Safety and Security

- Ransomware
- I viewed explicit content on my work network or device
- [To Do] Malware Guide
- [To Do] How to use the internet and be safe
- [To Do] Working / Learning from Home

Ransomware

> “ https://web.archive.org/web/20171104224702/https://rtechsupport.org/kb/ransomware/

Crypto-ransomware is a large threat today and is only expected to get worse. The key to it’s success is the business model employed for many strains and the method of deployment used.

I am infected! Please help!

1. Remove your infected machine from the network to prevent spread of the virus.

2. Do not panic, you are already infected and your files are already encrypted, take a breath and decide how you want to settle this issue. Hold off on removing the virus, if you come to terms with paying the ransom removing the virus may remove your ability to decrypt the files. Remove it only after deciding on one of the below solutions.

You have several options:

1. If you have backups you can just nuke your install and start fresh, but if you are here it can be assumed you do not have backups.
2. Try a decryptor, several exist and can be found below: Identify your ransomware here or try the NoMoreRansom Project.

A list of cryptoransomware with known decryptors can be found here.

- Kaspersky
- Avast
- Emisoft
- NoMoreRansom

3. Pay a company to attempt recovery of your data or pay the ransomer. You need to assess

the worth of your data and decide if this option is viable.

4. If no decryptor currently exists for your strain you can either set the drive aside or make an image of it to hopefully have a chance at recovering the data at a later date.
5. These are the only options, there is no magic way to solve this and there is no way to crack the encryption yourself.

What do I do next?

- Backup your stuff immediately. Preferably, do this to multiple locations.
- Enable file extensions. Many forms of ransomware use social-engineering to exploit the user, a popular method is a script that an email claims is a invoice, this is actually a javascript file but without file extensions on you will not see the .js extension on the file, as opposed to the .docx that should be on a document.
- Disable macros in Microsoft Office. Much like the previous point, ransomware can also exploit macros in Office to run their malicious payloads.
- Do not open attachments in emails that you are not expecting, see the above two points for why.
- Stay up to date on all OS and application updates, an unpatched system is a vulnerable system.

I viewed explicit content on my work network or device

Clicked on a NSFW Link or 'accidentally' watched porn for 15 minuets at the cubucal at work?

It happens.. more than you think and we dont care unless you give us a reason to. The rule of thumb here is, do we need an excuse to look in to your internet and office pc usages?

We only care if it is illegal or causing issues on the network like bandwidth hogging. Most companies will have a firewall and block anything malicious or sites employees should not be visiting.

Personal Device

If you are using your own device like a mobile phone or laptop that does not have any work software on it then the most we can see if the website you are accessing. Like www.google.com

Work Device

If you are using a work device such as a work mobile phone or Work/school laptop then expect we can see everything encluding any encrypted (HTTPS) websites. Expect your device to be controll by software that gives us full access to everything you are doing on it.

[To Do] Malware Guide

[To Do] How to use the internet and be safe

[To Do] Working / Learning from Home

Using personal device for work for school, browser addons etc etc