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

# Ransomware Tip Sheet People Managers

## 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 increase your chances of being attacked. As a people manager within an organization, you have responsibility for your team and should ensure that they know what to do in the event that they encounter ransomware.

## 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:

- **Monitoring and promoting cybersecurity best practices.** There are many simple, routine habits that we can promote 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.
- **Ensuring that your team has security software installed and activated.** This will help protect them and the organization from cyber threats. It may also help detect ransomware and could stop emails that include malicious files.
- **Check to make sure that your team's operating systems are up-to-date and any software is 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.
- **Confirm system access and privileges for all team members.** Individuals should only have the system privileges they need to do their jobs. They should also only have access to files and software they need in the course of their work. Also, check to make sure that no unauthorized applications are installed on your systems.

- **Training you and your team** to recognize common signs of phishing and other social engineering techniques and what to do if they encounter them. Also, ensure that you are aware and guide your team on reporting processes when detecting suspicious system behaviours, emails, texts or phone calls.

If someone on your team discovers ransomware on their system, this should be immediately reported to the IT or cyber security professionals as well as senior leadership. This should instigate the organizational incident response plan.

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

- **Knowing who to call.** Whether your team is working in the office or remotely, they should know who to call if something goes wrong or they encounter suspicious activity. Typically, the first call is to the IT or cybersecurity professional who can provide further guidance and they should provide instructions. 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.
- **Understanding your role and your team's role.** If you or anyone on your team has a formal role in incident response, then ensure that the appropriate training and instructions are provided. If there are no formal responsibilities defined, guidance should be provided by senior leadership or other authority on what you should do.
- **Ensuring that your team files and software are being backed up.** This should be done often and the backups should be stored separately, away from administrative or operational systems that may come under attack. Check your back ups occasionally to see that they are relatively current and contain the expected files and software needed.
- **Having a contingency employment plan.** Often when systems go down for an extended period of time, employees that rely on those systems are often left trying to figure out what to do. Have a contingency employment plan in place should systems become unavailable due to a cyber attack such as ransomware.
- **Ensuring there's a process for your team to report the incident.** Everyone on your team should be aware of internal reporting requirements and you should be aware of when the organization should be reporting incidents to the Canadian Anti-Fraud Centre, the Canadian Centre for Cyber Security and, if personal information is compromised, 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.