Cyber Byte

October 2024.

What is Ransomware?

Ransomware attacks are devasting for its victims. This type of cyberattack carries a type of malware when activated, by clicking a link for example, prevents you from accessing your device and the data stored on it, usually by encrypting your files. This includes employee and customer data, personal and confidential information, banking details including photographs and the memories they evoke.

Your computer may become locked and data on it might be encrypted, stolen, or deleted. The criminal group who attacked you with this malware will then demand a ransom in exchange for decryption of these files and also threaten to leak the stolen data on social or public media.

Ransomware - Should I pay the ransom?

Law enforcement does not encourage, endorse nor condone the payment of ransom demands. If you do, however, pay the ransom be aware,

- there is no guarantee that the criminals will allow you access to your data or computer.
- your computer might remain infected.
- you will be funding criminal groups.
- you are more likely to be targeted in future.

For these reasons alone, it is important that you always have a recent offline backup of your most important files and data.

Backing up your data - NCSC.GOV.UK

The following link to the NCSC (National Cyber Security Centre) will provide you with a downloadable infographic highlighting valuable points for consideration.

Ransomware: what you need to know (ncsc.gov.uk)

The Cyber Byte, sent out for your information by

Police Scotland Cybercrime Harm Prevention Team.

All information correct at time of distribution.