Ransomware: 'WannaCry' guidance for home users and small businesses

24. Septembar 2017

Guidance for home users or small businesses who want to reduce the likelihood of being held to ransom by WannaCry (or other types of ransomware).

The NCSC is currently working with organisations and partners in the UK affected by the ransomware 'WannaCry'. This page contains guidance for home users or small businesses who want to reduce the likelihood of being held to ransom by WannaCry (or other types of ransomware).

- This guidance will be updated as more information becomes available.
- There is more general advice and guidance on protecting yourself online at CyberAware.

What is WannaCry?

WannaCry is a type of malicious software known as *ransomware.* Ransomware makes your data or systems unusable until the victim makes a payment.

What can I do to protect myself?

There are three main things you should do to protect yourself.

1. Update Windows

WannaCry only affects computers running Microsoft Windows operating systems that don't have the latest security patches installed. If you are using a recent version of Windows (Windows 7, Windows 8, Windows 8.1 or Windows 10) **and** have automatic updates turned on, you should already be protected automatically against WannaCry.

To update your version of Windows:

- If you are using a currently supported version (Windows 7, Windows 8, Windows 8.1 or Windows 10), run Windows Update and apply any updates.
- If you are using Windows XP, Windows Vista or older versions of Windows, download the WannaCry security update from here and install it.

Note: We **strongly recommend** that you do not continue to use unsupported operating systems, but instead upgrade to one which receives regular security updates from the vendor.

2. Run antivirus

- Make sure your antivirus product is turned on and up to date. Windows has a built in malware protection tool (Microsoft Defender) which is suitable for this purpose.
- Run a full scan to make sure your computer is currently free of all known malware.

3. Keep a safe backup of your important files

- Regularly create a backup copy of your important files (such as photos, documents, and other files that can't be replaced). If you have backups of files that you can recover, you can't be blackmailed.
- Make sure that this copy is **kept separate from your computer**. If it's on a USB stick, or a hard drive, or on any type of removable media, do **not** leave it connected (or **anywhere** on your network) or it may also be attacked by ransomware.
- You should consider using cloud services to back up your files. Many cloud service providers (for example, email providers) offer an amount of cloud storage space for free.

What to do if you have been infected with ransomware

The National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk.

If a small business has been a victim of ransomware and are worried about the infection spreading to other parts of your network, these steps may help guide your actions:

- Immediately disconnect you computer, laptop or tablet from network. Turn off your Wi-Fi.
- Safely format or replace your disk drives.
- Whilst you're still disconnected from your network, directly connect this computer to the Internet.
- Install and update the operating system and all other software.
- Install, update, and run antivirus software.
- Reconnect to your network.
- Monitor network traffic and/or run antivirus scans to identify if any infection remains.

Files encrypted by the WannaCry attack have no way of being decrypted by anyone other than the attacker. Don't waste your time or money on services that are promising to do it.

Should I pay the ransom?

The NCA encourages industry and the public **not** to pay the ransom. If you do:

- There is no guarantee that you will get access to your data.
- Your computer will still be infected unless you complete extensive clean-up activities.
- You will be paying criminal groups.

Source: The National Cyber Security Centre (https://www.ncsc.gov.uk/)