contact a family
for families with disabled children

General Information and Tips to help understand and prevent ransomware attacks

Wanna Decryptor is a piece of malicious software that encrypts files on a user's computer or file server, blocking them from view and threatening to delete them unless a payment is made.

The virus is usually covertly installed on computers by being hidden within innocent-looking e-mails, containing links which users are tricked into opening. Once opened, the malware can install on to a system without the user's knowledge.

The virus is then able to encrypt files and block user access to them, displaying a pop-up window on-screen telling users they have been blocked and demanding payment – often via a digital currency such as Bitcoin.

Transactions through digital currencies such as Bitcoin are harder to trace as they do not involve a central banking system to process or confirm transactions, instead relying on other users to do so in a peer-to-peer system, which increases the chances of anonymity.

It is possible to remove ransomware such as Wanna Decryptor without payment by using advanced anti-malware software. The malware can also be removed manually from a computer in "safe mode", however security experts warn this runs the risk of damage to a PC, as users must go through sensitive system files in order to find and isolate files created by the Wanna Decryptor software.

Clearly, the best way to avoid the need for any form of action, is to protect yourself and make sure that you don't get attacked in the first place.

---

contact a family
for families with disabled children

Hints and tips to stay safe:

- Don’t panic!
- Don't pay any ransoms - there is no guarantee that attackers will decrypt your files - and it will encourage them or others to target you again, once you are known to be someone who pays up or who in vulnerable to attack.
- Remember that although ransomware does not traditionally aim to steal personal or sensitive data held on a computer or system, instead it focusses on blocking access to and threatening to delete files; other viruses and malware can be designed to attack or destroy your systems and PCs as well as steal information.
- Everyone is prone to unsolicited calls from “technical departments” who say they are calling to resolve your virus or system problems. Always be wary of them and ask for credentials. They often will not have any specific details, so do not supply any. *Now is the time they might be calling, preying on people’s fears*.
- Be suspicious of all unsolicited e-mails. Don't open attachments or click links in an e-mail from someone you don't know and take care even when the e-mail purports to be from someone you know, as they could have had their account hacked. This may be specifically important if you are working with one of the affected Trusts and you get a surprise email from someone in the Trust you may (or may not) know.
- When a user hovers their mouse over a link, the real link address often appears in the status bar at the bottom of the screen. If there is any doubt about the link address, do not click it.
- Ransomware works by using a program known as a Trojan to enter and take over the computer, and opening an attachment or link is what activates it. These Trojans are hidden in the emails or attachments, as can other viruses.
- Back up your important files and set up a recovery system or process so that, if the worst comes to the worst, you can reformat your computer's hard drive and start

again from scratch. Keep the back-up files separate, on an external drive, cloud storage or both.

- Change your usernames and password often. Many users use cookies with passwords and access to websites remembered by your PCs; this means they can be forgotten.
- Make sure you have effective antivirus software installed.
- Keep all of your other software up to date, with automatic updates enabled. Software developers regularly update programs to fix the vulnerabilities that ransomware and other malware exploit.
- Enable "show file extensions" in your operating system's settings. Scammers use extensions to hide malware, making it look like a video, photo or Pdf file. Files with extensions such as .exe, .vbs and .scr should be avoided at all costs.
- Disconnect infected computers from the web and local networks, to minimise the risk of other machines being affected.
- Create your own data security policy and ensure that all relevant volunteers and staff are aware of it.
- If you are using external providers for your websites or databases, ensure that their systems are secure and that they have relevant procedures in place.
- **If in doubt call an expert you know and trust.**