7 EASY WAYS TO RECOGNIZE SCAMMERS AND MALWARE

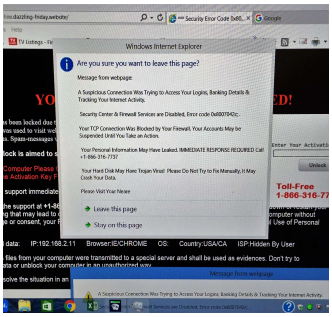
Scammers appeal to your emotions of fear or greed to get you to do what they want. Recognize them to avoid malware and having your identity or money stolen!

1. Microsoft Calling?

You receive telephone calls and the caller says your computer is sending out errors. They say they are Microsoft and can help.

ACTION: HANG UP! Never let a stranger into your computer! The scammers want to put malware on your computer and charge you lots of money to remove it.

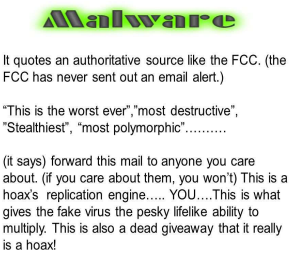
2. Call Microsoft Pop-up?



Your browser pops up scary messages urging you to call Microsoft tech support immediately. Your computer freezes, talks to you and sometimes sirens blare.

ACTION: DO NOT CALL! The scammers want money to remove non-existent malware. To close the pop-up, do CTRL-ALT-DEL, open TASKMANAGER, select the browser, and click END TASK.

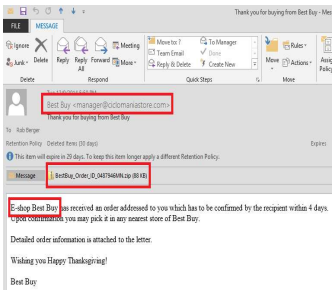
3. FW: e-mail from friend with attachment?



You receive forwarded e-mails from friends asking you to open the attachment, and then forward it to 20 of your friends to also enjoy.

ACTION: DO NOT CLICK TO OPEN! Your friend did not create the attachment. Scammers deliver malware payloads to stolen e-mail addresses ... and viral to your friends.

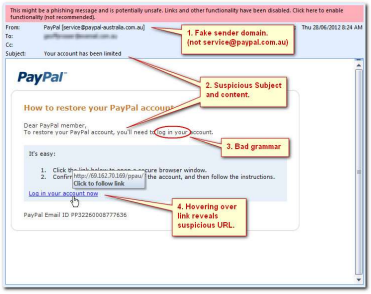
4. E-mail with attached .ZIP file?



You receive e-mails that looks as if they are from a bank, postal delivery tracking or contains an invoice. The e-mail requests that you open the attached .ZIP file to see the details.

ACTION: DO NOT CLICK TO OPEN! The scammer delivers a very serious malicious payload when the the file is opened.

5. E-mail requests you to log-in to your account?



You receive e-mails that appears to be from your bank, credit card, Amazon, PayPal or e-mail service. The e-mail requests that you click a link and log in to verify your account.

ACTION: DO NOT LOG IN FROM ANY E-MAIL! Phishing e-mails from scammers are designed to steal your identity or your money.

6. Different search page?

Your search page is no longer Google or Bing, and you did not change it.

ACTION: DO NOT SEARCH FROM AN UNKNOWN SEARCH PAGE! Scammers change search engines to send you to their malware infected websites.

7. Request to pay to unlock your files?

You click to open a file and are redirected to a page that asks for $$ in bitcoin or iTunes cards to unlock your encrypted files. Your computer has been attacked by Ransomware!

ACTION: TURN OFF YOUR COMPUTER. Do not use your computer; take it immediately to a computer professional at a computer repair shop. Hopefully, you previously backed up your personal files.

Once you recognize how the scammers get into your computer, you will be empowered to avoid the malware they install and be able to better protect your money and identity. I wish you healthy and safe computing.

Linda Lindquist – Contact: pccoach@computerandinternethelp.com

Computer and Internet Help