

Introduction:

- West Sussex is seen as a hot sport for scams with 1949 reported in the UK between Oct-Dec 2022 of which 970 were in West Sussex.
- 80% online of all fraud reported amounted to £4.67M in UK lost of which £2.28M in West Sussex
- Av. age of victim is 75 (56%) 60-74 (26%) 30-59 (14%) Under 29 (4%) 63% are female 37% live alone
- Cost to economy £5-10 billion, 69% chance of being scammed again.

Oversharing:

With the various social media platforms, it is very easy to overshare.

We post photos when we are away on holiday (advertising we are away from home), fill out fun quizzes with lots of personal information (mother's maiden name, DOB, first pet etc)

Protect your privacy online – check your settings to ensure it is only friends and not public. Check your location settings – ie only on when using. Keep location on photos off. Search for your name and see what comes up.

1. **Courier fraud** (biggest in West Sussex)

- Avoid sharing personal info over phone
- Never disclose PIN
- Never give card to others
- Never transfer money on instruction of caller

2. **Romance Fraud** (1:3 marriages start online now)

- Secretive signs
- Invented reason for help – medical need, get back to the UK etc
- Pictures too perfect
- Reluctant to meet
- **Don't** rush into online relationships
- **Analyse** their profile
- **Talk** to friends and family
- **Evade** scammers
- **Stay** on the dating site messenger service

Top Tips:

Don't part with your hard-earned money.

Use the Google image reverse search, put a photo in here and it will show where this has appeared on the internet.

3. Investment Fraud

- Crypto currency, Bitcoin – if return on investment seems too good to be true.....it probably is.

4. Phishing emails

- Poor spelling, bad grammar
- Incorrect date
- Dear customer
- Asks to click on link – Don't
- Asks to open attachment – Don't
- Urgency to Act now
- You can hover over the email address to see if an alternative (real address) is displayed
- report@phishing.gov.uk

5. Car Buying Scams

- Marketplace – if an offer looks too good to be true - beware
- Seller asks for deposit before delivery
- Money received but car removed from marketplace

6. Telephone Scams

- Cloned numbers/contacts
- Out of the blue
- Ask for personal details
- Can they name the bank
- Wait 5 mins to stop line being kept open.
Then dial 159 national bank fraud line or use another phone
- Call blocking via Trading Standards or Telephone Preference Service

<https://www.westsussex.gov.uk/business-and-consumers/trading-standards-information-for-consumers/stay-safe-on-the-phone>

7. Mhishing - SMS Message Scams

- Report by forwarding message to 7726, it's a free service used by many organisations

8. General

- Privacy and Location settings
- Passwords - create a strong one (3 random words, capitals, numbers and symbol eg 10RoseCatNewspaper%
It's ok to write your passwords down or use a Password Manager
- Spot it - Stop it - Report it: ActionFraud 0300 123 2040, Call 101 or Scamalytics
- Further Scam Savvy session – Wed 15 Nov hosted online and in person at Crawley Library – bookable www.eventbrite.co.uk or to attend in person
- WSCC Resources: Website: www.westsussex.gov.uk/staying-safe-online
- Facebook & Twitter - @WSxSafeOnline
- E-newsletter – Staying Safe Online
<https://public.govdelivery.com/accounts/UKWSCC/Subscriber/new>

USEFUL CONTACTS

- **Sussex Police — Report a Crime (101)**
www.bit.ly/Sussex-Police-Report
- **CrimeStoppers**
www.bit.ly/Crimestoppers-Report
0800 555 111
- **National Cyber Security Centre**
www.ncsc.gov.uk
- **Action Fraud**
www.actionfraud.police.uk
0300 123 2040
- **Age UK**
0800 678 1602



Stay in Contact

Join my monthly E-Mail newsletter about my work for you in West Sussex and Westminster.

SCAN
HERE
TO
JOIN



AndrewGriffithMP.com/Sign-Up

Or fill in the below form and send to: Freepost REPRESENT

First Name

Surname

Post Code

E-Mail

Paid for Andrew Griffith, promoted by Josh Funnell, both of Top Floor, 62 Lower Street, Pulborough, RH20 2BW. Printed by Solopress, 9 Stock Rd, Southend-on-Sea SS2 5QF.

STAY SAFE FROM DIGITAL FRAUD

KNOW THE FACTS

- *Sophisticated digital fraud is on the rise*
- *Fraudsters can 'spoof' E-Mail addresses and phone numbers to appear legitimate*
- *Fraudsters rely on pressure tactics to trick victims into action*
- *The average victim loses over £10,000*

Remember, you should NEVER:

- X** Share any passwords or usernames
- X** Approve payments in an app or over the phone that you have not initiated
- X** Move or withdraw money at the request of someone claiming to be the bank or police
- X** Give out your PIN or One-Time-Passcode
- X** Follow suspicious links in unknown E-Mails that attempt to put you under pressure

Andrew Griffith MP
House of Commons
London SW1A 0AA

You can contact me by writing to:
Andrew.Griffith.MP@Parliament.uk

**ANDREW
GRIFFITH MP**

west sussex county council **Staying safe online**

Scam & Fraud Resource Sheet

Staying safe online team

We are an integral part of the Community Safety & Wellbeing Team at West Sussex County Council.

