

SCAMS AWARENESS UPDATE



Older Persons Scams Awareness & Aftercare Project

In this update:

Top tools to avoid fraud
Pages 2 & 3

Current frauds
Page 4

My money, my info - no thank you!

Top tools for keeping your money and information safe

The best way to prevent criminals from getting their hands on our hard-earned cash or personal details, is to build habits to protect ourselves in the first place.

You may want to spend that hard-earned money on yourself, friends, family or make investments for the future. Whatever the reason, it's your money and your information to keep, not for fraudsters to take.

We can't remember every scam out there, but we can make a few simple checks before handing over our money or details to buy goods and services.

So, this month, we are exploring a few simple tools to help us get into good habits when deciding what to do with our money.

We believe the best way to protect yourself from fraud is to have a personalised scams advice session. That way, we can talk about what's important to **you**. To book a free appointment, contact our Scams Awareness & Aftercare Team on 01625 612958 or enquiries@ageukce.org

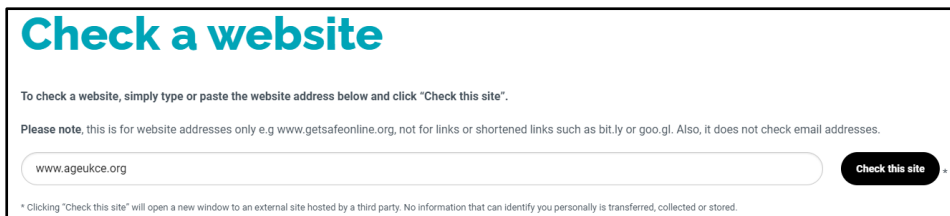
TOP TOOLS TO FIGHT FRAUD

1

Get Safe Online website checker - [Check a website](#) is an easy-to-use online tool which helps you to see whether a website is likely to be legitimate or a scam ... before you visit it. Simply type in the address of the website you want to check, and your results will appear within seconds.

It searches more than 40 data sources as well as thousands of reports of malicious websites

from law enforcement agencies, regulators and consumer brands every week to give a trust score.



Check a website

To check a website, simply type or paste the website address below and click "Check this site".

Please note, this is for website addresses only e.g www.getsafeonline.org, not for links or shortened links such as bit.ly or goo.gl. Also, it does not check email addresses.

www.ageukce.org

* Clicking "Check this site" will open a new window to an external site hosted by a third party. No information that can identify you personally is transferred, collected or stored.

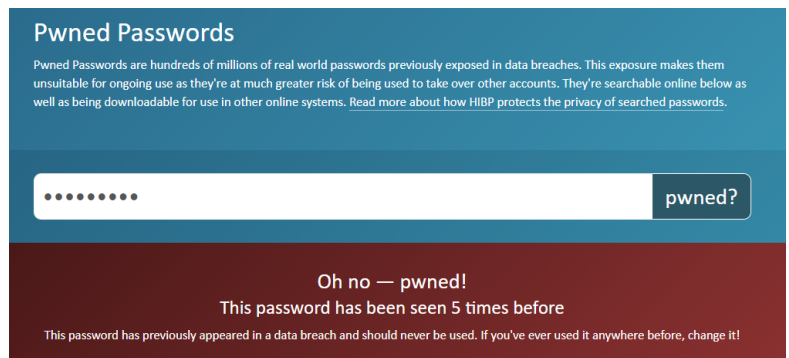
This would be useful if

you're sent a link to a website in a text or email. You can check it out without clicking on the link. With more than 159,000 fraudulent website addresses being taken down over the last 2 years by the suspicious email reporting service, it's worth a quick check for peace of mind.

2

Have I been pwned? website - This website shows you if your [password](#), [email address](#) or [mobile phone](#) number has been in a data breach.

If it has, it warns you to change your password immediately, so criminals cannot get into your email or online accounts.



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

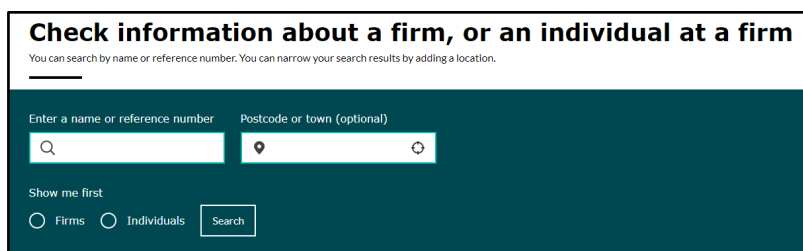
.....

