



## CANADIAN CENTRE FOR CYBER SECURITY

# RANSOMWARE: HOW TO PREVENT AND RECOVER

SEPTEMBER 2019

ITSAP.00.099

Ransomware is becoming an increasingly common threat, targeting everyone from individuals and small businesses to large private enterprises and government organizations. As such, it's important to develop a strategic plan to prevent an attack, as well as to prepare yourself for the worst-case scenario and think about how you would recover if you were ever infected by ransomware. This document describes how ransomware works, the steps you can take to prevent it, whether to pay the threat actors or not, and what you should do to recover from an attack.

## WHAT IS RANSOMWARE?

Ransomware is a type of malware (malicious software) that makes data inaccessible. When ransomware infects a device, it will either lock the screen or encrypt all of the files. Ransomware can also use a network to spread to other connected devices. It will be obvious if your device is infected with ransomware because it will announce itself with a page explaining that your files are inaccessible and that you need to pay a ransom to retrieve them. Sometimes this ransom note is made to look like it came from a law enforcement agency, and it will say that your files were locked because your computer was used for some form of illegal activity.

The attacker will usually ask for the ransom payment to be made in the form of a digital currency (e.g. Bitcoin) since the transfer would be untraceable. The attacker will usually give a time limit to pay the ransom. After the time limit, the price might increase or the attacker might threaten to destroy all of the files so they can never be recovered.

## PREVENTING RANSOMWARE

While there is no way to fully prevent ransomware, there are a number of steps you can take to minimize your risk.

### **Provide security awareness training for employees.**

Email phishing is the most common method that attackers use to spread ransomware. Regardless of what security features are installed on someone's device, if a malicious link is opened, that device could be compromised. Therefore, it is important that employees know how to recognize phishing attempts, and that there is a procedure in place for employees to report them to the organization's IT desk.

### **Patch operating systems (OS) and third-party apps.**

Unpatched and unsupported operating systems are easy vulnerabilities for cyber threat actors to exploit. Be sure to keep your OS and all third-party apps patched with the newest updates.

**Disable macros.** A number of ransomware strains are sent as Microsoft Office attachments. When a user opens the attachment, they are asked to enable macros to see the contents of the document. Once they enable macros, the actual ransomware payload will download and execute. Keep macros disabled by default, and make sure employees are aware that a prompt to enable macros can be a red flag.

**Use least privilege.** Users should only have the minimum amount of access required to fulfill their job duties. Restrict administrative privileges as much as possible, and ensure administrative users are required to confirm any actions that need elevated rights.

**Back-ups, back-ups, back-ups!** Be sure to perform frequent back-ups and store them offline. If ransomware is planted on just one device, it can spread across your entire network quickly and covertly. Make sure your back-ups are not connected to the Internet or any local network. These clean, offline back-ups are the key to recovery if you are ever infected by a ransomware attack. Back-ups allow you to restore your safe files without having to deal with the cyber threat actor and their ransom demands, greatly reducing the impact that a ransomware attack would cause for you. Cloud customers should understand the back-up limitations and the available configurations offered by service providers. The goal of your cloud service is to ensure that back-ups are secured to your level of satisfaction.

**Practice recovering.** You should run a simulated ransomware event and practice recovery procedures. How long would it take you to get yourself back online? For many organizations, it takes a lot longer in practice than anticipated. These exercises can show you what to focus on to improve your recovery procedures.

Together, these steps can help you create a strategic plan for preventing and recovering from ransomware. Various cyber attacks should be included in your business continuity planning (BCP) so that you know the level of impact your organization is willing to accept from these events and how quickly you need to get your devices back up and running.

## AWARENESS SERIES

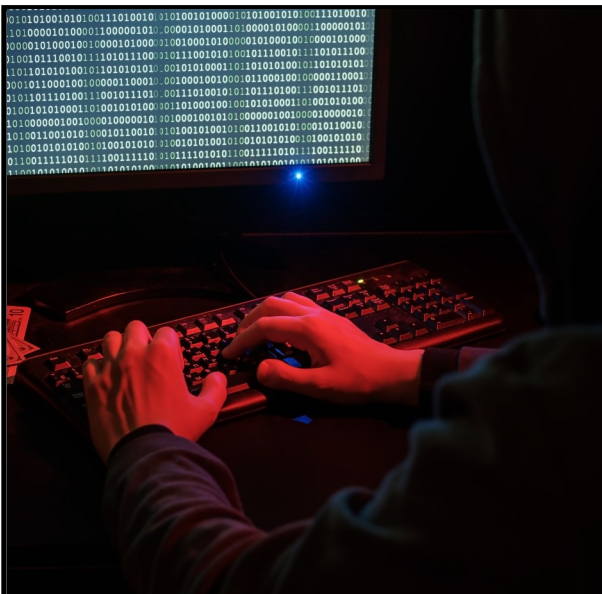
© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

