IS RANSOMWARE TAKING YOUR DATA?

Ransomware is malicious software on your device from an unknown source that prevents access to your device and data unless a ransom is paid.

If it can connect to the internet, it is vulnerable.

MITIGATE YOUR RISK FROM RANSOMWARE:

BE VIGILANT WITH YOUR EMAILS
Be wary of links and attachments you don’t expect, even if they seem to be from a trusted source. Verify emails by calling, messaging, or sending a NEW email to the source.

Learn more about how to Report Suspicious Emails at Queen’s.

KEEP YOUR SOFTWARE UP-TO-DATE
Install updates promptly on your device, your browser, and any other software or applications you use.

And learn how IT Services can manage and deploy Windows updates, patches, antivirus for you with System Center Configuration Manager.

PROTECT YOUR DEVICE
Use anti-malware and applications from reputable stores, and make sure only YOU have access to your device. Don’t allow family or friends to use your work device.

Check the Queen’s Software Centre first to see if it has the tools and software you need.

BACK UP YOUR DATA
Store and back-up files on OneDrive for Business and Teams for free and safe storage, anywhere online access, and real-time collaboration.

Learn more about OneDrive for Business and Teams at Queen’s.

If you think your system is infected, contact the IT Support Centre.

Check out other infographics on the IT Services website.

Need help? IT Services has you covered!

(613) 533-6666 during business hours
queensu.ca/its
Online Help Form
queensu.ca/its/helpform

Published by Queen’s IT Services 2021. iso@queensu.ca

Check out other infographics on the IT Services website