Our role is to raise online safety awareness amongst residents and partners across the county.

This resource sheet has links to documents, videos, and partner websites to help communities across West Sussex stay safe when they're online.

Staying safe online

Staying Safe Online eNewsletter – to sign up, visit: www.westsussex.gov.uk/email-alerts

Follow us on Twitter & Facebook by searching @WSxSafeOnline

Visit our webpage for information and to find out about local events: www.westsussex.gov.uk/staying-safe-online

What exactly are scams and frauds?

Scams and frauds are on the rise and nationally account for almost 50% of reports to the police each year.

Often targeting those most vulnerable in our communities, scammers will contact us by phone, computer, post, and even our front door.

The majority of scams pressure us to make a quick, one-off decision to part with our money or personal details for a promise of a service or product that does not exist.



west sussex county council **Staying safe online**

Important links

Action Fraud is the UK's national reporting centre for fraud & cybercrime. www.actionfraud.police.uk

Friends Against Scams is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims. www.friendsagainstscams.org.uk

Visit the **Take Five** website to test your knowledge with scams and frauds. www.quiz.takefive-stopfraud.org.uk

Citizens Advice is an independent organisation offering confidential information and advice. www.citizensadvice.org.uk

Operation Signature is a Sussex Police campaign to identify and support vulnerable victims of fraud. www.sussex.police.uk

Video resources

Archie Hicks Video
This video demonstrates some of the tactics scammers employ when contacting us. www.bit.ly/307B5dx

Scams – The Secret Crime
This eight minute video gives an overview of current scams and frauds. www.bit.ly/38DMFG5

Courier Fraud Videos
Our team have recorded a 41 minute YouTube video explaining courier fraud. www.bit.ly/courierfraudwebinar

Call **159** to verify a call from a bank or building society is genuine and forward unwanted or suspected scam messages to **7726** or **SPAM**.

In an emergency call **999** to report it to the police or **101** in a non-emergency.



Here is the link to the full video [Courier and impersonator fraud webinar - YouTube](#)

Here is the link to the shortened video [Courier fraud shortened video](#)

Staying safe online
TOP TIPS

TOP TIP

Create strong passwords using 3 random words

It is important to use different passwords for each of your online accounts. When creating passwords, the most secure method is using 3 random words and if possible, include numbers and symbols too. For example, "RedTreeDog4!".

Do not use words that can be guessed (such as your pet's name).

TOP TIP

Turn on two-factor authentication (2FA)

Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password.

Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity, such as:

- A PIN, password, or code
- Biometrics - a fingerprint or face ID

Visit <https://www.ncsc.gov.uk/cyberaware/home> for guides about how to set up 2FA.

TOP TIP

Your email account is very important

If a hacker gets into your email, they could:

- Reset your other account passwords
- Access information you have saved about yourself or your business

Your email password should be strong and different to all your other passwords.

Visit <https://www.ncsc.gov.uk/cyberaware/home> for guides about how to change your email password.

TOP TIP

Update your devices

Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack. Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.

Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time.

Some devices and software need to be updated manually. You may get reminders on your phone or computer. Do not ignore these reminders. Updating will help to keep you safe online.

Visit <https://www.ncsc.gov.uk/cyberaware/home> for guides about how to set up software updates.

TOP TIP

Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.

Visit <https://www.ncsc.gov.uk/cyberaware/home> for guides about how to set up automatic backups.

TOP TIP

Think before you click

Fraudsters are very skilled at sending 'phishing' emails where they impersonate trusted organisations like your favourite online shop or your bank. When you're reading an email, be very cautious about clicking on any links in the email or downloading an attachment unless you are 100% sure you know who the email is from.

TOP TIP

Is the webpage secure?

Before entering private information such as passwords or credit card details on a website, you can ensure that the link is secure in two ways:

- There should be a padlock symbol in the browser window frame, that appears when you attempt to log in or register. Be sure that the padlock is not on the page itself - this will probably indicate a fraudulent site.
- The web address should begin with 'https://'. The 's' stands for 'secure'.

TOP TIP

Security Software

Security software (also known as anti-virus software) helps to protect you from a range of threats that could put you at risk from hackers and fraudsters. Apart from the security features that come with your device, a number of third-party products are available. To get the best protection from any security software, you need to keep it up to date.

For more information visit: <https://www.getsafeonline.org/protecting-your-computer/viruses-and-spyware/>

TOP TIP

Help with Online Scams

You can contact Citizens Advice scams advisers if you:

- Think you might have found an online scam
- Need advice about scams
- Want to report an online scam

You can get advice from a Scams Action adviser by calling 0808 250 5050. The service is open from Monday to Friday, 9am to 5pm. Calls are free from mobiles and landlines.

TOP TIP

Help with Staying Safe Online

To find out more about how to stay safe online, access free resources, register for events and to sign up to the free monthly Staying Safe Online E-newsletter, visit www.westsussex.gov.uk/staying-safe-online or follow us on social media [WSxSafeOnline](https://www.facebook.com/WSxSafeOnline).