FACT SHEET

Fundamentals to Countering Fraud

Ransomware

What is Ransomware?

Ransomware is a malicious computer program that encrypts files, preventing access to them. Victims have to pay the ransomware author or group to unlock their files.

Ransomware usually spreads via malicious email attachments or downloads, and often targets businesses.

How to protect yourself from Ransomware

- **Regularly back up all files in offline storage.**
- **Make sure your system is fully updated.**
- **Never download or open untrusted documents or files.**
- **Never plug in unknown USB sticks.**
- **Create a response plan for if you fall victim to ransomware.**

Cost of Ransomware

Ransomware attacks cost UK businesses £365 million in 2020, with roughly 40% of all businesses having been targetted.

Sadly, 20% of businesses that fell victim to ransomware had to cease operation (SerbusGroup, 2021).

Types of Ransomware

There are numerous types of ransomware, but they all function in a similar way.
Examples include:

- Petya
- GandCrab
- Wannacry
- Cryptolocker
- Ryuk
- Locky

What to do if you fall victim to Ransomware

- Follow the NCSC guidance which can be found here: www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- More guidance can be found at The No More Ransom Project: www.nomoreransom.org/en/index.html
- Report the attack here: report.ncsc.gov.uk/ and alert Action Fraud.