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

Ransomware Tip Sheet Business Leaders

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 several ways. One of the most common is for a cybercriminal to find a vulnerability or weakness in your system through which they can gain access and install the ransomware. Another common way is through a phishing email, text or phone call that appears to be legitimate. The email or text will entice the user to click on a link, open an attachment, provide system access or information that will facilitate installation of the ransomware.

Why should you be concerned?

If you are connected to the internet, you are not immune. Any organization or individual can be a target. If you rely heavily on digital files or have valuable sensitive data such as personal, medical, or legal information, you should be concerned. Equally, if you are well recognized within your industry or in the public domain, this raises your visibility and may likely increase your chances of being attacked. Just think about the potential consequences of an attack: whether you pay or not, there are costs both to your organization and your reputation that can have a significant impact on your business.

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:

- **Ensuring that security software is installed and activated.** This will help protect you and your system, but it may also help detect ransomware and could stop emails with malicious files.Use cybersecurity best practices.
- **Keeping your operating systems up-to-date and software patched.** System updates and patches are intended to improve system performance, but they also often include security patches that will help reduce vulnerabilities that can be exploited by cybercriminals. Install or activate your security software.
- **Establishing cyber security policies and procedures** in your organization that limit system access and privileges only to those who need it to do their job. Ensure that no unauthorized applications can be installed or executed on your systems.
- **Training yourself and your employees.** You should understand what you're dealing with as you can be a target as well. Ensure that your employees are also able to recognize common signs of phishing and other social engineering techniques and what to do if they detect suspicious activity. Also, include a reporting process so that they know who to talk to when they have concerns or questions.

If you are attacked, you can pay the ransom, but this raises issues, primarily that you are helping to fund criminal activity. However, you may be in a situation where the costs or harms of not paying ransom are far higher. Consequently, you may feel compelled to pay. Keep in mind that paying the ransom not only perpetuates the cyber criminal behaviour, but it is also is no guarantee that your system will be unlocked or your files will not be stolen or corrupted.

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

- **Having an incident response plan** that includes ransomware scenarios and exercise at least annually through a Tabletop Exercise to identify any gaps and ensure that everyone understands their roles and responsibilities. Ensure everyone has the requisite training to fulfill their responsibilities. Include crisis management activities such as confirming communications and reporting authorities, confirming communication channels and preparing draft media releases.
- **Backing up your files** often and ensuring that the backup is segregated from your operating and administrative networks to avoid them being held hostage as well. Regularly test your backups to ensure that they'll work when you need them.
- **Identifying expertise and tools** to support ransomware removal and system recovery. This can be in-house or through a third-party security service. Ensure that critical contact information is also available outside of systems you use as you may not have access to them if you are locked out.
- **Having recovery protocols in place** and ensuring that they are tested so that you can be confident that you can return to normal operations as quickly as possible.
- **Ensuring external reporting processes are in place.** If you are hit with a ransomware attack, it is a crime and it may involve compromise of personal information. In addition to internal communications, external reporting channels should be identified to include the Canadian Anti-Fraud Centre, the Canadian Centre for Cyber Security and, if personal information is compromised, to the local Privacy Commissioner.

Contact us or visit our website to learn more and keep up-to-date on our Ransomware role-based training products and events.

Rogers Cybersecure Catalyst Corporate Training & Cyber Range program offers a variety of training options, from introductory cybersecurity concepts to complex technical experiences.

Our training offerings are versatile and can be tailored to meet the specific needs of our clients and include interactive workshops and Tabletop Exercises.