## RECOVERY AFTER AN ATTACK

If you do get infected with ransomware, know that paying the ransom does not guarantee that the files will be decrypted. Some attackers continue to demand more money in exchange for nothing. Also, even if the attacker does release the files, you are still in a situation where you have had a data breach. The attacker had access to your files and most likely made copies of them. Your information might be leaked, or the attacker might try to access exposed online accounts. Paying the ransom also encourages cyber threat actors to continue infecting devices with ransomware. It validates the use of cybercrime and shows that threat actors can generate revenue from it. Cyber threat actors usually put a bigger price on the files of large organizations.

The decision to pay or not to pay a cyber threat actor should be based on your organization's risk tolerance. For example, some organizations find themselves in a tight spot after getting infected with ransomware and choose to pay the ransom to recover sensitive files. This example underlines the importance of frequently backing up your files and saving these back ups in a safe location in order to keep options open for self-recovery without paying ransom.



If ransomware has been planted on one of your devices, take the following steps (if needed, hire a cyber security specialist to help):

- 1. Isolate the device immediately.** Remove the device's access to the Internet and any other networks. Isolation prevents the infection from spreading to other connected devices or any cloud services that you use. Some strains of ransomware are designed to stay dormant on a device and quietly spread to other network-connected devices before actually encrypting the files. In these cases, you may not be able to stop the ransomware from spreading. Isolating the device is paramount.
- 2. Identify what type of ransomware it is.** There are a number of online tools that you can use to check if your specific ransomware has been seen before and if there is a solution available to decrypt it. Take note of any URLs to which the ransom page is trying to direct you, as this might be a clue as to the type of ransomware. Also, look at your encrypted files to see if they have been renamed with a new file extension. This technique is often used by cyber threat actors. For example, the Locky ransomware in 2016 renamed files with ".locky" as the extension. This may indicate the name of the ransomware and will help you track down any solutions online.
- 3. Remove the ransomware.** If you're lucky, you may locate a decryption tool online that you can use to clear the ransomware. Then you can proceed to steps 5, 6, and 7. If you're not so lucky, carry on with step 4.
- 4. Reset the device and wipe all the data.** If there is no decryption tool available online for your strain of ransomware, you will need to return the device back to its factory settings and wipe all of its data (including the ransomware). You can then restore all the files from your most recent and clean back-up that has been stored safely offsite.
- 5. Time for some updates.** After you've dealt with the infection, you'll need to do some updates to prevent a future attack. Patch your operating system and make sure all anti-virus, anti-malware, and firewall software are up to date.
- 6. Change passwords.** Be sure to change the passwords on any accounts that had been accessed from the previously infected device (e.g. social media, banking, email). The cyber threat actor most likely has copies of this information, including the log-in credentials for various websites.
- 7. Report the crime.** Although it may not feel useful, it is important to report the ransomware to law enforcement and the Canadian Anti-Fraud Centre. If you are unlucky enough to be the first person ever hit by this strain of ransomware, then at least law enforcement will be made aware and can monitor for subsequent infections.
- 8. Train your users.** Spend the time and effort to train users on cyber security. Help prevent threat actors from infecting you with ransomware by learning to identify attempted phishing attacks. Read *ITSAP.00.100 Spotting Malicious Email Messages* for more information.

During a ransomware attack, the cyber threat actor may use intimidation tactics to try to make you pay right away. Remember not to panic. Ideally, you frequently back up your information, giving you something to fall back on. At most, you may lose a couple days' worth of data, but this is certainly a safer choice than getting financially involved with a cyber threat actor.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?  
Come visit us at Canadian Centre for Cyber Security (CCCS) at [cyber.gc.ca](https://cyber.gc.ca)

