NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 3/25 (2 Jun 25)

(The Community Awareness Update provides general information to enable personnel to keep up-to-date with routine crime prevention and security awareness correspondence; it is not provided for mission-related items and does not replace the Emergency Messaging System.)

WELCOME TO ALL OUR NEW 'FAMILY' MEMBERS; THE COMMUNITY AWARENESS UPDATE IS DESIGNED TO PROVIDE YOU WITH, HOPEFULLY, INFORMATIVE AND USEFUL INFORMATION.

- **E-scooters.**
- **EU Entry/Exit System (EES) update.**
- **UK speed limits (*limits not targets*).**
- **Rogue traders.**
- **Trending scams today.**
- **Stay Alert, Stay Alive.**

E-SCOOTERS:

What is an e-scooter?

Electrical scooters (also known as e-scooters) come under the category of 'powered transporters'. This covers a range of personal transport devices that are powered by a motor. E-scooters are classed as motor vehicles under the Road Traffic Act 1988. This means the rules that apply to motor vehicles, also apply to e-scooters including the need to have a licence and insurance.

There are two ways of using an e-scooter:
- By privately owning one.
- By renting one through an authorised rental scheme.

Owning your own e-scooter:
- It's not currently possible to get insurance for privately owned e-scooters. This means it's illegal to use them on the road or in public spaces, such as parks, street pavements and shopping centres.
- If you use a privately-owned e-scooter in public, you risk the vehicle being seized under S.165 Road Traffic Act 1988 for having no insurance.
- If you cause serious harm to another person whilst riding an e-scooter, the incident will be investigated in the same way it would if you were riding a motorcycle or driving a car.

Where you can use your own e-scooter:
- If you own an e-scooter, you can only use it in on private land, such as in a garden. But you must have the permission of the landowner to do so.

Rental e-scooters:
You can rent e-scooters in some parts of the UK through e-scooter rental trials. Where a rental trial scheme is running, rental e-scooters can be used on public roads, some cycle lanes, and other public spaces. But you must follow the relevant road traffic laws. If you don't, you could face prosecution.

NIFC COMMUNITY AWARENESS UPDATE

To use a rental e-scooter in an approved area you must:

- Hold the correct driving licence.
- Have insurance (the rental companies provide this when you hire from them.
- Meet the minimum age limit (this can vary depending on the rental company, so please check with them).

When riding an e-scooter, you should always keep to the speed limit and it is recommended that you wear safety protection such as a helmet.

Penalties and offences for e-scooters:

- If you breach the rules when using an e-scooter you could face a fixed penalty notice or other form of penalty.

You could also be committing an offence if you're caught:

- Riding on a pavement: fixed penalty notice and possible £50 fine.
- Using a mobile phone or other handheld mobile device while riding: £200 and six penalty points.
- Riding through red lights: fixed penalty notice, £100 fine and possible penalty points.
- Drink driving: the same as if you were driving a car, you could face court imposed fines, a driving ban and possible imprisonment.

If you're using an e-scooter in public in an antisocial manner, you can also risk the e-scooter being seized under section 59 of the Police Reform Act.

EU ENTRY/EXIT SYSTEM (EES) UPDATE:

On 5 Mar 25, EU Home Affairs Ministers endorsed a revised timeline for the implementation of the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). After the EES becomes operational first in October 2025, ETIAS is expected to follow in the last quarter of 2026.

UK SPEED LIMITS (*Limits not targets*):

In the UK, national speed limits are 30 mph in built-up areas (generally roads with street lighting), 60 mph on single carriageways, and 70 mph on dual carriageways and motorways. Many areas in Scotland and Wales operate a 20 mph limit in built-up areas.

Specific Limits:

- Built-up areas: 30 mph in England, Scotland and Northern Ireland; 20 mph in many areas in Scotland and Wales.
- Single carriageways: 60 mph for cars, motorcycles, car-derived vans and dual-purpose vehicles.
- Dual carriageways and motorways: 70 mph for cars, motorcycles, car-derived vans and dual-purpose vehicles.
- Cars towing caravans or trailers: 50 mph on single carriageways, 60 mph on dual carriageways and motorways.
- Buses, coaches, and minibuses: 70 mph on motorways.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

- Goods vehicles (up to 7.5 tonnes): 70 mph on motorways.

