What is Ransomeware

- Ransomware is a form of malicious software which encrypts or locks all of your files and then demands a ransom be paid in order to regain access to your data.
- Ransomware will also attempt to spread to any connected systems including Western's central file shares. This is particularly concerning for users with elevated access privileges.
- The motive for Ransomware attacks is almost always monetary, and is easily identifiable, as the end user will generally receive either a pop up on their screen or an email demanding payment generally through a virtual currency such as BitCoin.

How does Ransomeware get onto my computer?

- A Drive-by-Download, refers to the ability of a malicious actor to download a program to a user's device without their knowledge or consent. This program, under the correct circumstances can then run without user interaction and infect the device.
- Phishing emails are the most common method of deployment. These email often appear to come from legitimate sources or possibly someone the user knows, and entices the receiver to either click on a malicious link or open a malicious attachment.

CONTACT US

KING'S Information Technology Services
Western University · Canada

Phone: 519.433.3491 x.4441
Email: support@kings.uwo.ca
Website: www.kings.uwo.ca/cyber-awareness

KING'S
Western University · Canada

Protect Yourself and King's from RANSOMWARE

What can I do to Protect King's Data?

Backup all Data

Perform frequent backups of your workstations, laptops and other devices. Verify that the backups are completing successfully and most importantly, are recoverable.

Use Central Storage

Save all King's data in the appropriate centralized data storage location. King's provided shares are centrally backed up daily.

Store Backups Separately

Store your backups on separate devices that are not accessible from the network or your computer.

Malicious actors will also encrypt your backups if they are accessible.

Stay Informed

Get to know King's/Western's Data Classification policies, and data handling standards. Participate in any Cyber Awareness training offered, and follow current Cyber news concerning threats and ransomware attacks.

What can we do to Prevent Ransomware

Update and Patch Devices

Exposed vulnerabilities in applications and Operating Systems provide an easy point of entry for ransomware attacks. Ensure both applications and the operating system of your devices are up to date with the latest patches.

Do Not click on unknown or suspicious links

Website addresses and links within email can often appear to be correct with only small variances in spelling or naming convention. Verify that the address is correct before proceeding.

Learn more about Phishing email

King's and Western provide a great deal of information regarding phishing email. Keep yourself informed through awareness training, seminars, handouts etc.

Use Virus & Malware prevention software

Install and maintain good Antivirus and Malware prevention software on all devices.

What to do in response to Ransomware

Power Off your Device

If you suspect or have discovered ransomware or other malware on your device, immediately power off your device and seek help.

Isolate your device

If you cannot power off your device, immediately remove the system from all networks. Unplug any network cable and turn off the wireless and Bluetooth functions.

Seek Help and Advice

Immediately report ransomware incidents to King's I.T. support, or contact King's ITS Help Desk (519 433-3491 or Ext. 4441)

Change your password

Once the ransomware has been removed, change your Western account password and any application passwords that you may have used during or prior to the ransomware attack.