CHECKLIST

Acronis

10 Simple Tips to Protect Yourself from Ransomware

The WannaCry ransomware attack, which took down hundreds of thousands of computers in 150 countries, marked the beginning of the coming tide of ransomware attacks. In just a few steps, you can protect yourself from any ransomware attack, including WannaCry.

1

Keep current with operating system and application updates
Malware attacks like WannaCry often exploit software vulnerabilities that you can close by installing the latest operating system and application patches, updates, and security releases.

- Install the windows security **update**
- Read customer guidance from **Microsoft**®

2

Perform regular backups
Regular full-image backups are the ultimate way to mitigate ransomware attacks. You should back up critical files regularly, preferably to secure cloud storage provided by your backup vendor. However, you need to check with your vendor to make sure that their cloud backup is protected against ransomware.

3

Enable Acronis Active Protection™ in your backup
Modern backup software has inbuilt, real-time protection against ransomware. Innovative technology using behavioural heuristics analysis detects and stops ransomware even when your anti-malware program does not. **Acronis Active Protection** also automatically restores any files damaged in a ransomware attack back to its original state.

4

Install anti-virus software and keep its signature database current
Anti-malware / anti-virus software provides a valuable defense against a variety of malicious viruses. Choose your software carefully and enable automatic updates to its signature database. However, note that many new ransomware variants can evade anti-virus defenses, so be sure to back up your systems and use Acronis Active Protection.

5

Make file extensions visible
Your operating system may hide file extensions (like .pdf for Adobe® files) by default. Make file extensions visible to make it harder for malware purveyors to camouflage malicious files as legitimate ones. For example, with file extensions visible, you would easily spot a JavaScript file (with the file extension .js) trying to masquerade as a Microsoft Word document (.docx).

6

Be careful with email attachments

If you receive something from a person you don't know, or something you don't expect — don't open it! Check it with the sender and run it through your anti-virus program. You may need do the same even for emails received from people you know. Be on the safe side: don't open suspicious email attachments and don't click the links, especially the ones asking you to download software "to read this attachment." Be careful: ask the email sender for a confirmation.

7

Don't enable macros in document attachments received via email

When you receive a Word document or Excel spreadsheet by email and it asks you to "enable macros" — do not do it! Harmful malware spreads this way (e.g., **Osiris Ransomware**). If the file is infected and you allow macros to execute, you may inadvertently enable the installation of ransomware and encryption of your data.

8

Don't give your computer users more rights than you need to

If your computer user (your computer login) has Administrator privileges, it could spell disaster to all computers and devices on your network. Do not switch UAC (User Account Control) in Windows either: the extra layer of security will not hurt.

9

Use new security features in your business applications

Essential business software applications, such as Microsoft Office® 2016, now include an option to "Block macros from running in Office files from the internet". This is handy. Make sure it's enabled on your computer.

10

Prevent programs from being launched from the AppData and LocalAppData folders

Many ransomware programs (e.g., Cryptolocker) copy files to these folders and run undetected, trying to masquarade as a standard Windows® process. You can create specific rules within your Windows installation to disallow files from being executed from these folders.

DON'T BECOME PART OF THIS STATISTIC

Many victims of ransomware attacks think it will never happen to them. And, when it does, these individuals are unprepared to withstand the attack and pay thousands of dollars in ransoms. With a few simple steps and robust ransomware protection software from companies like Acronis, you can protect your valuable data in the most efficient and cost-effective way.

For additional information, please visit **www.acronis.com**

Acronis