Additional limits will be signposted where necessary.

ROGUE TRADERS:

- Cambs Police received a call last week from a worried woman whose elderly mother had been targeted by suspected rogue traders. Her mother reported that she saw two men pull up at her home in Cambridge on her doorbell camera. They asked if she wanted her gutters cleaning, but before she could answer, they retrieved a ladder form their van and headed up towards the roof.
- The woman said they were up there for less than five minutes before coming back down and demanding £100 payment, which she dutifully paid.
- She was approached twice more the very same week by people asking if she wanted her gutters clearing. Thankfully, she refused on these occasions and they left.
- We often see a spike in reports of rogue trading during the summer months, as people require garden work and home improvements.
- Look out for elderly or vulnerable family, friends and neighbours and report anything suspicious.

What are rogue trader or doorstep scams?

- You're at home one day when you hear a knock at the door. A supposed tradesperson, often a roofer, driveway builder or gardener, is there. They say they're working in your area. They've noticed some urgent work that needs to be done on your home and they've kindly come round to offer their services. For a cash fee. Or perhaps there's a small job they wouldn't mind patching up for you for a surprisingly low cash-in-hand price.
- You don't want to let this opportunity pass. And you're worried about the damage to your property if you let this issue continue. So, you agree to their price given the urgency of the situation.
- The scammer may trick you into paying in full upfront, before they've even started work. They may find 'additional problems' after starting work, which need extra cash immediately. Or they may get you to pay some of the quote but then never return to finish the job or make good.

Common reports include:

- Taking a deposit and never returning to do the work
- Quoting a price and then increasing the cost as the job progresses
- No statutory cancellation notices (cooling off period - see below), guarantees or warranties provided
- Produce poor quality work and refuse to sort out problems or finish the work

Avoiding Rogue Traders Advice:

- Be cautious; if a trader knocks at your door, do not agree to on the spot house repairs without taking advice. Say 'no thank you' and close the door.
- Be wary of special offers. They will use tactics such as 'I am only in your area today and would need to do the work now'.
- Do not believe when told that guttering, roofing, gardening or paving work is in need of urgent repair – this may cause you to panic and allow the work to take place.

- Don't allow anyone to pressure you into agreeing to have work carried out. If you ask them to leave and they don't, they are committing a criminal offence - contact the police on 999.
- Do not make snap decisions. If you feel that any work needs carrying out on your property, take time to talk to family or neighbours before you make a decision.
- Don't ever go to a bank or cash point with a trader; legitimate traders would never do this!

SCAMS TODAY:

Pre-Mar 20, the world was very different; before lockdown even began, opportunistic scammers were pulling out all the stops to catch out innocent people, leading Action Fraud to warn that coronavirus-related fraud - such as shopping scams peddling PPE and hand sanitiser - fuelled a 400% increase in scam reports. Scams are now part of daily life and some of the biggest include:

- 2021: Delivery text scams and bank impersonation scams.
- 2022: 'Hi Mum and Dad' WhatsApp scam and energy impersonation scams.
- 2023: The rise of QR code scams.
- 2024: Parking fine scams and celebrity AI scams.
- 2025: Sim-swap and purchase scams thrive.

Delivery text scams and bank impersonation scams: Delivery text scams were rife in 2021, with scammers capitalising on the continued demand for online shopping and delivery. These scams involve various claims that you've missed a parcel, underpaid for postage or have incomplete address information. These scammers phished for details in the hope they could do further damage by infecting your device with malware or gain enough information to con you at a later date.

'Hi Mum and Dad' WhatsApp scam and energy impersonation scams: As the cost of living crisis started to bite, it was no surprise that scammers saw yet another opportunity to catch people out. The UK's energy crisis deepened and we saw scammers impersonating many of the big energy companies to offer refunds and grants - all examples were attempts to steal your details. As households adjusted to sharp increases in bills, scammers also found success in impersonating adult children on WhatsApp and appealing to their parents for money to pay a bill or fix a broken phone.

