Walter Hubbard
PC QuickHelp
Winchester, MA

Why bad things happen to good computers

Thank you. I want to talk to you today about security: your computer's security, your personal security. My goal today is to scare the dickens out of you and then tell you how to protect yourself.

How many people here use Windows? Mac?

The bad guys are out to get you and your money. They target people of all ages but especially senior citizens. And it is approaching epidemic proportions, on PCs AND Macs. I have come here to warn you.

Why are the bad guys doing this? Money!

Who are they? They come from several countries primarily from India, Russia, and the United States.

How are they attacking? By establishing your confidence to let them onto your computer through:

- After you click on a nefarious link, your screen may say that you have been infected, and that you need to call Microsoft. DO NOT CALL. Unplug your computer now!
- Telephone calls purporting to be representatives from Microsoft or Apple, or Norton
- Convincing phishing emails that look like they are coming from Geek Squad, Norton, Amazon, Comcast, etc
- One type tells you that they have made a charge to your account and ask you to call an 800 number if you dispute the charges
- Another type entices you to click on a link that takes you to a convincing page for you to enter your username and password

- Some emails come with virus payloads when an attachment is opened, it will infect, steal, and encrypt your data. (Example: client with Ransomware.)
- Promotional links in Google searches that when clicked, will take you to a fake support page that displays the telephone number of fake support. (Example: fake Apple support)
-

The weakest link to your computer is you. Once allowed inside your computer by YOU, the attacker possibly will:

- Show you fake diagnostic or virus scans that the perpetrator can then "fix" for a fee, payable by credit card, debit card, or bank routing and account numbers.
- Ask you to open your bank account page so that the attacker can "refund" an amount to your account. BUT behind the scenes, the attacker is editing that bank page to show a fake entry showing a deposit of several thousand dollars, then asks you to return that amount and then may threaten you if you do not.
- Steal all the passwords that you have saved in your browser such as Google Chrome, Edge, or Safari
- Or they may have infiltrated your email by using old username and passwords that were hacked years ago from hacked websites such as LinkedIn, Ebay, Yahoo, etc. Thereby, the hacker will steal your contacts and send out a fake email purporting to be you asking for gift cards to be purchased and sent to a fictitious address.

How to protect yourself:

- Think before you click.
- Be very cautious when calling any number you find on the internet or email
- Never let anyone that you don't know onto your computer.
- Never give out any passwords to anyone BUT: Write down your passwords and keep them is a secure place and tell your most trusted companion. In the case of your passing, your loved ones can then log into your email, banking, and social media accounts.
-
- Never give out your credit card or banking information to someone you don't know
- Do not store financial or email passwords in your browser.

- **Use a different password for each website**, or better yet, use a password manager such as BitWarden, 1Password, RoboForm, etc.
- Use antivirus software such as Malwarebytes.

I hope that today that we have scared you and educated you enough to take action and precaution when using the internet.