Lancashire Cyber Crime Bulletin

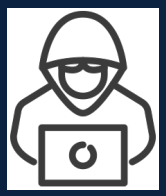
Bulletin week commencing: 20/04/20

At this unprecedented time, cyber criminals have been taking advantage of ransomware. This document can help develop knowledge to ensure you are aware of scams and crimes taking place.

The **National Police Chiefs Council (NPCC)** have highlighted ransomware as a threat during this uncertain period. NPCC emphasise that prevention of ransomware is key as business resources are stretched.

The Facts

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it).



The computer itself may become locked, or the data on it might be stolen, deleted or encrypted.

Even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files.

Normally you're asked to make a payment (often demanded in a cryptocurrency e.g. Bitcoin), in order to unlock your computer/ access data.

Prevention

Backups:

- Regular backups of your most important files.
- Turn on auto-backup if available.

321 Backups:

- 3 Backups
- 2 Backups on different storage media (e.g. two hardrives)
- 1 Backup offsite (cloud or other location)

Protecting Devices:

- Keep your operating system and applications up to date.
- Make sure your antivirus is turned on and up to date.
- Download apps from manufactured approved app stores.

Recovery from an Attack

- Contact **Action Fraud** on www.actionfraud.police.uk or call 0300123 2040.

Should I Pay the Ransom?

- The NCSC encourages you **NOT** to pay the ransom. There is no guarantee that you will get access to your files or device and the device will still be infected.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

For more guidance and information please visit:
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks