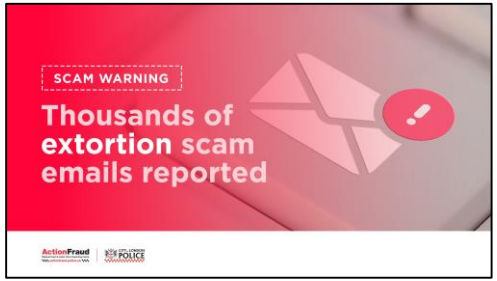
Fraud and Cyber Crime

Solihull – May/June 25

West Midlands POLICE

Current Trends



Action Fraud are urging the public to look out for phishing emails that relate to extortion as the Suspicious Email Reporting Service (SERS) received over 2,924 reports in March 2025, a staggering increase compared to only 133 reports made in February.

Read More- https://www.actionfraud.police.uk/news/extortion-alert

The reported phishing emails received by the National Cyber Security Centre's SERS relate to a type of extortion referred to as 'Financially Motivated Sexual Extortion' (FMSE).
Criminals will go to great lengths to make these types of extortion scams more convincing, including using a leaked password or home address in the phishing email to make it seem genuine.

What to do if you receive an email like this:

- As with other phishing emails, do not to engage with the phisher, forward the email to report@phishing.gov.uk, which is the NCSC's Suspicious Email Reporting Service (SERS), and then delete it.
- If you are considering paying the Bitcoin ransom, you should be aware that doing so, you will likely become the target of more scams, as the phisher will know they have a 'willing' customer.
- The inclusion of genuine passwords or other personal information in phishing emails is a strong indication that you may have been affected by a historic data breach. You can use this service to check which of your online accounts were affected: https://haveibeenpwned.com
- If the phishing email includes a password you still use, then change it immediately. Advice on how to create suitable passwords and enable other factors of authentication is available here: https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/improve-your-password-security/

If you have been a victim of extortion, or concerned that someone may be in possession of intimate images of you, you should report it to your local police force by calling 101.
Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you've lost money or provided financial information as a result of any phishing scam, notify your bank immediately and report it to Action Fraud at https://www.actionfraud.police.uk/report-phishingor by calling 0300 123 2040.

Ticket Fraud

When you buy tickets from a website or agent for a music concert or festival, a sporting contest such as a football match or rugby tournament, or a live comedian or performer, the tickets either don't arrive or turn out to be fake and you aren't refunded.

Only buy tickets from the venue's box office, the promoter, an official agent or a well-known and reputable ticket exchange site.

Protect Yourself

- Should you choose to buy tickets from an individual (for example on eBay or on a social media), never transfer the money directly into their bank account but use a secure payment site such as PayPal.
- Paying for your tickets by credit card will offer increased protection over other payments methods, such as debit card, cash, or money transfer services. Avoid making payments through bank transfer or money transfer services, as the payment may not be recoverable.

Spot the signs

- Check the contact details of the site you're buying the tickets from. There should be a landline phone number and a full postal address. Avoid using the site if there is only a PO box address and mobile phone number, as it could be difficult to get in touch after you buy tickets. PO box addresses and mobile phone numbers are easy to change and difficult to trace.
- Before entering any payment details on a website, make sure the web address starts with https (the 's' stands for secure). There should be That there is a locked padlock icon in the browser's address bar.
- Is the vendor a member of Society of Ticket Agents and Retailers (STAR)? If they are, you're buying from a company that has signed up to their strict governing standards. STAR also offers a service to help customers with outstanding complaints https://www.star.org.uk/dispute-resolution/

How it happens

You may find a website advertised via email or social media offering you the chance to buy tickets to a popular event.
Fraudsters create their own bogus ticket retail companies; their websites are easy to make and look genuine. Some even use a name or website address very similar to a legitimate ticket sales website.
This is a form of phishing; fraudsters take advantage of the huge demand for the most popular events. The tickets they're advertising have either already sold out, or haven't officially gone on sale yet, but their website claims to have tickets available. In some instances the event they're promoting doesn't even exist.
You pay for the tickets, but they aren't delivered. In some cases you may be told that a customer representative will meet you at the venue on the day to give you your ticket, but nobody turns up. You may even get the tickets in the post or print off an e-ticket, but when you arrive at the event, the organisers tell you the tickets are fake.
When you try to call the company you bought the tickets from, your calls aren't answered or you're told the company doesn't provide refunds.
If you're buying football tickets, it's illegal for anyone to re-sell them in most instances.

How to report it

Action Fraud call 0300 123 2040, online https://www.actionfraud.police.uk/

Courier Fraud

Victims are being contacted by telephone impersonating Police Officers or Bank officials.

- The suspect may have basic details about the victim such as their full name and address.

- They will claim that there is an issue with the victims bank account, or request their assistance with a false investigation.

- The victim is asked to co-operate in an investigation by attending their bank and withdrawing money / foreign currency from an exchange / purchasing high value items such as: jewellery, watches or gold (coins or bullion) or providing their Bank Card / PIN number and promising to send a 'courier' to collect these from their home.

- At the time of handover, victims are promised the money / items they have purchased / Bank Card / PIN number will be reimbursed but there is no further contact and the money / items are never seen again.

- In some cases, they may even convince the victim to transfer money to a supposed safe account.

- The bank or police will never ask for help with an investigation; to provide your bank card or PIN number, withdraw cash or purchase high value items.

- Your debit or credit card is yours: don't let a stranger take it from you. You should only ever have to hand it over at your Bank. If it's cancelled or expired, you should destroy it yourself.

- If you receive an unexpected call, hang up, wait a few moments as fraudsters may stay on the line after you hang up, and call a number known to you to confirm Their identity and the legitimacy of the call. Where possible, use a different phone line altogether.

Awareness videos: Video 1 / Video 2

Online Shopping Fraud

Suspects are exploiting both buyers and sellers via various 'Market Place' platforms. Facebook Marketplace is the most reported platform and the most frequently reported items are: iPhones, PlayStations, Air Fryers, and TV's.

- Suspects are publishing various fake listings. **Buyers** are encouraged by the offender to pay by an unsecured payment method.

- The buyer makes payment as requested; the item(s) never arrives or an item is received that is significantly different to what was ordered.

- In some instances, the offender sends an empty parcel to the victim, this is so that they can provide tracking details and proof of delivery should the victim make a claim of none receipt.

- **Sellers** have lost high value items after being led to believe that a payment for their listed item has been made or is pending and posts or hands over their item.

- The buyers in question may show fake bank transfer screenshots or email confirmations as proof of payment.

- After the seller has posted or handed over the item, they check their account and then discover the payment has not been made and that the 'buyer's' contact details are false.

- Check when the profile was created; if it was created very recently or has very limited information available, approach with caution.
- Check the seller or buyer's review history and feedback from other reviewers. Beware of accounts that may have been set up very recently with lots of favourable feedback that sounds similar, this could be an indication of fake reviews.
- Always use the site's recommended payment site, if they have one, and read the terms and conditions to understand what you are protected for. If you pay any other way than via a recommended payment site, you may not be able to recover your money.
- Always check your account or third-party payment facility to ensure a payment has been cleared before handing over or posting items. Do not use links or websites supplied by the buyer to check for payment, as these can also be forged and look genuine.
- If a buyer makes you feel uncomfortable, don't be afraid to block them and report them.
- **If you're meeting to exchange items, ensure your safety, take a friend or relative, and arrange to meet in a busy public place.**

Horizon Scanning and Seasonal Threats

Holiday Fraud

What it is-
When you've paid a travel agent or agency, or someone offering short-term lodging for rent online, and find out that the holiday you've booked (or parts of it) doesn't exist.

