# 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 electronic 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. Trend Micro researchers anticipate that ransomware will make further grounds in 2018 and that it's not going away anytime soon.

## 3 ways computers are commonly infected

1. Email – the individual clicks on a malicious link or attachment in a phishing email.
2. Malvertising – the individual visits a site that displays infected advertisements
3. Drive-by-Downloading – the individual visits a legitimate or illegitimate website with an exploit that has not been patched. This means that simply opening the website will run the ransomware without the user knowing.

## Steps to lower the risk of infection and to help with recovery

- Make sure all software is kept up-to-date with the latest patches including Windows, web browsers, Java and Adobe.
- Perform regular backups of your data. Ideally, this data should be kept on a different device other than your computer.
- Don't open links or attachments in emails from untrusted or unknown sources.
- Ensure your anti-virus is up to date.
- Consider using a security application from a reputable company on your mobile device.
- Don't download or install applications from untrusted or unknown sources.
- Never click on pop-up windows that claim your computer has a virus.

## How to protect against a ransomware infection

*Be skeptical.* 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 pop-up, or come across a file that prompts you to pay a ransom to regain access to your files, you need to:

1. Disable Wi-Fi (if using)
2. Disconnect the network cable from the device to try and halt the spread
3. Leave the device powered on for investigative reasons
4. Go to another workstation and change key online passwords such as online banking
5. Report the problem immediately to your IT department

## If this happens on your home computer

You are always at risk of online malware infections. If you experience 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

## 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.gov.bc.ca/informationsecurity