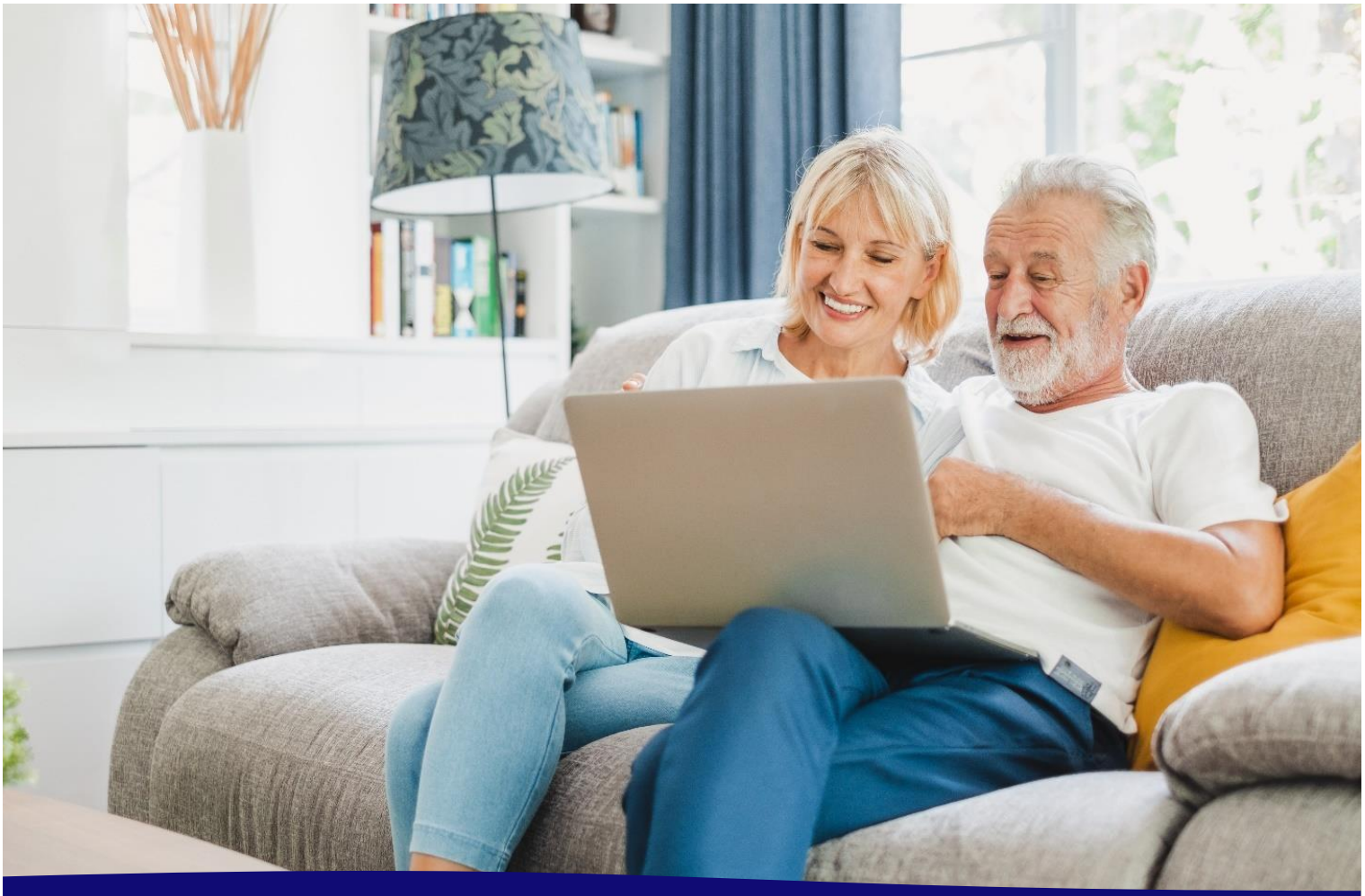

THE CHURCH OF ENGLAND
PENSIONS BOARD

How to stay safe online

January 2023

Getting online can make life easier in many ways, but there is also a risk of scams and fraud. Online scams are becoming increasingly common, but you can protect yourself by knowing what to look out for, an what to do if you suspect a scam.

This leaflet explains tips and help to keep people safe online, with help from Age UK.

What are online scams?

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.

But there are ways to avoid being taken in by scams if you know what to look for.

