AWARE | SECURE | RESILIENT

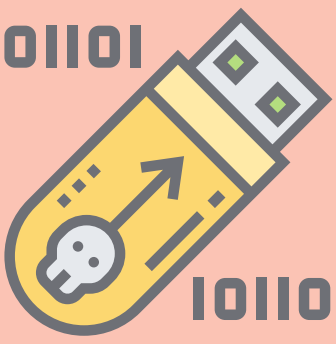
A GUIDE TO RANSOMWARE

Protect yourself from ransomware attacks

WHAT IS RANSOMWARE?

- Ransomware is a type of malware (malicious software) that locks access to, or encrypts the data on a computer system or network of systems. Victims are requested to pay a ransom in return for regaining access to the data and systems.
- New strains of ransomware are being released very frequently and the most recent forms are also exfiltrating data before encryption. This provides the cyber-criminals with an additional way to extort money out of the victims by threatening to release the data unless a ransom payment is made.

HOW DOES RANSOMWARE INFECT YOUR SYSTEM?

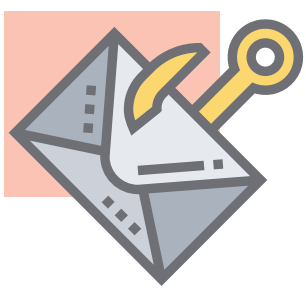


- Computers are infected with ransomware via a number of methods. Sometimes users are tricked into running legitimate-looking programs and documents which contain the ransomware. These may arrive via authentic-looking email attachments or links to apparently genuine websites (known as phishing).
- More recently, ransomware infections are being seen that rely on unpatched vulnerabilities in software, and simply visiting a malicious website can be enough to result in being infected.
- Ransomware may also be introduced as a result of another malware infection. Botnets are a common way for ransomware to be introduced to a system and networks. Botnets infect computer systems and wait for commands from a Command & Control (C2) server which could include the download of ransomware.

RANSOMWARE PREVENTION

ANTI-VIRUS SOFTWARE

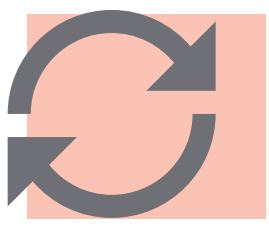
A reputable security product is a necessity for any computer system or mobile device. Anti-virus protection is a valuable tool that will search for, identify and remove any known malware, plus typically contains other features that will keep you and your system protected. Ensure it is enabled, regularly check the status and updates. Set it to automatically complete full scans, ensuring that a full scan is performed at least once a month.



DEFEND AGAINST PHISHING ATTACKS

Check for obvious signs of scam emails, like poor spelling or grammar. Does the sender's email address look legitimate or is it trying to disguise itself as someone you recognise? Be wary of emails asking you to click links or open attachments from unknown senders. If in doubt, contact the legitimate person or organisation directly using known contact details.

KEEP YOUR SOFTWARE UPDATED



Ensure that applications such as your web browser are always up to date to reduce the possibility of a vulnerability being exploited to infect your computer. Always update your operating system when it is suggested as security flaws are regularly patched. Anti-malware signatures should also be kept up to date to give you the best chance of being protected.

MACRO-SECURITY

Unless you are sure of the authenticity of a document, do not enable or run macros if asked. Macros are automated procedures (typically built into spreadsheets and word processed documents) that can be used to execute code which can download and install malicious software onto your system.

Additional preventative measures for ransomware can be found on our OCSIA Advisory Notices webpage.

AWARE | SECURE | RESILIENT

BACKUP YOUR IMPORTANT DATA

- You should keep backups of any important files that you may have.
- Do not store them on the same system as the original files and do not store them on a device connected to your network as ransomware can spread to network-connected systems.
- If your files are being stored on an external hard drive, disconnect it from the system when not in use.
- It is recommended to follow the "3-2-1" rule - Have at least 3 copies of your important data, on 2 devices with 1 of those backups being offsite.

WHAT TO DO IF YOU HAVE BEEN INFECTED:

- It is highly recommended that you do not pay the ransom - it encourages and funds the attackers, and there is no guarantee that you will be able to regain access to your files.
- Immediately disconnect your computer from the network by unplugging any network cables, disconnecting Wi-Fi and turning your computer off.
- If at work, inform the security team of the situation without delay and await further instructions.
- If using a home computer, unless you are comfortable with formatting and re-installing your Operating System, contact a qualified IT repair centre or experienced IT technician.
- There is a high chance that your data will not be retrievable if you have not backed it up prior to infection.

WHAT ABOUT "DECRYPTORS"?

- Some reputable cyber-security firms and researchers have started producing "decryptors" for some of the variants of ransomware in circulation, however, these decryption tools are specific to each version of ransomware so using the incorrect tool may result in further encrypting your files.
- It is highly recommended that you consult with an experienced IT specialist to determine if, and how, your files can be decrypted.
- No More Ransom () is a website with a collection of official decryptors for various ransomware strains and versions.

For more cyber-security guidance and resources, please take a look at our OCSIA Knowledge Base.

If you have any concerns, or have been affected by a cyber-related issue, report it to OCSIA by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia