What is Ransomware and How to Prevent Ransomware Attacks

Ransomware. You've heard about it at the office and probably read about it in the news. Have you ever wondered what it is, where it came from and what to do to protect against it?

What is ransomware? It is a form of malware that locks and encrypts files on a victim's computer or device, then demands a ransom payment in order to restore access.

In most cases, the victim must pay the cyber criminal within a set amount of time or they will risk losing their data permanently. However, paying the ransom does not guarantee that access to data will be restored.

The idea behind a ransomware may be simple but fighting back when you are a victim of a malicious attack can be more complex.

News stories about ransomware have become mainstream. Ransomware attacks are frequently occurring on weekends and during holiday hours, adding to the challenge of remediation. Ransomware victims must remain cognizant of these threats and be prepared to handle them. Enacting preventative pre and post ransomware mitigations is imperative to reducing any potential damage.

Where does ransomware come from?

Ransomware is typically spread via spam or phishing emails, exploitation of software vulnerabilities, or remote admin (e.g., remote desktop protocol or RDP) connections that are accessible from the Internet. Once a device becomes infected, ransomware restricts access to files by encrypting data so that a decryption key or code is required to regain access. At this point, a 'ransom' notification will pop up asking for funds before access to the data is restored.

How do I know if my device has been infected?

Notifications can vary based on the type of ransomware. They typically have a timer, a note indicating that your files have been encrypted or your access to files have been restricted and give instructions on how to regain access by paying a fee.

The example shows the notification received when infected by the “WannaCry” ransomware.

Can it spread further?

A ransomware attack may result in significant service disruption, financial hardship, and the loss of trust from stakeholders. In addition, because many of these attacks are preceded by a breach of network security, privacy issues may also arise due to cyber criminals gaining access to personally identifiable information (PII), such as social insurance numbers, home addresses, etc. Consequently, it is strongly recommended that impacted organizations obtain professional help and notify their local police service. To aid in ransomware recovery, it is strongly advised that organizations back up their data off-network to ensure that they can recover from an attack, so they are not left in the position of having to consider paying a ransom.

Reporting ransomware

Most police services do not endorse the payment of ransomware as it encourages further victimization. The Ontario Provincial Police (OPP) issued an advisory warning about the risks of paying ransomware demands, as there is no guarantee that paying will result in all encrypted data being recovered.

The role of law enforcement is to investigate the incident to find the cyber criminals who are responsible. Officers and analysts will work alongside the victim to preserve and collect any digital evidence and intelligence without interfering in the organization’s remediation efforts. Data collected by law enforcement as part of the investigation will remain confidential and analyzed solely for the purpose of the investigation. While retaining confidentiality, the data may also be used for the purposes of threat intelligence gathering and trend analysis for the further enhancement of the OPP outreach program.

The local police are building the capacity and capability to investigate cyber crimes including these complex cases. Unfortunately, cyber crimes still often go unreported. Cyber crimes must be

reported so that the scope of the criminal activity is understood, properly investigated, and that the victims receive the necessary supports.

Preventing ransomware attacks starts with awareness

Phishing and fraudulent emails remain a prominent way in which attackers can gain access and compromise security. Educating users on cyber security best practices is the first step in tackling the ransomware issue.

Below are some DOs and DON'Ts of ransomware:

- **DO conduct internal phishing campaigns** to educate employees on the dangers of phishing.
- **DO enable the use of passwords** containing lower / upper case letters, numbers and special characters wherever possible.
- **DO recommend that passphrases are used for passwords** when possible, avoiding dictionary words. Get more details on what passphrases are and how to use them.
- **DO encourage users not to use the same password** for all their accounts; different passwords for different accounts is the best practice. Consider using a password manager to keep track of them.
- **DON'T automatically open email attachments.** Email is one of the main methods for delivering ransomware.

For Cyber Security educational materials and advice contact: cyberadvice@ontario.ca.