Here are some common online scams.

Contact us

pensions@churchofengland.org

020 7898 1802

PO Box 2026, Pershore, WR10 9BW

Email scams

Scammers send emails hoping people will enter their personal or financial details.

Some emails may also have a link or a file attached for you to click on or open. Opening these links or downloading the files may harm your device. Scam emails can appear to be from official places, like HMRC or your bank, but look out for:

- Check the time it was sent, scam emails usually come from countries in a different time zone.
- Scammers often send emails to hundreds of people at once. They'll hide the email addresses they send it to. If the 'To' field is blank, it could be a scam.
- Scammers often don't know your name, so look out for a generic greeting like 'Hello' or 'Dear Ladies and Gentlemen'
- Errors in the spelling or grammar, or an unusual style of writing.
- Requests for personal information, such as your username, full password, or bank details – genuine organisations will never ask this.
- Threats that unless you act, a deal will expire, or your account will close.

Fake websites

Scammers create fake websites which look official, requesting you to provide personal or financial information. For example, a fake bank website may be set up asking you to update your account or security information. Often, they will look very similar and only a few details may be different.

Relationship scams

Scammers can use social networks like Facebook or dating sites. Once they've gained your trust they'll start asking for money, often by telling you an emotional or hard luck story. These tricks are hard to spot, so it's always worth talking to a friend or relative about it, especially if things seem to be moving fast.

Health scams

False and misleading claims may be made about medical related products, such as miracle health cures, and fake online pharmacies may offer medicines cheaply. However, the actual medicine delivered to you can turn out to be poor quality and even harmful.

Top tips

Email

Often the email address it comes from looks legitimate. Click on the reply button, and see who the email is really from.

Hover over any links in the email. Be careful not to click on it. The real link will appear. If it doesn't look genuine, or it's not a link to your own account, don't click on it.

If you are worried, delete the email straight away. If the email claims to be from an organisation, phone them directly using the phone number on their website and ask.

Fake websites

Find the official web address from a letter, or on Google. If you aren't sure about which website to use for a Government service, go through GOV.UK, the Government's official website, to find what you need.

Relationship scams

Never send the person money or give them your account details.

Health scams

Check if it's legitimate by clicking on the 'Registered Pharmacy' logo on the websites home page. This should lead to the General Pharmaceutical Council website.

How to shop safely online

- Use online retailers with a good reputation, or well-known shops or established online stores.
- Look for the company's full contact details. A reputable company will always display this.
- Search for the name of the company on the internet to see if anyone has experience problems with the retailer.
- If a deal looks too good to be true, it probably is.
- Check your bank statement regularly and contact your bank immediately if there are any unusual transactions.
- Use a credit card rather than a debit card as it has additional protection. If your purchase costs more than £100 and you use a credit card, the seller and your card company are equally responsible if anything goes wrong.

How can I protect my computer, tablet and smartphone?

It's second nature to keep your valuables stored safely in your home and out of sight of burglars. But it is equally important to keep your personal information safe from criminals when you're online. As well as being alert to scams, there are simple steps you can take to protect your device.

Keep your passwords strong. Setting strong passwords is one of the simplest, most effective things you can do to stay safe online. Avoid passwords made up of common words or numbers or keyboard patterns (such as password, or 123456), and don't include personal information like your name, date of birth or any family details. Use different passwords for different accounts.

Install security software on your computer. Anti-virus software will look for and remove viruses before they can infect your computer. Anti-spyware software prevents unwanted adverts from popping up and stops programs tracking your activities or scanning your computer for private data. You can buy a package from a reputable provider such as McAfee or Norton either online or from a computer shop.

Protect your tablet and your mobile phone. You can check emails, shop and bank online on tablets and smartphones, so they need protecting too. Start by password-protecting any device. You can download anti-virus and anti-spyware protection for tablets and phones and lots of the apps are free.

Protect your wireless network. You can protect your wireless network (also known as Wi-Fi) so that people living nearby can't access it. Read the instructions that come with your router to find out how to set up a key (a type of password) so no one else can access it.

Keep your device updated. Every device has an operating system, which is the software it needs to run. Your device can be better protected if you keep it updated. You should receive notifications when a new update is ready, but you can also update it manually yourself.

Scammers are always looking for new and sophisticated ways to trick people. If you think you've been a victim of a scam, contact the police, then Action Fraud on 0300 123 2040. The information you give can help track down the scammer. Don't suffer in silence.