RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

PREVENT RANSOMWARE

How It Happens

1. User clicks on link or opens attachment in spam/spoofed email, or

2. User unknowingly visits malicious/ compromised website, or

3. User plugs in infected device (e.g., USB key or USB hard drive).

4. After successful compromise, cybercriminal installs malware.

5. Malware is released and infection spreads.

6. Computer is locked and message appears demanding payment to unlock files or system.

7. This can happen on a single computer or an entire network.

8. A message will warn that only the scammer can decrypt the files. Not true! Visit links below for more guidance.

For more help visit:
cyber.gc.ca
nomoreransom.org

If your system gets infected with ransomware - **you are the victim of a crime** - report it to the police as soon as possible!

We strongly recommend that you do not pay the ransom. Take necessary mitigation measures with the help of IT professionals to minimize further harm.

Protect & Prevent

Paying is not a guarantee that your computer or network will be unlocked. It is better to **PROTECT** your systems with measures that help **PREVENT** infection.

Large Businesses – a multi-point protection approach is best:

- Email and Web – block spam and access to malicious links.
- Server– protect servers from exploitable vulnerabilities.
- Network and endpoint – prevent ransomware from spreading and running on endpoint.

Small Businesses – a two-point approach to protection is effective:

- Email and Web– block spam and access to malicious links.
- Endpoint– block access to malicious/compromised sites and prevent ransomware from running.

Home User – one step provides necessary protection:

- Use a security solution that stops spam, prevents access to malicious links and stops infection.

Follow Good Cyber Hygiene Rules

Use strong passwords – 12+ characters with numbers, symbols, upper and lower case letters.

Install reputable antivirus and malware software; use network firewalls; secure your router.

Use multi-factor authentication – such as a code sent to your cell phone after entering your password.

Avoid opening emails from unknown addresses or clicking links embedded in them.

Regularly update software to protect against the latest vulnerabilities. Follow instructions from software provider.

Create backup copies on at least 2 different devices with 1 backup stored in a separate location.