CARERS GUIDE

ONLINE SAFETY

FOR OLDER PEOPLE

Training pack aimed at scam spotting, reducing the risk of fraud and keeping older people safe.

AWARE | SECURE | RESILIENT

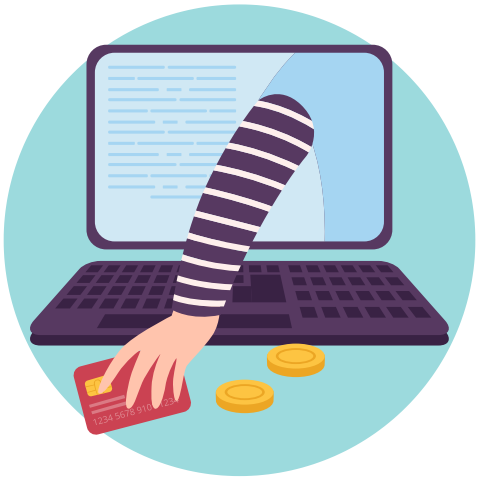
Office of Cyber-Security & Information Assurance

Online Safety For Older People

Going online has made it easier than ever to keep in touch with family and friends. Online banking and shopping has been invaluable recently when it's not always easy to get out.

However, it's also the perfect place for people to take advantage of the anonymity that a computer screen offers. Most know that young teenagers are the ideal target for predators, but few think about online safety for older people.

As a carer for an older person, you can help them navigate their way around and stay safe.



Online scams are becoming increasingly sophisticated and many people are caught out – even those who are regular internet users.

Every year in the UK, millions of people lose money to scammers or unknowingly share their personal information.

OCSIA have produced a short video about internet safety aimed at older people.

Please share this video to help older people stay safe online.

SCAN ME

Here are some tips to help your older relative or client protect their money and information while they are shopping or banking online:

Shop Safely

- Use online retailers with a good reputation, such as well-known supermarkets, high street shops, or established online stores.
- Beware of pop up messages that warn about a website's security certificate. They may direct to a fake website that's designed to get you to hand over your security details.
- If a deal looks too good to be true, it probably is, and be cautious of anything offered in an unsolicited email.
- For additional protection, use a credit card for online transactions rather than a debit card. If the purchase costs more than £100 and a credit card is used, the seller and the card company are equally responsible if anything goes wrong.
- Use the same card for internet transactions only and check the bank statement for this card regularly for any unusual transactions. Contact your bank immediately if there's a problem.

Bank Safely

Using online banking means your relative or client can keep control of their finances from home or whilst they're out and about, using their bank's website or smartphone app. But here are some things to remember:

- Make sure only the official Bank app or website is used.
- Callers or visitors should never be allowed to access their relative/clients online banking.
- Login details should never be left on display or shared.

Safety on Social Media

Phishing: This could be where you receive an email from your bank or other financial institution claiming that you need to reset your password, or directing you to click on another link. If you click the link you are taken to a fake page. Once you enter your password, the criminal has your data.

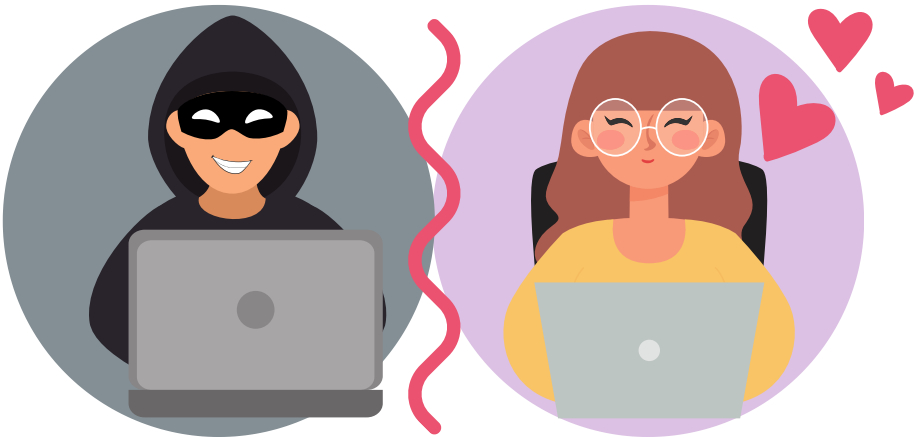
These days, banks never send such emails so make sure your older relative never replies or clicks links within the email. Ask them to show you if they are unsure about an email, and make sure they know to only open attachments from people they trust because these can contain viruses.

Romance Fraud

Scammers can use social networks like Facebook, or dating websites to gain trust. They'll then start asking for money – often by sharing an emotional story or asking for help in an emergency situation.

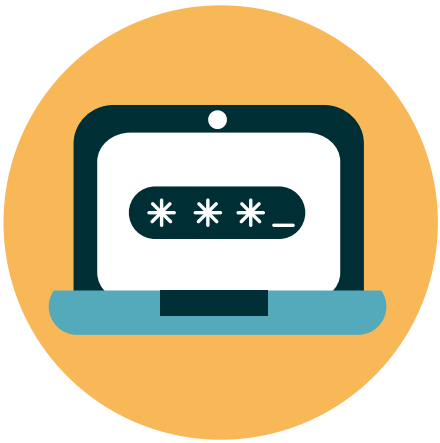
If your elderly relative or client uses social media, make sure they know the dangers.

They should not share too much personal information like date of birth, location, address, photos of home, etc. They should also change the privacy settings so that only people they know can see their profile, and you might want to help them do this.



Protecting Passwords

Keeping passwords secure is one of the most important things in keeping safe online. You can help older people to keep their personal information safe.



They should try to use a different password for each online account, particularly for accounts storing their private and sensitive information.

They should never tell anyone else their login information – remind them that if they forget their passwords they can easily reset them. They shouldn't leave their login details on display and they should always log out.

To create strong passwords they can use three random but memorable words for each password. Passwords can be made stronger by using a mix of upper and lower case letters, numbers and special characters.

Suspicious Emails

Remind your relative or client not to open emails from unknown sources, download attachments or click on links unless they are sure that they are genuine.

If a deal looks too good to be true, it probably is, and be cautious of anything offered in an unsolicited email.

Reporting

SERS Reporting Page

If you or an older person you know receives an email you think could be suspicious, you can report it to the Suspicious Email Reporting Service (SERS) by emailing SERS@ocsia.im. By sending your suspicious emails to them they can better understand the threats on our Island and provide relevant advice and warnings.

Office of Cyber-Security & Information Assurance
Oik son Shickyrys Lectraneagh as Sauchys Fysseree

OCSIA

The Office of Cyber-Security and Information Assurance (OCSIA) offers tips and advice on how to stay safe online. Visit www.gov.im/ocsia.

IOM Police Constabulary

Visit www.iompolice.im for more information on Cyber-Security and how to report scams and fraud.

Victim Support Isle of Man
Helping people cope with crime

Victim Support

Victim Support is available to anyone who has been affected by crime. If you or an older person you know has been affected by crime, you can contact:01624 679950

OCSIA have produced a short video about internet safety aimed at older people.

Please share this video to help older people stay safe online.

SCAN ME