Ransomware Scams

Ransomware is a piece of malicious software that can encrypt and lock your online device.

Criminals can distribute Ransomware via fake emails and text messages 📧, hoping that the person receiving the message will open a web link or attachment in the message and download the malicious software to their device.

When your device is locked by Ransomware there is a ransom message displayed asking you to make a payment in order to recover access to your device, but there is no guarantee that you will regain access.

Create regular backups of your most important files (such as photographs and documents) to a secure and separate location to help keep your data safe. If you choose to backup your data to a USB memory stick or external hard drive, ensure the device is disconnected after the backup has finished to reduce the risk of malicious software spreading to your copy.

If you receive a phone call 📞 offering to clean up your computer, this is a common scam. Hang up the call immediately, do not give the caller your personal information ✋

Always be aware when receiving messages out of the blue. Do not click on web links or attachments in messages, or use any contact details contained within them. Verify using your own trusted method 👆

For further advice on Ransomware and creating backups of your data, see the National Cyber Security Centre (NCSC) UK government website.

Thank you for reading.

From your Cyber CSO

Gwent Police Cyber Crime Team