Fraud and Cybercrime – Keep your school safe

What are the main threats?

Phishing –Emails will be sent at random, purporting to come from a genuine company operating on the internet, possibly a company you deal with, in an attempt to trick you into disclosing sensitive information. Such emails usually claim that it is necessary to "update" or "verify" your details via a link to a bogus website. The criminals will then capture any information entered for their own fraudulent purposes.

Vishing-This is a voice version of phishing and involves a fraudster telephoning and claiming to be from your bank. They may have already obtained some details from you as a result of a response to a phishing email. Details of recent payments made online may also be known by the fraudster. The aim of the call will be to obtain smartcard codes which are required for them to take funds from your account.

Trojan-This is a type of computer virus which can be remotely installed on a computer without you realising. Fraudsters will try and trick you into following a link from an email to a malicious website, where vulnerabilities in your web browser could be exploited to install the virus or other malicious software.

Spyware-Software that could be installed on your computer via a Trojan or as part of another application, to monitor activity on the infected machine and report back to the fraudster. This could take the form of a keystroke logger, which is designed to read keystrokes entered on your computer keyboard and capture passwords and other security information. Spyware is often installed remotely, but physical devices could also be directly installed on your computer.

Bogus Boss Fraud-A criminal hacks into a Head Teacher's email address. An email is then sent to the secretary/school business manager advising that an urgent payment is made. The criminal is hoping that as you have been told it is urgent and it has come from the Head Teacher's email address, that the invoice will be paid without question.

Mandate Fraud-An email will be sent, appearing to be from a supplier, advising that their bank details have changed and all further invoices are to be paid to the new bank account. When payment is made, the funds will go to the fraudster, rather than the genuine supplier. Not only will the school have lost the funds paid to the fraudster, the supplier will still need to be paid.

Fraud or scam?

If you have been a victim of fraud, there has been no involvement by the victim, a card has been cloned etc and the transactions are not authorised, which means that costs can be recovered. If you have been a victim of a scam, you have been tricked into making a payment, which is an authorised transaction and the money may never be recovered.

Following a recent Fraud and Cybercrime seminar in Birmingham, run by Nat West Bank and West Midlands Police, the websites below give advice on keeping your school safe.

Get Safe Online: www.getsafeonline.org

Action Fraud: www.actionfraud.police.uk

Remember

Do not click on links in emails, go the actual website and enter your login details from there

Make sure your operating systems are up to date

Back up your data regularly, preferably to the cloud

Create strong passwords-three random words that you will remember, with a number and a symbol.

Have a strong resilience plan in place, in the event you become a victim of fraud or scam. Know what needs to be done, who you need to contact and have a predefined set of actions.