Online Scams

An email in **broken or poor English** tells you a deposed or decesased leader has left millions and you can obtain a bonus payment if you help to process the funds in the frozen account through your own account. However, the draft is forged or fake and the fee you paid is lost.

You receive an email telling you that you have **won big in the lottery** of another country and that you just need to send a processors fee to an account or via western Union to receive your prize. If you didn't buy a ticket, then you didn't win so don't get caught.

A retailer calls telling you your card is **being fraudulently used** and can you confirm your account details to stop the fraud. The caller pretends to hang up but your next call to your bank is still with the fraudster and you are asked for your PIN and security codes.

A caller tells you your **computer has problems** and asks for access to help you fix it. These 'problems' are normal issues every computer and any fee will be wasted. Microsoft do not cold call customers.

This attack comes from **opening an infected email** or an infected website which enables malware to be downloaded to your computer and its contents to be encrypted. A fee, usually in bitcoins, is demanded to decrypt the contents of the computer. Help is available on websites which offer advice or tools to free the content but anti-virus and malware protection should be updated regularly.

These are emails from your **bank or a service provider** telling you that your account is locked. You are asked to follow a link and provide your bank account details and PIN to get access again. However, the link is to a fake website where bank/account details are scrapped and sold on or used fraudulently. Banks never ask for personal information online.

You receive an **urgent email message** from a relative or friend saying they have been mugged on holidays and need urgent help with funds for travel and getting home. You are asked to transfer funds over a money transfer service. However the fraudster uses fake ID to collect the money. Always check with friends that they are on holidays. Call them even if the suggestion is their phone has been stolen.

Where an **advert is cloned** on a website with details of a pervious advert. Any purchase of the goods is fraudulent and any funds are lost. Users should check that the same goods haven't been sold and always use secure payment services such as PayPal. If unsure about an advert or it looks too good to be true it probably is.

Fake buyers offer to purchase goods and say they have lodged funds as the winning offer. They then try to complete the sale and you receive a 'confirmation' email from 'PayPal' stating the funds have been paid. You are asked to confirm you have sent the product but you soon realise the email is forged. PayPal never confirm payments by email.

You receive an email from the **company CEO** instructing the payment of money for a 'secret' deal using new account details for a supplier or customer. He/She wants an immediate confirmation that the funds have been transferred. These frauds rely on the 'fear factor' of not doing something the CEO wants. Always check email addresses for subtle differences such as Michael@domaine.com instead of Micheal@domaine.com and have an authentication process in place for changes in payment processes.

You are the **losing bidder** on an auction and receive an email from the 'seller' offering a second chance to purchase the same product. You complete the purchase using a payment processing service but the seller is false. Only purchase from legitimate adverts and don't respond to communications which are off site or are unsolicited by you first.

REPORT ALL CRIMES TO YOUR LOCAL GARDA STATION