TIPS & ADVICE

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

To Prevent Police Ransomware Infecting Your Computer

If a message claiming to be from a law enforcement agency pops up on your computer screen and accuses you of having visited illegal websites, then you have been infected with "Police Ransomware". This is malicious software that can lock your computer and also encrypt its data and files, demanding that you pay a fine to get them unlocked/decrypted.

This type of malware can not only infect computers but also Android smartphones and tablets.

This type of 'ransom' demand would never be issued by a law enforcement agency. 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 (EC3) 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 you safe.

USE ANTI-VIRUS SOFTWARE. Anti-virus (AV) software can help keep your computer free of the most common malware. You can easily find many free options of such software. Always check downloaded files with AV software. Do not install programs or applications on your computer if you don't know where they have come from.

BROWSE AND DOWNLOAD SOFTWARE ONLY FROM TRUSTED WEBSITES. Use official sources and reliable websites to keep your software patched with the latest security releases.

REGULARLY BACK UP THE DATA STORED ON YOUR COMPUTER. There are a number of high quality data backup solutions available on the Internet for free. Full data backups will save you a lot of time and money when restoring your computer. Even if you are unlucky enough to be affected by Ransomware, you will still be able to access your personal files (pictures, contact lists, etc.) from another computer.

REPORT IT. If you are a victim of Ransomware, report it immediately to your local police and the payment processor involved. Law enforcement agencies throughout the EU and around the world work together to disrupt the activities of identity fraudsters and bring scammers to justice. The more information you give to the authorities, the more effectively they can target the most dangerous criminal organisations.

CONSULT YOUR ANTI-VIRUS PROVIDER ON HOW TO UNLOCK AND REMOVE THE INFECTION FROM THE COMPUTER. There are numerous official websites and blogs with instructions on how to safely remove this type of malware from your computer.

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

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 also 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. No law enforcement agency will ever ask citizens to pay a fine in such an aggressive way. None of the means of payment proposed for paying the fine are currently used by police or any courts of law. In addition, even if you decided to pay, there is no guarantee that your problem will be solved.

Created by Europol