Tips & advice 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 by "Police Ransomware". This is malicious software which locks your computer and then demands that you pay a fine in order to get it unlocked.

This type of demand will never be issued by a law enforcement agency. It is a scam designed to generate huge profits for organised criminal groups.

In order to prevent and minimize the effects of Ransomware Europol's Cyber Crime Centre advises you to take the following measures:

DO:

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 software can help keep your computer free of the most common malware; there are even many free options. 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 last 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'T:

CLICK ON 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.

TAKE ANYTHING FOR GRANTED. If a website warns you about obsolete software, drivers or codecs (programs that encode and decode you 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 EXECUTE 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 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.