Oh no — pwned!
This password has been seen 5 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

3

Financial Conduct Authority (FCA) register and warning list - We've mentioned this before. It's really important that you checkout ANY individual or company before making an investment.



Check information about a firm, or an individual at a firm

You can search by name or reference number. You can narrow your search results by adding a location.

Enter a name or reference number Postcode or town (optional)

Show me first
 Firms Individuals

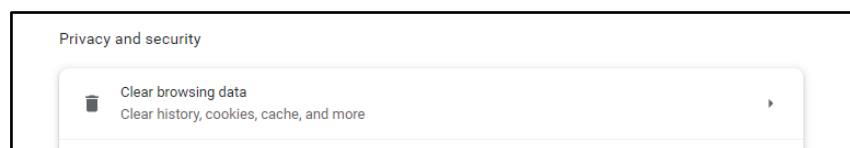
The [register](#) tells you if an individual or company are registered to give financial advice, the type of advice they can give and any warnings against them. The [warning list](#) shows investments that the Financial

Conduct Authority believes are scams. You can also call to check on 0800 111 6768.

As over £171 million was lost by individuals to investment fraud in 2021, it's worth a check.

4

Clear your browsing history - When we search for things on the internet, from investments to walking sticks, it remembers what we've searched for, so it can show us similar things later on.



This means you may see adverts for the item or service you've just been looking for. However, some of those adverts or search results may be fraudulent. The best thing to do is clear your browsing history regularly, so less adverts appear.

You can do this on the internet by clicking on the 3 dots at the top right of the screen, selecting "settings", then "privacy & security" on left hand side, then "clear browsing history" in the centre.

5

Say no to public WiFi - Lots of places offer free WiFi - from coffee shops and sports clubs to charities and community centres.

Often there's no need for a password, or the password is the same for everyone. Criminals can use this free WiFi to access what people are looking at online and steal user names and passwords to accounts.



So, only use this facility to browse the internet. Never use it to access any of your accounts, such as emails, online shopping or banking. If you want to use any of your accounts that have a password, use the data from your phone provider (4G or 5G) instead.

6



Call 159 to check if your bank really called you - If you receive a call or message from somebody claiming to be from a trusted organisation, and who suggests money should be transferred from your bank account, you can now check to see if it's genuine.

All you need to do is: hang up, wait a few minutes for the line to clear, then call "159". You can then select your bank and be put through to their fraud department.

The number works in the same way as 101 for the police or 111 for the NHS. It's the number you can trust to get you through to your bank, every time.

If you're not sure how to use any of these tools, ask a trusted family member or friend to show you or book an IT buddy session at your local library.

Here are some recent frauds to look out for. Please share with family, friends and community.



Fake alternative energy advice

One of our readers had a card through his door from a company providing

alternative energy sources. The card included the logos of various energy and trade approval schemes. Trading Standards checked and the company wasn't recognised by any of the schemes.

Be vigilant when receiving any form of contact from companies offering alternative energy sources to save you money. Their claims may not always be accurate. You can speak to the [Energy Saving Trust](#) to find out how to make your home more energy efficient.



Rise of rogue gardeners in neighbouring county

Staffordshire County Council's Trading

Standards service has received more than 20 reports of rogue gardeners within the last two months.

Gardeners, tree surgeons and landscapers tend to be more active in the summer months. Rogue ones will promise to do a job at a reasonable price but then often ask for more money or even cash 'up front'. Watch out for ones who can start straight away. Rarely will you find good workers that can start immediately.



£400 energy rebate payment open to fraud

In June's bulletin, we warned of criminals sending

fraudulent messages about the £400 energy rebate payment due in the autumn.

The government has now [set out how this will be paid](#). It depends on how you pay for your gas and electric. It will be administered by your supplier and spread over several months.

You do not need to apply for it, so any form of contact asking you to do so is a scam.



Amazon gift card email fraud

When we talk to people about fraud, they often mention fake calls

or emails pretending to be from Amazon. As regular readers of this bulletin, you may be very vigilant. But, others are not. Action Fraud continues to get reports of people responding to emails offering a £1000 Amazon voucher as a prize.

Please continue to be vigilant, not respond to offers too good to be true, and share with friends who may not read this bulletin.

COMING NEXT TIME

- Current fraud alerts
- Banking fraud

Though we don't like to see you leave, you can unsubscribe from these bulletins by emailing sally.wilson@ageukce.org

The Older Persons Scams Awareness & Aftercare Project is brought to you by