The rise of QR code scams: Since 2023, reports of QR code scams have rapidly increased. QR codes are the black-and-white squares that you can scan with a smartphone to send you to a website. The technology has been around for years, and scammers find them a useful means of disguising a dodgy link. The link could expose you to malware or sign you up for a subscription trap. These scams began to appear as stickers on parking payment machines to con you into using a fake website. More recently, they've appeared on restaurant menus and packages. It can be hard to tell if a QR code is genuine, so always vet the website it's sending you to before you click through. Inspect the link by clicking on additional settings within the scanner, or you could turn off internet access for your device (put it on airplane mode) and open the link to view the address details first.

Parking fine scams and celebrity AI scams: Text message scams continued to plague our devices in 2024, this time with claims of outstanding parking fines. While it may not sound convincing to some, if you've been caught off-guard or if you've had a recent parking problem, then these messages can cause just enough panic to get you to follow the instruction to click on a link and share your details. In many examples, we also saw copycat government websites. 2024 also saw an incredibly convincing new wave of celebrity impersonation scams using artificial intelligence (AI). Using free (and cheap) AI tech, scammers can create convincing footage and images of celebs endorsing and peddling all manner of goods and services - from fake crypto offers to Le Creuset giveaways.

Sim-swap and purchase scams thrive: In January, warnings were issued about Sim-swap fraud and why scammers want your phone number. This scam is proving to be popular and it's no surprise - scammers are hijacking phone numbers to steal bank security codes and access your social media. With access to your accounts, they can carry out all kinds of damage. First investigated in 2020, there has been an increase in reports in 2024 and 2025. A top tip is to secure your mobile account by asking your network provider for additional security measures, such as a Pin or password to be used to approve any account changes in-store or over the phone.

Trending today:

Several types of scams are trending today, including romance scams, investment scams, phishing attempts, social media scams and package delivery scams. AI-powered scams, like deepfake videos and cloned voices, are also becoming increasingly prevalent.

Some of the most common and concerning scams:

- **Romance Scams:** These scams often start with a fake online profile or a message on a dating app. The scammer builds a relationship, gaining your trust, before asking for money or gifts.
- Investment Scams: Scammers lure victims with promises of high returns on investments, often using social media or fake websites.
- **Phishing Scams:** These scams involve sending fake emails, text messages, or messages on social media that appear to be from legitimate companies. They often ask for personal information or urge you to click on a link to a fake website.
- **Social Media Scams:** Scammers use social media platforms to create fake profiles, post fake prize draws or sales, or impersonate individuals to trick victims into parting with their money or personal information.
- **Package Delivery Scams:** Scammers send fake emails or text messages claiming there's a problem with a delivery and ask for personal information or payment to resolve the issue.
- **AI-Powered Scams:** Scammers are using AI technology to create deepfake videos and cloned voices to impersonate individuals and promote fake products, services, or investments.
- **Impersonation Scams:** Scammers pretend to be from reputable companies, such as banks or government agencies, to trick victims into giving them personal information or money.
- **Advance Fee Fraud:** This scam involves promising victims a large sum of money or a valuable item in exchange for an upfront fee.
- **Cash App Scams:** Scammers use Cash App to trick victims into sending money, often by pretending to be a legitimate business or service.
- **Chargeback Scams:** Scammers make fraudulent chargebacks on e-commerce transactions, leading to losses for retailers.

NIFC COMMUNITY AWARENESS UPDATE

APR-MAY SCAMS:

29 May - Diet pill scam email: A scam email promoting weight loss pills. A dodgy email promoting a weight loss pill that 'naturally burns fat' claims that the product was successful on the TV show Dragon's Den. It goes on to provide a link to buy the pills. This will lead to a dodgy website created to steal your personal and financial information and send you nothing in return.

21 May - B&Q scam advert: A scam advert posted to Facebook. An advert on Facebook shares fake story which claims their daughter works at B&Q and the retailer is clearing extra stock. It goes on to say that you can receive a pallet of 'All Purpose Garden Soil' by following a link left in the comments to leave a 'quick review'. This link will take you to a dodgy website where your personal and financial information will be asked for.

