TIPS & ADVICE

EUROPOL EC3 | European Cybercrime Centre

To Prevent Ransomware from Infecting Your Electronic Devices

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files, demanding that a ransom is paid through certain online payment methods (and by an established deadline) in order to regain control of your data.

It can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan).

It is a scam designed to generate huge profits for organised criminal groups. To prevent and minimise the effects of Ransomware, Europol's European Cybercrime Centre advises you to take the following measures:

DOS

UPDATE YOUR SOFTWARE REGULARLY.

Many malware infections are the result of criminals exploiting bugs in software (web browsers, operating systems, common tools, etc.). Keeping these up to date can help to keep your devices and files safe.

USE ANTI-VIRUS SOFTWARE.

Install and keep anti-virus (AV) and firewall software updated on your devices. AV can help keep your computer free of the most common malware. Always check downloaded files with AV software.

BROWSE AND DOWNLOAD SOFTWARE ONLY FROM TRUSTED WEBSITES.

Use official sources and reliable websites to keep your software patched with the latest security releases. Always use the official version of software.

REGULARLY BACK UP THE DATA STORED ON YOUR COMPUTER.

Full data backups will save you a lot of time and money when restoring your computer. Even if you are affected by Ransomware, you will still be able to access your personal files (pictures, contact lists, etc.) from another computer. There are a number of high quality data backup solutions available on the internet for free.

REPORT IT.

If you are a victim of Ransomware, report it immediately to your local police and the payment processor involved. The more information you give to the authorities, the more effectively they can disrupt the criminal infrastructure.

CONSULT YOUR ANTI-VIRUS PROVIDER ON HOW TO UNLOCK AND REMOVE THE INFECTION FROM THE DEVICE.

There are numerous official websites and blogs with instructions on how to safely remove this type of malware from your electronic devices. Always consult www.nomoreransom.org to check whether you have been infected with one of the Ransomware variants for which there are decryption tools available free of charge.

DON'TS

CLICK ON ATTACHMENTS, BANNERS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN.

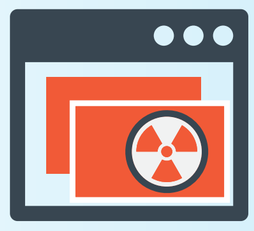
What looks like a harmless advertisement or image can actually redirect you to the website from where the malicious software is downloaded. The same can happen when opening attachments in emails received from unknown sources.

INSTALL MOBILE APPS FROM UNKNOWN PROVIDERS/SOURCES.

Always download from official and trusted resources only. In the settings of your Android device, always keep the option "Unknown sources" disabled and the "Verify Apps" option checked.

TAKE ANYTHING FOR GRANTED.

If a website warns you about obsolete software, drivers or codecs (programs that encode and decode your data) installed on your computer, do not fully trust it. It is really easy for criminals to fake company and software logos. A quick web search can tell you if your software is really out of date.



INSTALL OR RUN NON-TRUSTED OR UNKNOWN SOFTWARE.

Do not install programs or applications on your computer if you do not know where they come from. Some pieces of malware install background programs that try to steal personal data – for more information on this, see our information sheet on Identity Theft.

DO NOT PAY OUT ANY MONEY.

Paying does not guarantee that your problem will be solved and that you will be able to access your files again. In addition, you will be supporting the cybercriminals' business and the financing of their illegal activities.