How to recognize phishing email messages, links, or phone calls

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.

What does a phishing email message look like?

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.
- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it.

  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?
- **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.

Beware of phishing phone calls

Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license. Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.

Once they've gained your trust, cybercriminals might ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable. Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

For more information, see Avoid tech support phone scams.

Report phishing scams

If you receive a fake phone call, take down the caller's information and report it to your local authorities.

You can use Microsoft tools to report a suspected scam on the web or in email.

- **Internet Explorer.** While you are on a suspicious site, click the gear icon and then point to **Safety**. Then click **Report Unsafe Website** and use the web page that is displayed to report the website.
- **Outlook.com (formerly Hotmail).** If you receive a suspicious email message that asks for personal information, click the check box next to the message in your Outlook inbox. Click the arrow next to **Junk** and then point to **Phishing scam**.
- **Microsoft Office Outlook 2010 and 2013.** Right-click the suspicious message, point to **Junk**, and then click **Report Junk**.