Spot a Scam and Report the Scammer

Protect yourself and Report Scammers

Scams are a common way that cybercriminals compromise accounts

Being alert to scam messages is a great way to protect yourself online. These 'scammers' may try to compromise your business, workplace or university accounts. Scammers often use email, text messages, phone calls and social media. Their goal is to scam people into paying money or giving away their personal information. They will often pretend to be a person or organisation you trust.

DON’T FALL FOR THE SCAM IN TWO STEPS

First, check if it is a scam

Know what to look for. View common types of scams such as dating scams, investment scams, phishing emails and text, or invoice fraud.

Go direct to a source you can trust. Visit the official website, log in to your account, or call their phone number. Don't use the links or contact details in the message or given to you on the phone.

Check what the official source says about what details they might request from you. Often companies or government agencies will say what they will and will not ask you online or over the phone. For example, the bank may tell you that they will never ask for your password. If someone claiming to be from the bank then asks you for your password, you know it is likely a scam.

Then, if you still think it’s a scam

Don’t click on links, open any attachments or reply to requests. Scam messages may try and trick you into giving out your personal information. A scammer might ask for your bank account details, passwords or credit card numbers. They may also ask you to download files, software, or allow remote access to your computer.

Contact your bank. Contact your financial institution if you think your credit cards or bank account may be at risk. They may be able to close your account or stop a transaction.

Report a cybercrime to the Cyber Crime Unit located at 6 mile, if you have fallen victim to a scam.