19 May - Council Tax scam calls and texts: Wandsworth Council has warned of scammers contacting residents with requests to pay Council Tax arrears. The calls and texts claim that you owe thousands of pounds in uncollected Council Tax and you must pay immediately. The scammers also say that the council is currently in court due to your unpaid tax.

15 May - M&S impersonation email: A scam email claiming to be from M&S tells you that you're eligible for a 'free Afternoon Tea Letterbox Hamper with your next qualifying order.' It invites you to 'unlock your free surprise' by clicking on a link. However, this link leads to a malicious website which has nothing to do with M&S. This website will ask for your personal and financial information to scam you now or at a later date. M&S recently experienced a data breach, read what to do if you're worried about this here.

12 May - Shein 'mystery box' scam: A dodgy email peddling a fake Shein mystery box leads to a malicious website. The site will gather your personal and financial details while offering you nothing in return.

8 May - Apple impersonation scam: An email claiming to be from 'Apple security' tells you that your iPhone has been infected with 44 viruses. It then provides a link to remove these threats, which leads to a malicious site intent on stealing your financial info and data.

6 May - Failed delivery scam text: A scam text from 'The Sorting Centre' tells you that providing incorrect address information has led to two failed deliveries and leads to a malicious website to 'update your address.' The message also uses 'the recent frequent incidents of lost parcels' to appear more legitimate. The dodgy link included in the text will lead to a site designed to steal your personal and financial data or download malware to your device.

29 Apr - PayPal impersonation scam: A scam email impersonating PayPal tells you that an unauthorised transaction was made using your PayPal account. It prompts you to call a dodgy number to receive a refund, which will put you through to a scammer trying to get your personal and financial details.

24 Apr - Oasis fans have lost over £2m to ticket scams: Lloyds Banking Group has estimated, based on the volume of fraud reports made by its own customers, that since Oasis reunion tickets were released, more than £2m has been stolen by ticket scammers across more than 1,000 cases.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

NIFC COMMUNITY AWARENESS UPDATE

The bank said that many cases began on social media and that across its banks - Lloyds Bank, Halifax and Bank of Scotland - Oasis fans made up more than half of all reported concert ticket scams so far this year, losing £436 on average. The biggest amount lost in a single case was over £1,700. Fake Oasis tickets were the biggest type of ticket scams, with the average victim losing around £200 more than the average lost to a concert ticket scam. People aged 35 to 44 were the most likely to be scammed, making up nearly a third of all cases. Edinburgh, Warrington and Manchester have the highest numbers of victims.

Follow these top tips to avoid falling victim to ticket fraud.

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known ticketing website.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal give you a better chance of recovering the money if you become a victim of fraud.
- The password you use for your email account, as well as any other accounts you use to purchase tickets, should be different from all your other passwords. Use three random words to create a strong and memorable password, and enable 2-step verification (2SV).
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information visit star.org.uk/buy_safe.

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040, or call Police Scotland on 101.

22 Apr - Weight loss pill scam: A scam email impersonating Mail Online promotes a 'miracle weight loss pill.' The email also says that the product scored a deal on tv show Dragon's Den and includes a phishing link for you to purchase the item. The link will lead to a dodgy website asking for your personal and financial information.

16 Apr - Boots impersonation scam: A scam post on Facebook tells you that Boots is offering mystery boxes for £3 full of 'leftover cosmetics' in exchange for completing a short survey.
The post, most likely published from a scam or hacked account, includes a malicious link to complete the survey which is where your personal and financial details will be stolen.

14 Apr - Scam text impersonating Binance: A dodgy text claiming to be from cryptocurrency exchange Binance asks you to call a number beginning with 0808 if you didn't initiate a withdrawal request. Recipients of the text say that it contains a verification code. This could mean that scammers are attempting to get into your account and need you to give them the verification code to gain access. If you ring the number the scammer will most likely try to get you to reveal your personal and financial information.