Protect yourself -

- Don't reply to unsolicited emails, texts, social media or calls with holiday offers. Links and attachments in emails may lead to malicious websites or download viruses.
- Book a holiday directly with an airline or hotel, or through a reputable agent. Check whether they're a member of the Association of British Travel Agents.
  If you decide to deal directly with the property owner or a letting agent, ask them questions about the booking, room, location and area.
- Don't book on websites that don't have a padlock icon (https) in the address bar, and be extra cautious if you're asked to pay using bank transfer or cash; pay by credit or debit card if you can.

Spot the signs -

You're contacted out of the blue by a travel agent or company you've never spoken to before, offering a holiday at a very low price. The details, pictures or address of the property or hotel on offer look suspicious, or independent website reviews aren't favourable or don't exist. You're asked to pay using bank transfer or cash; pay by credit or debit card if you can for extra protection.

How it happens -

Fraudsters use fake online adverts, bogus sales calls, emails and text messages offering incredibly cheap rates to tempt you in to booking a holiday with them.

They may steal images of hotels or rented apartments from other travel websites and pass them off as their own.

You're told to pay in cash or via a bank transfer, such as MoneyWise or Western Union, which can be difficult to trace and isn't refundable.

You may find out at the airport that you're not booked on the promised flight, or once you arrive the hotel or letting doesn't have your name booked for a stay, or extras that were part of your booking – such as excursions or transport – aren't included.

In some cases, the fraudster may completely end contact after you've paid and won't confirm anything you've booked; the holiday they've offered doesn't exist.

You may be offered the chance to go on a free holiday in return for watching a presentation; this is holiday club fraud.

How to report it-
Report it to Action Fraud online or call 0300 123 2040. If they're a member of the Association of British Travel Agents, report to them too.

Identity Theft

IDENTITY THEFT happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit a fraud. Identity theft can take place whether the victim is alive or deceased.

Identity theft is often a pre-cursor to fraud but is not considered a recordable crime. A recordable crime is committed when a financial gain is made from the use of that person's identity by another individual. In fraud cases, the individual or company e.g., your bank who has or may have suffered a financial loss through the use of the stolen identity, will be the person considered the victim of fraud and you will be considered as a victim of identity theft.

If you're a victim of identity theft, it can lead to fraud that can have a direct impact on your personal finances and could also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved. You can find more information on what to do if your identity has been stolen by using the identity theft checklist.

If you have had your identity stolen but have not lost any money, you should still report it to the relevant organisations and should follow the steps in the identity fraud checklist which set out what you need to do to protect yourself.

IDENTITY FRAUD

Identity fraud can be described as the use of that stolen identity in criminal activity to obtain goods or services by deception.
Fraudsters can use your identity details to:
Open bank accounts.
Obtain credit cards, loans and state benefits.
Order goods in your name.
Take over your existing accounts.
Take out mobile phone contracts.
Obtain genuine documents such as passports and driving licenses in your name.
Stealing an individual's identity details does not, on its own, constitute identity fraud. But using that identity for any of the above activities does.

The first you know of it may be when you receive bills or invoices for things you haven't ordered, or when you receive letters from debt collectors for debts that aren't yours.
Once you realise that identity fraud has occurred you should sign up to a credit referencing agency, check and report any activity that you do not recognise.

The government has put together this checklist to help on the steps to take to repair your identity and prevent revictimization
(Attached in the email)

Crime Prevention Materials

Crime Prevention Advice

Cyber Security Training for School Staff https://scamcentre.co.uk/cyber-security-training-for-school-staff/

WMP Fraud Crime Prevention https://www.westmidlands.police.uk/advice/advice-and-information/fa/fraud/

National Cyber Security Centre https://www.ncsc.gov.uk/

Action Fraud A-Z of fraud – https://www.actionfraud.police.uk/a-z-of-fraud

Take Five To Stop Fraud https://www.takefive-stopfraud.org.uk/

If you get a call that seems off, stop, hang up, wait a moment to make sure the line is clear and dial **159**. It's a safe and direct way to connect with your bank when you're most at risk of being scammed. It's simple, easy to remember, and can't be faked so 159 will never call you.

Working in partnership, making communities safer

west-midlands.police.uk