an urgent tone and they seek sensitive information that legitimate companies don't typically ask for via e-mail. If you notice these mistakes in an email, it might be a scam.
Beware of links in email:
If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below 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.

Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

Threats:
Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised. For more information, see Watch out for fake alerts.

Spoofing popular websites or companies:
Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. For more information, see Avoid scams that use the Microsoft name fraudulently.
Other examples of spam mail

- A recent e-mail scam asks PayPal customers to provide additional information or risk getting their account deleted because of changes in the service agreement. Recipients are urged to click on a hyperlink that says "Get Verified!"

- E-mails that look like they come from the FDIC include a subject line that says "check your Bank Deposit Insurance Coverage" or "FDIC has officially named your bank a failed bank." The e-mails include a link to a fake FDIC site where visitors are prompted to open forms to fill out. Clicking on the form links downloads the Zeus virus, which is designed to steal bank passwords and other information.

- E-mails that look like they come from the IRS tell recipients that they are eligible to receive a tax refund and that the money could be claimed by clicking on a link in the e-mail. The link directs visitors to a fake IRS site that prompts for personal and financial information.

- A legitimate-looking Facebook e-mail asks people to provide information to help the social network update its log-in system. Clicking the "update" button in the e-mail takes users to a fake Facebook log-in screen where the user name is filled in and visitors are prompted to provide their password. When the password is typed in, people end up on a page that offers an "Update Tool," but which is actually a Trojan.
Avoiding spam and phishing attacks

• Try to stay off spam lists. Don't post your e-mail address on public sites.

• If an e-mail looks reasonable contact the company directly if you receive an e-mail asking you to verify information. Type the address of the company into the address bar directly rather than click on a link. Or call them, but don't use any phone number provided in the e-mail.

• Don't give out personal information requested via e-mail. Legitimate companies and agencies will use regular mail for important communications and never ask customers to confirm log-in or passwords by clicking on links in e-mail.
• Look carefully at the Web address a link directs to and type in addresses in the browser for businesses if you are uncertain.

• Don't open e-mail attachments that you did not expect to receive. Similarly, don't open download links in IM.
• Make sure you are using a secure Web site when submitting financial and sensitive information. Look for the green padlock icon on the address bar.

• Change passwords frequently. Don't use the same password on multiple sites.

• Regularly log into online accounts to monitor the activity and check statements.

• Keep your antivirus software and your operating system and applications up-to-date.