The Oasis Centre - Cornwall

Registered Charity Number 1139355, founded to serve the communities in the parishes of St Columb Major, St Mawgan-in-Pydar, St Eval and St Ervan

Looking Out for …… Dodgy E-mails

Number 03 in a series of notes on important issues.

This is all about dodgy e-mails. Over the last decade, letter writing has become a quaint, outdated practice for many people. Instead, we send e-mails from our laptops and mobile phones. They are quick. No need to find pen and paper, no need for a stamp or to find a post box and they go instantly with the click of a button. No wonder they are so popular and no wonder criminals have found plenty of uses for them too.

Dodgy e-mails come in all shapes and forms and new and more sophisticated ones are being invented every day. There are however some features that are fairly common. First, they all claim some form of 'authority' by pretending to be the police, the local council, HM Revenue and Customs, a bank, a government department, a well-known trader or perhaps a courier firm with vans up and down the country making deliveries. They may even impersonate a social media site like Facebook or Twitter and the very clever ones may even address you by name or pretend to be from a friend or relative.

Secondly, the dodgy email will contain something to capture your interest. It may claim to disclose the name of the lottery winner (or paedophile) who has just moved in to your street. It may say that your order has been cancelled, there is a delivery on its way to you, an unopened message is waiting for you, you have won a prize, you are entitled to an unexpected inheritance, you are due a tax rebate or even a refund on your last holiday. They are inventive people these criminals and they will flavour the bait they are offering you with a sense of urgency requiring immediate action – otherwise you will lose out. They do not want you to stop and think.

The third feature of these dodgy e-mails is the attachment to be opened or the box or Internet link that you are invited to click on for 'more information', to claim the prize, read the 'message' or even to cancel the 'order'. No matter how tempting it is, don't do it! If you do, the consequences will not be nice and could cost you a lot.

In short, there are a number of malicious infections that could, almost instantly, be inserted into your equipment. One of these might enable the criminals to gain instant access to and copy all your personal information. This could be used to impersonate you for identity fraud and of course be sold on to other criminals. Alternatively, the entire contents of your equipment may be encrypted and you will be invited to pay a ransom (quickly or it will increase) to have it unlocked. To add to your woes everyone on your address list could receive an e-mail purporting to be from you inviting them to click on a similar link!

The most important step, if you receive such an e-mail, is to check the real address from which the e-mail has been sent. It will appear if you hover your cursor over the sender's name and will confirm your suspicions. A minor or insignificant variation from the address of the organisation being impersonated is all that the criminal needs to create his or her hoax address or website.

Jeremy Simmonds, Chair, The Oasis Centre - Cornwall