Step 1: Preparation

Preparation is key to preventing malicious infections, including ransomware, and to reducing the impact when they occur. Here are some tips to protect yourself from a ransomware attack:

Have backups

- Backup all data on an isolated and protected server with separate authentication protocols and credentials.
- Ensure that your backup strategy allows you to restore files to any point in time up to a minimum of two weeks prior to the most current backup.

Regularly patch your software

- Make sure to keep up to date with all the latest patches and software upgrades.

Secure services on your systems

- Use multi-factor authentication for login wherever possible, especially when a system is accessible from the Internet.
    - Multi-factor authentication is easy to set up on Office365 and Google Suite services.

- Do not have RDP or other remote admin connections exposed on Internet-facing systems. It is trivial for attackers to exploit these systems.
    - Remote access services are frequently targeted by attackers. You may have a RDP service open to the Internet if you have external consultants working remotely on your systems and not using a virtual private network (VPN).
    - Ask your IT provider if you are not sure whether you may have a RDP open to the Internet.
    - Instead of exposing RDP directly to the Internet, consider using a VPN. Ask your IT Service provider about this option.
    - Contact Cyber Security at cyberadvice@ontario.ca for tips on securing remote access services.
- Restrict Administrator / Root privileges.
- Use Endpoint Anti-Malware Protection.
- Disable unused accounts on your applications and systems.

Develop and document an incident response process

Develop policies, procedures and operational guidelines, and ensure they answer the following guiding questions:

- Do you know who to contact in case of a Cyber incident?
    - These resources should have numbers that are reachable 24x7x365 as many attacks occur on weekends and holidays.
- Do you know what entities your organization connects with? Are you connected to another group / organization to provide or receive data / services?
    - You may have legal obligations to notify other organizations in the event your environment is infected with malware. Understand what these obligations are.
- Can you procure cyber incident response and legal services quickly if needed?
    - Consider putting these services on hold if you can.
- Do you have cyber insurance?
    - If you do have cyber insurance, ensure that the number to contact them is easily accessible. Their services may include legal and cyber incident response professionals who can provide you with advice and guidance.
- Do you have a Business Continuity Plan for cyber incidents?
- Have you identified resources that can prepare and distribute a public statement in the event you suffer a breach?
- Do you have a communication plan for informing internal staff and your clients about a cyber incident?

Assess threat detection capabilities

- What are your in-house capabilities around detecting and responding to cyber threats?
- How can you address gaps (if any)?

Perform ongoing collection and analysis of threat intelligence

- Are you subscribed to information feeds about potential cyber threats to your sector?
- Consider signing up for the Canadian Centre for Cyber Security's alerts and advisories.

Email protection

- Do you have spam filtering or any email protection in place? Spam filtering will reduce your exposure to fraudulent, phishing and potentially malicious messages.
- Consider email attachment filtering, allowing only attachment types required forbusiness.
- Consider sanitizing attachments such as macros in Microsoft office files and JavaScript before email attachments are delivered to users.
- Consider having email attachments scanned by an anti-malware tool.
- Consider disabling active content in email messages, this means that users will needto copy and paste web addresses into their browser.
- Consider an email / phishing education campaign to make sure that all users are familiar with phishing and related threats.
- Consider the Malicious Email Mitigation Strategies for more information and guidance.
- Contact Cyber Security at cyberadvice@ontario.ca if you have any questions or need more information.

Note: See the links in the Additional Resources section for Office365 and Google Suite configuration tips if you are using either of those services for email.

