Ryerson University | ROGERS cybersecure catalyst | corporate training and cyber range

Ransomware Tip Sheet General Users

What is ransomware?

There are various forms of ransomware, but in general, ransomware is a type of malicious software that a cybercriminal uses to encrypt or lock your digital files or software. Once the ransomware is installed, the cybercriminal then typically demands a ransom to unencrypt the files or software and restore your access. The size of the ransom can vary.

How does it happen?

Ransomware can be installed in your systems in many ways. The most common is where a cybercriminal will send you a phishing email, text, or phone call that appears to be legitimate. They will demand, ask, or entice you to take some type of action such as clicking on a link, opening an attachment, providing your password, or allowing them remote access. This will open a door and allow them to install the ransomware. Another common way is for a cybercriminal to find a vulnerability or weakness in your system through which they can gain access and install the ransomware.

Why should you be concerned?

If you are using a computer or phone that is connected to the internet, whether at home or at work, you are a potential target for ransomware and could be locked out of your system. Even if you pay the ransom, there's no guarantee that you regain access to your system or files.

What can you do about it?

There are measures you can take that will help you **prevent** and **prepare** for a ransomware attack.

Prevent – Things you can do to help prevent ransomware include:

- **Be vigilant.** Keep an eye out for decreases in system performance or suspicious emails, texts or phone messages. Don't click on any links or respond to any suspect requests. Try to find a way to verify the legitimacy of the correspondence and report any suspicious activity to your organizational IT support team or, if it's your home computer, refer to an IT or cyber security service to help.
- **Use cybersecurity best practices.** There are many simple, routine habits that we can adopt that will significantly reduce the likelihood and impact of a ransomware attack such as such as not sharing passwords, properly identifying and storing sensitive information, not using public Wi-Fi, not sharing organizational information on personal social media, clearing our caches and properly logging out at the end of the day.
- **Install or activate your security software.** This is always a good idea to help protect you and your system, but it may also help detect ransomware and could stop emails with malicious files.
- **Keep your operating systems and other software patched.** If your operating system or software says that there's an update, accept it. While many patches or repairs are for system or software performance, security patches often come with these updates and these will reduce system vulnerabilities or weaknesses that cyber criminals can exploit.
- **Get the training you need.** If you don't understand the threats and what they can look like, how can you take action? Get training and learn about the IT systems you use, how to recognize anomalies or potential cyber attacks, and what to do if you see something suspicious.

If you are attacked, you can pay the ransom, but this raises issues, primarily of which is that you are helping to fund criminal activity. However, there may be cases where the costs or harms of not paying are likely to be far higher.

Prepare – You should be prepared to respond to a ransomware attack by:

- **Knowing who to call.** Whether you are using an organizational IT system or your home computer, you should refer the issue to an IT professional to help provide guidance on what to do. Keep in mind that since you may be locked out of your system that any contact or reporting information you might need should be written down and available.
- **Disconnecting from the internet.** If you don't have access to an IT professional to help, disconnect from the internet and take the infected system off of your local network (e.g. wifi). This will help stop the spread of the ransomware and reduce the potential impact.
- **Backing up your files.** Losing access to your important files can be devastating. Regularly backing up your files in another location such as on a USB or in the cloud will help ensure that you have access to the most recent backed up files even if you are locked out of your system. There are many services that will do this automatically for you.