Phishing, Fraud and Scams
Recently we had an enquiry from a user relating to an email they had received purporting to be from HMRC about a tax refund. They were worried that it might be a scam (it was) and also wondered how the fraudster had got their email address. This made us think that this might be a good time to warn our customers about some of the many fraudsters out there on the internet and some of the methods they use.

The main aims of these frauds are

- to get you to send money to someone
- to get personal details off you which they can use to access your bank accounts and steal from you
- to get access to your computer to install malicious applications on it which they can use to steal your personal data or take over your computer to use in internet attacks

Some of the ones you may have come across are

- an email supposedly from a friend or relative stranded abroad asking you to send them money immediately
- emails from people abroad asking you to help them move money out of their country in return for a percentage but you need to send them a small sum first to enable them to set up the transfer
- you are told you have won a prize in a competition but need to send a fee to cover the administration
- an email from your bank or building society asking you to update your details because of a security breach – complete with a link to 'their' website. The website in question is fake
- the phone call from 'Microsoft' telling you there is a fault on your computer and asking you to let them log on to fix it for you
- not strictly illegal but ethically dubious are the look alike web sites usually for government services which charge a fee for doing things like filling in forms and submitting applications which you could easily do yourself for free

The list is almost endless but one which has surfaced recently is particularly insidious. You get an email from a supplier or service provider (maybe a tradesman who has just done some work for you) to whom you genuinely owe money, telling you he has changed his bank and asking you to pay it into a different account from the one on the invoice. The new bank account belongs to a fraudster who has hacked the tradesman's computer.

The moral is always be cautious around emails asking for money

How do the fraudsters get the information and email addresses?

- By guesswork; they use computer programs to generate lists of possible user names and email address combinations – some of them are bound to work
- from publicly available information; there is a lot of information floating about the web. It's relatively easy to build up a profile about someone from social media, the electoral register and suchlike and then target them posing as being referred by a friend or colleague
- hacking; getting access to someone's computer and getting all their email contacts

How to protect yourself

- Think before responding to unsolicited emails. Banks, Building Societies, HMRC and other official bodies all have websites and phone numbers you can use; check by phone if you're not sure and never send personal details in a reply to an email without checking first
- Don't follow links in unsolicited emails. If you think a site might be of interest enter it into your browser yourself. A link to Amzon.co.uk can easily be misread as Amazon if you're not looking closely
- If an email from a friend looks a bit odd – it probably is. Check with them by phone before opening any document you weren't expecting or following any links in it.

Finally
If you're worried about internet fraud or just want to know more there are lots of websites with more information. Try these for starters

https://www.getsafeonline.org/
http://www.bbc.co.uk/guides/zxq8frd

We are planning a session on security and Internet fraud at the Club on Friday Sept 30th. Please come if you want to know more, it is held every Friday at our Melling office from 1-5 pm, there will be tea, and if you have some please bring cake.

Noun ˈfiSHiNG **phishing** the activity of defrauding an online account holder of financial information by posing as a legitimate company.: "phishing exercises in which criminals create replicas of commercial Web sites".