Fraud: A problem that is getting worse

A recent report from the government gave the startling fact that 53% of ALL crime reported was fraud or cybercrime; and that's just reported crimes. How many of us would report being tricked out of money either because we are embarrassed, or because we believe the authorities will do nothing about it? However, it is important to report the crime as there are some clever and powerful agencies within the Police and government that are constantly battling against this crime and they need us to report so that others can be protected.

It is very difficult today to pay bills, order goods, buy tickets and so on without having to go online. But we can do some simple things to protect us.

Anti-virus: Ensure your PC/tablet/smartphone has an anti-virus software. There are a number of good free packages available.

Passwords: add numbers and special characters~~,~~and use a mix of upper- and lower-case letters. Any word used as the core of the password must be relevant only to you. Another idea is to think of a phrase and use the first letter/number of each word. You would say the phrase to yourself as you type the password.

Credit card numbers shouldn't be saved on every supplier's website willy-nilly. It's hardly a chore to type in the number every time. And you can reduce the number of suppliers who have your personal details by paying with PayPal or another payment provider. You need to trust someone, so why not just have one payment company?

Phishing (pronounced fishing) is a way of obtaining your details through fake emails. Check the address the attractive email has come from. If the address doesn't look quite right, then it may be a fake. Almost all government business is transacted through the *www.gov.uk* portal. There is no government department called *www.passportoffice.uk*, for example. Never open any attachment from a suspicious email, nor click on any link. Hover your mouse over the link in the email and the underlying address should pop up. Fake links should be obvious. If in doubt, check the domain name in a search engine (i.e. *www.passportoffice.uk* in the above example). Never divulge your personal details via an email. You can do that once logged in to the supplier's account using a username and secure password.

Secure webpages have a web address (called a URL) starting *https://* - note the "*s*". The full address will have a padlock symbol to its left at the top of the web page. These are secure websites. Never reveal any personal details on webpages that lack these.

Public Wi-Fi can be very useful to use while you are in town having a coffee, but never do any financial business using public Wi-Fi. Just look at how many people around you are working on a laptop or phone. Do you trust them not to eavesdrop electronically on you?

Be sensible, and be safe.