Ransomware

Learn what to do if you fall prey to ransomware.

1. What Is Ransomware? How Does It Get Into a Device?

Ransomware is mostly used to target small and medium businesses. This is because these businesses might lack the resources to have a lot of IT staff and data security practices.

However, cybercriminals are increasingly using ransomware to attack anyone and everyone, from large corporations to government and public sector agencies to individuals

This can happen in a few different ways:

- A link containing malware
- An attachment containing malware
- A user visits a malicious website that contains malware
- A user falls for a phishing scheme
- A user falls for a social engineering scheme

Once ransomware is on a device, the attack commences:

- The ransomware proceeds to infect your system and encrypt files
- The ransomware locks the user out of their systems and files
- The cybercriminals running the attack then demand ransom money to release the system and files

The worst ransomware attacks encrypt files, but others lock you out of your system or just bombard you with pop-up ads until you pay the ransom

2. Handling a Ransomware Attack

- **Identify the ransomware**
  Visit a site that can help you identify the type of ransomware you are dealing with by scanning your system
- **Report the attack**
  Ransomware is a crime. You can report attacks to law enforcement and local FBI offices
- **Avoid paying the ransom!**
  While these attacks can be scary, the general consensus from cybersecurity experts and legal experts is to not pay the ransom since that can just further embolden the criminals and you might not actually get your data back
- **Isolate the infected device or devices**
  Turn off WiFi and Bluetooth, disconnect the devices from external storage or LAN, etc. Doing this can help prevent the ransomware infection from spreading to other devices on the same network.
- **Restore your system**
  Different sites exist that can help you scan and remove ransomware from your system

3. How Can You Avoid Ransomware?

- **Backup your data**
  If you have your data backed up, whether in the cloud or via an external storage device, you can more easily reinstall your system and recover your data
- **Be alert to malware and schemes**
  Know how schemes and malware work and be cautious with opening suspicious links or files, visiting unknown sites, and installing unknown apps
- **Keep your security up to date**
  Install updates and patches and make sure your devices are using updated software
- **Practice good cybersecurity**
  Protect your accounts with things like multi-factor authentication, manage your security settings, and practice good password hygiene