

Lloyds Bank's School team warns education establishments to be aware of fraudsters targeting them with ransomware.

Fraudsters are finding new and devious methods to extract money from unsuspecting schools using ransomware.

Ransomware is a type of malicious software (Malware) which fraudsters apply to a victim's computer system. It usually means that a genuine user of the infected PC can't access the data stored on it, without paying the ransom demanded by the fraudster to remove the malware.

Schools are reporting that they've received a phone call prior to the attack by someone purporting to be from a 'Department of Education', saying that an email with sensitive information, such as exam details, needs to be sent for urgent action to be taken.

The caller can turn out to be a fraudster however, purely obtaining the information they need to carry out the attack and they're also preparing the school so that when the email lands a member of staff clicks on links or attachments without considering whether it's genuine. The sending email address is also likely to be a "spoof" for a department which the school normally deals with which makes this scam even more convincing

Ian Buss, UK Head of Education, Lloyds Bank SME Industry Specialists said: "There's some top tips which we think all schools should adopt to either prevent their PC's being infected in the first place, or which means that they can recover data without losing out financially."

- Install good quality Anti-Virus software on all PC's, updating it regularly and running frequent scans.
- Regularly back up all data from your PC's to a drive or device that is totally separate to your normal network.
- Always install operating system updates as soon as they become available from the provider so that you benefit from security improvements.
- Don't click on links or open attachments contained within emails unless you're sure you know who they're from. Remember a sender's email address may look genuine but it might have been spoofed by a fraudster. It's easy not to think first, particularly if you believe a genuine government department has called beforehand and told you to expect the email.
- If you are targeted in a ransomware scam, report it immediately to the Police at www.actionfraud.police.uk and also tell you Bank.

You'll find more information on many other fraudulent scams by visiting www.lloydsbank.com/fraud or www.bankofscotland.co.uk/fraud

A good watchword for any school to adopt to prevent fraudulent scams is "**Take Five**". This is the Government campaign which is aimed at getting the UK to take five minutes before they act, whether that when they receive a phone call, a letter, an email or when going online. Read more at: www.takefive-stopfraud.org.uk/

