PETYA RANSOMWARE: WHAT CAN YOU DO?

EUROPOL EC3 | European Cybercrime Centre

IF YOU HAVE BEEN INFECTED:

Do not pay. You will not only be financing criminals, but it is unlikely that you will regain access to your files. This is particularly relevant in the case of Petya, as the email account used to manage ransom demands has been blocked, thus disabling attackers' access to the only communication channel known at the moment.

Report it to your national police. Make sure that you **keep a copy of the phishing email** received from the attackers and provide it to the police. This will help law enforcement with their investigation.

Disconnect the infected device from the internet. If the infected device is part of a network, try to isolate it as soon as possible, in order to prevent the infection from spreading to other machines. You can then format the hard drive, reinstall the operating system and apps, run any available updates and, finally, restore the locked files from your back-up device.

IF YOU HAVE NOT BEEN INFECTED:

Keep all apps and operating system up to date, making sure that you install all Microsoft patches as soon as they are made available. If the device offers the option of automatic updates, take it.

Back-up your data. Even if you are affected by ransomware, you can easily retrieve your files. It is best to create two back-up copies: one to be stored in the cloud and one to store physically.

Use **robust security products** to protect your system from all threats, including ransomware.

Do not use high privileges accounts (accounts with administrator rights) for daily business.

Do not click on attachments or links that accompany suspicious or unexpected emails, even if they seem to be coming from a trusted party such as a bank or an online store. Trust no one.

For more tips and for the latest available decryption keys, visit https://www.nomoreransom.org/

NO MORE RANSOM!

Created by Europol