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?

If yes, then you are a potential ransomware victim, unless you learn about what it is and how to avoid it.

What is RANSOMWARE?

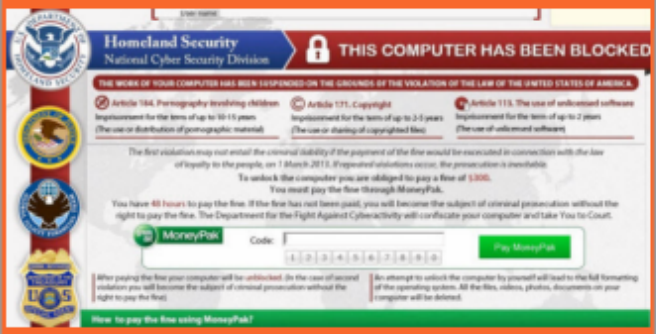
A type of malware that can stop you from using your PC, rename, or encrypt your files so you can't use them. You may be warned that you need to pay money, BitCoins, complete surveys, or perform other actions before you can use your PC again.

What does it look like?

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


ЖДИТЕ 2.59
Error
You either didn't made any payment or your payment information is in processing. Please be patient, in case this message repeats within 3 hours after payment please contact us to: mvplocksvc@yahoo.com
OK
verify your payment status within 2-3 hours after
ion. Please be patient since it's manual process.
In case you made a payment, but decryption process won't start, use this e-mail to contact us:
mvplocksvc@yahoo.com
files
info
copy
decrypt
Where can a ransomware attack happen?
Computers
wireless devices
Mobile devices
phones
Spam mails
https
Untrusted websites
Malwares
Pirated softwares
When does it start?
Downloads in your device!
Locks your screen or your files!
Displays the ransom you have to pay!

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 the stuff you already own - your data or 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 lock yourfiles
- Put 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 in external hard drive
- Beware of phishing emails, spams, and clicking malicious attachment
- Disable the loading of macros in your Office programs
- Keep your Windows OS and antivirus up-to-date.
- Upgrade to Windows 10
- Enable file history or system protection.
- Use Microsoft Edge to get SmartScreen protection
- Use two factor authentication
- Disable your Remote Desktop feature whenever possible
- Use OneDrive for Consumer or for Business
- Use a safe internet connection
- Avoid seedy web sites

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 OneDrive for Consumer or Business

Microsoft