

Understanding Ransomware

Ransomware

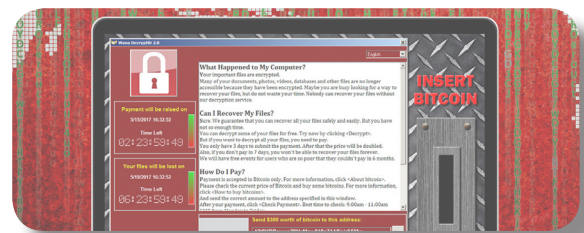
Ransomware is a form of malware (a virus) that encrypts files, or denies the user the ability to access their device, or both. There are many forms of ransomware, but they all lead to a demand for payment of a ransom for access to be allowed.

Attacks typically come in the form of phishing emails, downloading free software, and remote access scams (someone being provided access to another person's device and installing ransomware whilst in control). Once the ransomware has been executed, such as by clicking on links or attachments, the criminals have largely automated their whole process. Pop-ups or other screen messaging will alert the user to "a virus" or "encryption" or "computer being locked". A contact point will be provided, typically with a short timeframe to respond to the ransom demand.

Detecting Ransomware

There are two ways to detect ransomware:

1. prior to executing the malware and
2. after executing the malware. The best way of detecting it before it's executed is through antivirus. Make sure you run antivirus on all devices frequently. The other way is when it's been executed and a demand is made.






Preventing Ransomware

- 1. Ensure you back-up all of your data.
- 2. Run anti-virus frequently and make sure it's the most recent version – millions of viruses are created each year so your anti-virus needs to keep up with these.
- 3. Turn off your cloud storage when you are not using it (like Google, DropBox, OneDrive etc).
- 4. Keep your operating system and apps/ software updated.
- 5. Consider blocking ads and pop-ups, and think twice before downloading freeware (free downloads) without checking their security first!
- 6. Become familiar with how to spot phishing emails and never provide remote access to your device when someone calls or emails you first.

Understanding Ransomware

Responding to Ransomware

There are hundreds of ransomware types, but unfortunately most cannot be decrypted. Ransomware encrypts and the criminals using it have the tools to decrypt. Before you think about paying, you may want to try the following:

-  EUROPOL and a number of software security vendors have launched a free decryption check called CRYPTO SHERIFF that can be accessed at nomoreransom.org.
-  Decryption services – these are by no means a guaranteed result and most cost money.
-  Assess what's at risk and what would be lost. If there's too much at stake you may have to consider paying but be careful, you're dealing with criminals.



Ransomware & Mobile Phones

Ransomware targeting mobile phones is an emerging trend internationally that is presently targeting the Android phone market, but likely to transition to other operating systems. Ransomware may infect a phone by following a spam link that downloads an application without your knowledge or by installing legitimate applications such as games that may have the program embedded within them. Visiting certain websites, such as pornography streaming services, may also trigger its installation. Please see our [Ransomware & Mobile Phones Fact Sheet](#) for more information.

Other Fact Sheets

- | | | |
|---|--|--|
|  Credit Reporting Agencies |  Engaging Organisations |  Devices and Technology |
|  Scam Prevention and Education |  Social Media |  Your Rights |

Disclaimer © 2018 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.