Ransomware

Ransomware is a form of malicious code or malware that infects a computer or network and spreads rapidly to encrypt the data. This malware makes the data inaccessible to the users and the criminals responsible will demand payment from the user in order to have their files unencrypted and returned. The payment is often requested in Bitcoin or other untraceable currency.

Businesses and individuals worldwide are currently under attack by ransomware. Individuals are reporting incidents in which their systems are frozen while an on-screen message demands payment to have their data returned. Individuals both at work and at home are at risk of these and similar attacks by hackers. IBM researchers believe ransomware will expand as a common threat and profitable business into 2016, moving to mobile devices as well. Security specialists worldwide have predicted that ransomware will be one of the fastest-growing malicious attacks.

There are three ways computers are commonly infected:

(1) via Email – the individual receives an email with a malicious link or attachment

- the user receives an email offering a software or system update and when the user accepts, the malware infection begins, spreading quickly, and the user receives the ransom notice. The user has to click on a link or open an attachment to begin the infection process.

(2) via Malvertising – the individual visits a legitimate site that displays infected third party advertisements

- this attack vector is currently causing security incidents among organizations globally. Hackers use online advertisements that will appear to be an official, legitimate ads, but are loaded with ransomware, hence the name “malvertising”. When the user clicks on the ad, the malware payload immediately encrypts everything in its path, including shared drives (A:\ through to Z:\). The current virus in play is called CryptoWall – it has been around for a long time, infecting systems around the world.

(3) via Zero Day Exploit – the individual visits a legitimate or illegitimate infected website

- this is the most concerning because it does not require any input from the user. The infected website contains a zero day exploit, such as those known to affect Java and Flash, and simply opening the website that contains the ad will run the ransomware without the user knowing.

Help in protecting against ransomware infection:

Be skeptical, as always. Do not click on any emails or attachments you do not recognize, and avoid suspicious websites altogether, such as the ads/links that often appear at the right or the bottom of a website. Do not accept any software updates that are triggered from a website or email. This includes offers of Windows 10, and updates to Java and Adobe Flash.

What to do if your workstation or other network-connected device is infected:

If you receive a ransomware popup, or come across a file that prompts you to pay a ransom to regain access to your files, you need to:

- immediately stop using your device and disconnect it from the network/Internet to try and halt the spread
- leave the device on and do not touch your device for investigative reasons
- go to another workstation and change key online passwords such as online banking
- report it immediately to your IT department or get assistance in fixing the infection

If this happens on your home computer:

You are always at risk of online malware infections. If you have experienced a ransomware attack *while working from home*, follow the same steps above.

If your personal computer is attacked with ransomware that encrypts your files, they cannot be retrieved. This is why ransomware is so profitable for hackers – many people and businesses will pay the ransom to get their files restored. Experience has shown that the files are usually returned, but extortionists often come again for more money. This is why you must back up your files to an external hard drive that is not left connected to your computer. If your files get encrypted, disconnect your computer and take it to a reputable computer repair shop, along with your backup hard drive, and explain what happened.

If you want to try doing this yourself, you can try using Windows Explorer to look through your files. The encrypted files will likely appear as HELP_YOUR_FILES with a .png, .htm, or .txt extension. Delete only infected files and restore them from your backup hard drive.

Resources
Trend Micro Ransomware Definition
http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

Microsoft's Malware Protection Centre
https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

For an in-depth article on malvertising and how it is used in fake ads:
https://nakedsecurity.sophos.com/2016/01/15/malvertising-why-fighting-adblockers-gets-users-backs-up/

For more information on security awareness issues:
http://www.cio.gov.bc.ca/cio/informationsecurity/isawareness/securityawareness.page