Step 2: Containment neutralization

Easy steps to contain and neutralize a malware infection (including ransomware):

1. If you have an IT service and / or cyber insurance provider, call them immediately. It is also strongly recommended to notify your local police.
2. Take steps to isolate your environment from any organization that connects with yours. This can be in the form of firewall blocks, disabling VPN or other external connections.
3. Contact organizations that are connected to yours and advise them of the situation so that they can take precautions on their end.
4. Speak to your users and try to identify the source of the infection. Did they open an email attachment or click on a strange link? Record these details. They can also help you identify security gaps.
5. If you have a Web Security Gateway, Firewall or Proxy service, check the log files for suspicious alerts. These can identify IP addresses for you to block and could be used to help other organizations determine if they were impacted. Your IT service provider should be able to assist with this.
6. Check if any information was compromised, especially PII.
    a. This can be tricky to determine without professional help. It is strongly recommended to bring in professional services, such as an IT security firm with incident handling / forensic capabilities, to help with this step.

b. If you are unable to rule out whether or not PII was compromised (which will likely be the case early on in an incident), contact the Privacy Commissioner of Ontario (416) 326-3333.

If you have staff on-site to respond to the incident, consider the steps below:

1. **Are the impacted systems connected to your organization's network?**
    a. If they are connected to your organization's network, disconnect them immediately.
    b. Does the infected system(s) have access to network shares? If it does, the shares are likely impacted; especially if it was a ransomware infection.
    c. Can all infected machines be immediately identified and isolated?
    Isolation can be in the form of pulling network cables, disabling switch ports, and disabling VPN accounts used by impacted remote users. It is not recommended to power off systems as valuable forensic evidence can be lost. Powering off systems should be a last resort.

2. **For ransomware infections, is a copy of the ransom note available?**
    a. Keep record of the ransom note file content and file extension. Both can be used to identify the ransomware family.
    b. Make note of the "Properties" tab of the ransom note file. This can help you identify where the infection originated from.
    c. Check to see if the user listed as the Owner of the file is a user account with a non-generic name. If it is, have the user disconnect from the network (VPN account disabled, active directory account disabled, machine isolated).
    d. Google the specifics of the note file, the extension of the file name and the location of the ransomware executable to try to identify the family it belongs to. Check resources below to see if a decryptor might be available.
    e. Have the file extensions changed?

3. **Are there any email addresses or other indicators of compromise available?**

4. **Did anyone receive any unusual emails, or accidentally click on any unusual sites?**

5. **Have any IT staff carried out any actions, or attempted to clean the infection?**

6. **Was antivirus software installed and up-to-date?**

7. **Is File Access Auditing enabled on the infected server?**
    - This can help you determine if a specific user account created / modified files as a result of the infection so you can have it disabled. It can also aid in determining if a compromised account accessed sensitive information.

Step 3: Data recovery

Questions to raise and items to consider:

1. Do backups exist?
2. If backups exist, what kind of backups are they (e.g. cloud, tape, age, etc.)?
3. Have the backups been tested?
4. If backups are encrypted or otherwise not available, can key data be recovered via temporary files, forensic methods or through a decryptor?
5. Once all impacted systems have been identified and isolated, firewall blocks, disabled VPN accounts and disconnected external connections restricting access to the organization's network can be removed / restored. This step should only be taken on the advice of your IT service / Cyber insurance partners.
6. Once the investigation has been completed, can the impacted machines be re-imaged?

Additional resources

Education and awareness links

- The Canadian Anti-Fraud Centre
- SANS Institute's Enterprise Survival Guide for Ransomware Attacks
- Windows Defender Advanced Threat Protection– Ransomware response playbook
- Canadian Centre for Cyber Security - Ransomware: How to Prevent and Recover
- SERENE-RISC's Cyber Security Tips

Ransomware decryptors

When you have identified the ransomware and are looking for decryptors, please use the links / resources below:

- Kaspersky's Free Ransom Decryptors
- No More Ransom's Decryptor
- Gitlab's Free Ransomware Decryptors List

Office365 and Google Suite configuration

Do Google or Microsoft host your email? Check out the links below for information on enhancing security for Google Suite and Office365.

- Google Suite - Advanced Phishing and Malware Protection
- Protect Against Threats in Office365