RANSOMWARE BULLETIN

RECOGNIZE IT!

What is Ransomware?
It is malicious software also known as malware, which infects a computer and denies access to the system or data, and demands a sum of money to restore the information. At present, the most common form of ransomware will encrypt data. Victims will receive an on-screen alert stating their files have been encrypted or a similar message, depending on the type of ransomware. Here is an actual example:

PERSONAL COMPUTER USER

REJECT IT!

How can I protect myself?
• Do not click on links or open attachments in e-mails sent to you by someone you do not know.
• Do not provide personal information over the phone or online to untrusted sources.
• Install only trusted software.
• Back up your system/data regularly and keep the backups on a separate removable hard drive. Don’t forget to disconnect when done. If possible, check the backup(s) from a separate computer that uses a different operating system.
• Install a reputable security software suite on all devices, including personal computers, mobile phones and tablets.
• Secure your wireless router.²³
• Disable file sharing and remote desktop.
• Make sure all your software, including anti-virus software is up to date on all your devices including personal computer, mobile phones and tablets.

BUSINESS COMPUTER USER

REJECT IT!

How can I protect my business?
• Train and educate staff on good security practices.
• Do not click on links or open attachments in e-mails sent to you by someone you do not know.
• Use a reputable security software suite.
• Restrict administrative privileges.
• Back up your system/data regularly to a cloud or removable media such as an external hard drive not constantly connected to the server. If possible, check the backup (s) from a separate computer that uses a different operating system.
• Use application whitelisting to help prevent malicious software and unapproved programs from running.⁴
• Make sure all software, including anti-virus software, is up to date on all computers, servers and devices including mobile phones and tablets.
• Develop a business continuity plan and incident response plan.


1,600 ransomware attacks a day.¹ By September 2016, the attacks nearly doubled. Those are the known cases. Unfortunately, many incidents still go unreported.


Bulletin 1. Version 1.0
May 2017
PERSONAL COMPUTER USER

REPORT IT!

How should I respond?
If you become a victim, do not panic. Do not do anything further on your computer. Contact a trusted IT professional who can try to isolate the threat.

Report the incident to your local police force of jurisdiction. Please remember that every report counts and is a valuable tool for investigators.

Please also contact the Canadian Anti-Fraud Centre (CAFC) by reporting the incident online 24/7 at: www.antifraudcentre-centreantifraude.ca, select “Report an Incident”, and the link to the “Fraud Reporting System (FRS)”, or alternatively call the CAFC at 1-888-495-8501, between 8:30 am and 5 pm EST Monday to Friday.

Additional help may be found on the ‘No More Ransom’ website at https://www.nomoreransom.org. The site is a tool to help victims retrieve their data, and was developed by law enforcement and IT security companies globally.

We strongly suggest that you **DO NOT PAY THE RANSOM** for the following reasons:

- There is no guarantee that your data will be recovered.
- You may be extorted for more money after the original ransom is paid.
- You can make yourself a future target.
- Extortion via Ransomware is a criminal offence, and the money you pay will be used to fund criminals and/or criminal organizations and motivate them to further victimize others.

We understand that there may be legitimate reasons for paying the ransom, such as the potential harm of not having access to the data as a result of no backup. We still encourage you to report incidents even if you have paid the ransom demanded by the extortionists.

Additional guidelines can be found at:
https://www.cyber.nj.gov/threat-profiles/ransomware/

BUSINESS COMPUTER USER

REPORT IT!

How should my business respond?
Do not do anything further on your computer. If available, consult your local IT department or an IT professional for assistance.

Critical infrastructure, businesses and provincial/territorial/municipal governments should immediately report the incident to the Canadian Cyber Incident Response Centre (CCIRC) via e-mail at: ps.cyberincident.sp@canada.ca, or visit https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccirc-en.aspx for more information. CCIRC will assist in mitigation and prevention.

You are encouraged to open a criminal investigation into the matter by reporting the incident to your local police force of jurisdiction and informing CCIRC you have done so. Please remember that every report counts and is a valuable tool for investigators.

You may also contact the Canadian Anti-Fraud Centre (CAFC) by reporting the incident online 24/7 at: www.antifraudcentre-centreantifraude.ca, select “Report an Incident”, and the link to the “Fraud Reporting System (FRS)”, or alternatively call the CAFC at 1-888-495-8501, between 8:30 am and 5 pm EST Monday to Friday.

Additional help may be found on the ‘No More Ransom’ website at https://www.nomoreransom.org.

Additional guidelines can be found at:
Get Cyber Safe Guide for Small and Medium Businesses:
US-CERT Tips
https://www.us-cert.gov/ncas/tips
NIST (National Institute of Standards and Technology) Guide:

In consultation with:

This document is the property of the Royal Canadian Mounted Police (RCMP), Federal Policing Criminal Operations. For any enquiries concerning the information, please contact the originator of the document.