Fraud: as much of a problem in the online world

Many of us do our business on a computer or phone. Indeed, it is very difficult today to pay bills, order goods, buy tickets, and so on without having to go online. But there are risks associated with this, and a few easy actions can make things safer for you.

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.

Internet banking is very safe as there are lots of proven security layers. But a good tip is to always log off when you are finished and not to use the browser's "back" button at any time – click the menu item to go back instead.

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 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. Is the email addressed "Dear customer"? Why don't they know your name? They should do, so be suspicious. 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 will be very obvious. If in doubt, check the domain name in a search engine – for instance, *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*" and 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 be electronically eavesdropping on you?

Are you going away? I've mentioned this before, but if you go on holiday please do not post photos of yourself on the beach or a cruise ship on social media. The burglars now know you are away from home. Bought a huge new expensive TV? Please don't brag about it on social media. Think about who you are telling.

Be sensible, and be safe.