10. How can I protect my privacy on social networks?

Social networks (e.g. Facebook and Twitter) are a great way to keep in touch with family and friends, make new friends, look at photos, find out about local events and much more.

However, on any social networking site, you must guard against people who want to steal your personal information. Use the privacy features on the site to choose who can see your profile and your posts, and avoid publishing information that identifies you, such as your telephone number, address or date of birth.

Take Five: five key things to remember

- ✓ Never disclose security details, such as your PIN or full password - it's never okay to reveal these details
- ✓ Don't assume an email request or caller is genuine - people aren't always who they say they are
- ✓ Don't be rushed – a genuine bank or organisation won't mind waiting to give you time to stop and think
- ✓ Listen to your instincts – if something feels wrong then it is usually right to pause and question it
- ✓ Stay in control – have the confidence to refuse unusual requests for information

Some useful websites for further information

https://www.getsafeonline.org

http://www.ageuk.org.uk/work-and-learning/technology-and-internet/internet-security/

http://www.connectsafely.org/seniors/

Produced by H. Towle October 2017

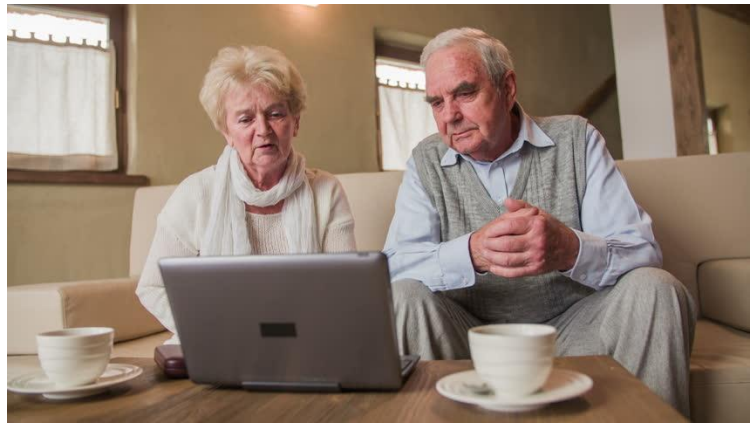
U3A

THE UNIVERSITY OF THE THIRD AGE

NEWCASTLE EMLYN

Stay Safe Online

Tips for staying safe when browsing and using the internet



More and more people are using computers, smartphones and tablets to get online. It's a great way to look up information, do your shopping, stay connected with loved ones, and even make new friends.

The internet has lots of positive aspects, but there are things you need to look out for.

1. Choose, use and protect your **passwords** carefully, and use a different one for every online account in case one or more get hacked.
   A strong password should:
   - be at least 8 characters long
   - include a combination of upper and lower case letters
   - include some numbers and keyboard symbols such as & or !
   - not include personal information, such as your name, date of birth or any family member's details
   - not include common words like 'password'

   If passwords with numbers and symbols are too hard to remember, using three random words together can make a stronger password, as long as those words don't contain your personal information.

2. Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode.

3. Ensure you always have **internet security software** loaded on computers and a similar app on your mobile devices, and that this is kept updated and switched on. Remember that smartphones and tablets can get compromised as much as computers.

4. You mustn't assume that **Wi-Fi hotspots** in places like cafes, bars and hotel rooms are secure, so never use them when you're doing anything confidential online. Instead, use 3G or 4G.

5. Never reveal **too much personal or financial information** in emails, on social networking and dating sites and in person. You never know who might see it, or use it.

6. Always consider that online or on the phone, **people aren't always who they claim to be**. Fake emails and phone calls are a favourite way for fraudsters to approach their victims. Take your time and **think twice**, because everything may not be as it seems. Remember that if something seems too good to be true, it probably is.

7. **Don't click on links in emails**, posts, tweets of texts – and **don't open attachments** if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving them.

8. **Stay safe when shopping and banking online?**
   Shopping online can be quick and convenient, but you need to protect your financial information. Make sure that you're using a secure website before entering any personal details.
   There are ways to spot that a website is secure, including:
   - the website address starts with 'https' - the 's' stands for secure
   - the address bar is green, which is an additional sign that you're using a safe website
   - a padlock symbol in the browser where the website address is (but don't be fooled if the padlock appears on the page itself)
   - a current security certificate which is registered to the correct address (this appears when you click on the padlock)

   Be aware that a padlock symbol is not an absolute guarantee of safety. If you ever have doubts it's best to leave the page.
   To help protect you while shopping or banking online, follow these simple tips:
   - Beware of pop-up messages that warn you about a website's security certificate. They may direct you to a fake website that's designed to get you to hand over your security details
   - Use online retailers with a good reputation, as either high-street shops or established online stores
   - Look for the company's full contact details. A reputable company will always display this information on its website
   - Cross-check information on the internet to see if anyone has experienced problems with the retailer
   - Find out where the seller is based because consumer rights vary from country to country. To find out more information about buying from sellers based in other EU countries, you can visit the UK European Consumer Centre Website
   - Use the same credit card for internet transactions only. If anything goes wrong, you can always cancel this card
   - If a deal looks too good to be true, it probably is, and be cautious of anything offered in an unsolicited email

9. Giving a caller remote access to your devices could compromise or even disable them. **Only an authorised support person** who you have contacted with a problem, should be allowed to gain access.