The 5Ws and 1H of Ransomware

WHO ARE THE POTENTIAL RANSOMWARE VICTIMS?

Do you use any mobile devices, laptops, personal computers, play online games, send emails, surf or shop online?

YES

Then you are a potential ransomware victim.
LEARN ABOUT WHAT IT IS AND HOW TO AVOID IT.

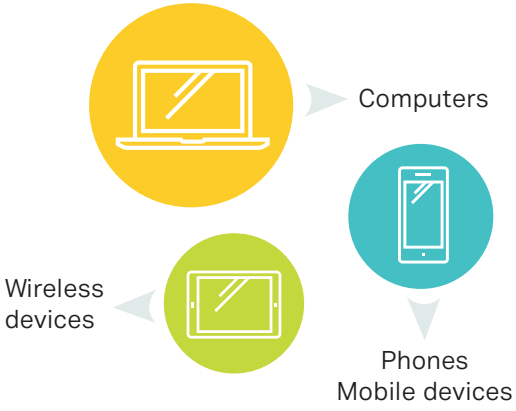
WHAT IS RAMSOMWARE?

A type of malware (malicious software) that can stop you from using your PC, rename or encrypt your files so you can't use them, among other things. You may be warned that you need to pay money, BitCoins, complete surveys, or perform other actions before you can use your PC again.

What does it look like?

- Ransomware note
- Encrypted files
- Renamed files
- Locked screen/ browser

WHERE CAN A RANSOMWARE ATTACK HAPPEN?



When does it start?

Spam emails, untrusted websites, pirated softwares, malwares

- Displays the ransom you have to pay!
- Locks your screen or your files!
- Downloads in your device!

RANSOMWARE LEVEL TYPES

LOCKSCREEN RANSOMWARE

ENCRYPTION RANSOMWARE

WHY MUST YOU EDUCATE YOURSELF ABOUT IT?

So you won't fall into the ransomware trap, because ransomware can:

- Take your hard-earned money in exchange of all the stuff you already own—your data files!
- Can violate your privacy
- Possibly harm your reputation
- Delete your files if you delay payment
- Disrupt your work or personal life when it renames or locks your files
- Puts lives in danger when they infect important services' systems (e.g. hospitals)

HOW CAN YOU AVOID A RANSOMWARE ATTACK?

Educate yourself about ransomware

Read up about ransomware prevention, detection, and recovery measures

Practice safe computing

PREVENT

- Back-up files on an external hard drive or with encrypted cloud storage, like OneDrive
- Beware of phishing emails, spams, and clicking malicious attachments
- Disable the loading of macros in your Office programs
- Keep your Windows OS and antivirus up-to-date
- Upgrade to Windows 10 or 11
- Enable file history or system protection
- Use Microsoft Edge to get SmartScreen protection
- Use multi-factor or two-factor authentication
- Disable your remote desktop feature whenever possible
- Use OneDrive for Consumer or for Business
- Use a safe internet connection
- Avoid seedy websites

DETECT

- Install, use, and update Windows Defender software
- Enable Microsoft Active Protection Service ransomware detection and blocking

RECOVER

- Restore files using File History
- Recover files from One Drive for Consumer or Business

About MERIT 2.0

MERIT was founded in 1983 and was re-branded in 2020 as MERIT 2.0. Our Mission Statement is *To educate every worker at every client and provide them the technology to improve.*

How to Contact MERIT 2.0

SERVICE/REPAIRS/HELPDESK:
service@meritsolutions.net
or call 757-420-5150
www.meritsolutions.net