How to Protect Against Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. Learning how to prevent ransomware attacks is a need-to-have set of knowledge and you can do it both at home and at work.

1. **Ensure antivirus is installed, and up to date**
   Keep in mind, AV is based on signatures so new variants may and will slip through the cracks, but this could easily be a first line of defense. Additionally, it's best to have a multi-faceted security solution that employs additional protective technologies such as heuristics, firewalls, behavioral-based threat prevention, etc.

2. **Establish security awareness and training programs**
   Stress the avoidance of clicking on links and attachments in email. Ask yourself these questions when receiving an email message with a link or an attached file:
   1) Do I know the sender?
   2) Do I really need to open that file or go to that link?
   3) Did I really order something from FedEx?

   Phishing is a common entrance vector for ransomware and because most end users never think twice, it's extremely successful.

3. **Restrict administrative rights**
   Reducing privileges will reduce the attack surface significantly. End users shouldn't be downloading and installing games anyway, right?

4. **Back up your information frequently**
   You can backup your data to an external hard drive or use a cloud provider service. Both options are recommended. If your physical location experiences a natural disaster, fire or theft, it is ideal to have a physical device backup stored at a different location. If using a cloud backup service, encrypt data before uploading for an added layer of protection. If you are working in a district, contact your IT department to leverage their backup system.

5. **Perform regular software and security updates and patches**
   All software comes with bugs and vulnerabilities. The vendors who create a software issue software and security updates for your operating systems, computer programs and apps. Some of the more common applications used by criminals are browsers, plug-ins, media players, Flash and Adobe Acrobat. Keep automatic updates turned on for computers and mobile devices to minimize a breach.

6. **Use good judgment with email and web browsing**
   Banking or shopping online should only be done from a computer or device that is on a network that you trust. Never use a public computer or an Internet café with free WIFI for sensitive website browsing. Other good practices are to use the private browsing feature and avoid use of multiple tabs.

7. **Be careful about clicking on a link or opening an attachment**
   Even if it looks like it came from someone you know, get into the habit of reviewing email message headers for fake emails. Criminals use generic names like "First Generic Bank Customer" to avoid the time it takes to send customized emails. Also, the sender may look authentic with the same font, color and logo of a company you recognize. When in doubt, do not click on a suspicious message.

8. **Use complex passwords**
   Passwords should be long and contain a mix of upper case, lower case and symbols. According to Instant Checkmate, it is reported nearly three out of four people use the same password for more than one site, while more than three out of five smartphones users do not use a passcode to protect their device. One third of people use the same password for every website with weak passwords like '12345.'

9. **Practice Password Management**
   Make sure to use unique passwords on different sites and change passwords frequently. Each site or account should have a different password.

10. **Encourage reporting of suspicious activity**
    Make sure employees know how and when to work with their IT departments to report suspicious activity.