Thornbury & District Stroke Support Group

Scams, Passwords and Protecting your Personal Details

In the age we now live in, companies we need to deal with, increasingly require us to do our business via the internet and over the telephone and fraudsters are quick to exploit any weaknesses. We hear about a lot of people having money taken from them but there are things you can do to guard against such frauds (or scams).

Telephone Scams

- A caller says there is a problem with your computer and if you give them permission, they can fix it for you. If you agree, they will steal your information and may freeze your computer until you pay them a ransom.
- You get a phone call or email telling you they need to update your account details otherwise your phone, internet, electricity or similar will be cut off. *Service providers don't do things this way, they want your business - ignore it.*
- Someone calls and says they are the police, or from your credit card company and tell you that your credit card has been used fraudulently and they need to know details to confirm it is yours. They may even say they will send a courier to pick up the card so that they can deal with it for you!
- A caller tells you are eligible for a prize or refund from a supplier and they ask for your bank details or ask you for an admin fee for a prize that will never arrive.
- You get a call from someone, saying they mistakenly paid some money into your bank account. They ask you for your account details to transfer it back to them and then you find they have cleared your bank account. *(even if they appear to have put some money into your bank account, don't be fooled and contact the bank).*

There are many variations on these types of scam, and some are very clever and convincing. For example, some will give you a telephone number to call back on so that you can "confirm the call is genuine".

In all of the above, just put the phone down or delete the email and if they have pretended to be from a company or official organisation and you are concerned, contact them on a telephone number you know is genuine *(for example the number on the back of your credit card or from a paper bill, etc.).*

Using a call blocker on your phone may reduce nuisance calls but the scammers have ways of getting around them, so don't feel too safe on the phone.

Internet Scams

Most of the telephone scam examples can also be carried out via the internet and it is very easy for the scammers to forge a company's web site so that it looks genuine. If you get an email you are not sure about with a link to something else, delete it immediately as it may not only lead you to a dodgy site, but it may also plant a virus on your computer. Look for clues on web sites and emails such as poor grammar and spelling.

If for example, you want to renew your passport, driving licence or other official document on the internet, make sure you log onto the official web site. It is better to type in the address given on an official document rather than Googling 'renew passport' for example. Many websites sites look just like an official one and although they may legally act as an agent and renew your passport for you, there will be an additional fee for doing so. There is also the risk that they may use the information you have given them for other purposes.

Passwords

Passwords are important to keep your data safe. It is relatively easy for a fraudster to guess a password if you do not use a strong one. Millions of people in the UK alone use '12345' and 'password' for example.

Do

- Have a strong password of at least 8 characters.
- Use a mixture of upper and lower case.
- Use numbers in place of letters such as 5 instead of s (*but not every time an s is used*).
- Use special characters such as @, £, #.
- Change your passwords regularly.
- Consider using a phrase that is nonsense such as 8Ha%79bD.

- Avoid password using:
    - Current partner's name
    - Child's name
    - Other family members' name
    - Pet's name
    - Place of birth
    - Favourite holiday
    - Something related to your favourite sports team

Do Not

- Use the same password for everything.
- Let an internet browser save the password for you.
- Give anyone your password *(an exception is if someone gives you a separate telephone password).*
- Leave your password in sight of anyone and destroy any copies securely.

Contrary to some advice, it is better to keep passwords that are not easy to remember in a little black book rather than having simple ones we can remember - **providing you keep it under lock & key!** (*Software is available to manage passwords, but it is outside the scope of this article to recommend what to use).*

Personal Data Protection

Many scammers are opportunists that take a chance on us being vulnerable or that we may be a customer of one of the big companies. Others, however, collect information by stealing information or by 'Hacking' into an organisation's records and then use it to defraud us.

To reduce the risk of your personal information falling into the wrong hands:

- If you no longer deal with a company, ask for your details to be removed from their records.
- If you are concerned about what details someone holds – ask them *(it is your right).*
- Always destroy paper documents securely by shredding or burning.
- Password protect your computer and further password-protect sensitive information stored on it.
- Don't put personal details on phones or tablets that are at a greater risk of being lost or stolen.
- If you replace a computer or hard drive, make sure it is cleared of all data.
- Be careful who you give information to.
- Keep your computer and anti-virus software up to date.

Despite all this, the internet is convenient for keeping in touch, banking and shopping. It is also a great source of information, education, and entertainment and we should not be afraid to make use of it.

So please don't be put off but follow this advice and do take care.