10 Apr - Boots scam email: A scam email impersonating Boots promoting a 'Nivea sunscreen pack' asks you to complete a short survey in order to receive the items. The email impersonating Boots will lead to a malicious website which will ask for your personal and financial information.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

NIFC COMMUNITY AWARENESS UPDATE

7 Apr - One in four Britons have experienced a ticket scam: Data analysed by Nationwide has found that one in four Britons have experienced a ticketing scam, losing £82 on average. When buying tickets, stick to official retailers and be alert to scammers on social media. Avoid offers that seem too good to be true and don't pay by bank transfer. If you've lost money to a scammer, call your bank immediately using the number on the back of your card. Report the scam to Action Fraud or call the police on 101 if you're in Scotland.

1 Apr - The UK is a hotbed for WhatsApp scams: Data analysed by Revolut has found that between 1 January 2023 and 31 December 2024, British consumers lost more money to scams through WhatsApp than any other country in Europe. It also revealed that WhatsApp fraud accounted for one in five of all reported scams in the UK and victims lost an average of £2,437 per fraud incident. In the second half of 2024, WhatsApp's fraudulent activity surged by 33% and two of the biggest scams on WhatsApp were job scams, making up half of cases on Revolut, and investment scams, making up four in 10.
You can report a WhatsApp message by selecting it in your conversation and tapping 'report'. To report the sender on WhatsApp, open up the chat, tap on the sender's contact details and select 'block and report'.

Purchase scams: When you pay for something you never receive, continue to lure victims in with tempting offers.

- In just the first three months of 2025, Santander customers lost almost £3.5m to a purchase scam. The bank also revealed that cases involving gig tickets exceeded 10% of all purchase scam claims. Some of these cases capitalised on the recent demand for Sabrina Carpenter and Coldplay tickets.
- Online shoppers are reminded to be cautious of offers that seem too good to be true, e.g. seven scam ads impersonating the retailer Bonmarché.

Protect yourself from scams:

- Be sceptical of unsolicited messages or calls.
- Verify the legitimacy of any requests for personal information or money.
- Research any investments or businesses before investing or doing business with them.
- Be careful about clicking on links in emails or text messages, and avoid sharing personal information on social media.
- If you suspect a scam, report it to the relevant authorities or the company.
- For scam calls received on WhatsApp, open the WhatsApp chat with the dodgy phone number and tap 'block.' You can report the contact by tapping 'report contact' and 'block'.
- If you spot any suspicious posts, you can report them to the social media platform and the National Cyber Security Centre to investigate. On social media, posts are usually reported by selecting the three dots in the top right corner of the post and pressing 'report.'
- Scam emails can be reported by forwarding them to report@phishing.gov.uk.
- Malicious websites can be reported to the National Cyber Security Centre.
- You can report scam texts by forwarding them to 7726.
- On an Android phone, text the word 'call' to 7726. You'll then receive a message asking you for the scam number.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

.. and watch out for:

Fraudsters have impersonated Google by 'spoofing' a Google email address and support page in a convincing and widespread scam.

- Spoofing is when scammers disguise themselves by masking their true identity with a genuine email address and phone number. This can make it difficult to spot a scam, unless you know what to look for and how to look for it. In this particular attack, the scammers also managed to bypass Google's filters for scam and suspicious emails.

- The scam email was first highlighted by Nick Johnson, a developer who'd received the message and posted it on X. The message appears to be sent from a Google email address, no-reply@google.com, with the familiar heading 'Security alert.' The email explains that you have been served a 'subpoena', which is a formal court order, to grant Google permission to 'produce a copy of your Google account content'. The message includes a link to your 'Google support case'. You're then encouraged to follow the link as you're informed that you can 'examine the case materials or submit a protest'.

- The website linked to the email convincingly impersonates Google's support page by beginning with 'sites.google.com'. It also prompts you to log in to your account if you aren't already signed in. It then offers you the opportunity to 'view your case', which is labelled as urgent. It's unclear where the scam goes from here, but it will most likely lead to malware being downloaded to your device or you being pressured to enter your personal and financial data, giving it over to the scammers.

How did the scammers do this?

- Anyone can create a Google Sites page. In this case, fraudsters have exploited this to mock up a fake support page, which they control and which could appear to be legitimate with its language and branding.
- While the attackers didn't send the email from no-reply@google.com, they made it look like they did by manipulating (spoofing) the 'from' address by creating a malicious code to alter the email.
- What's more, because the body of the email was copied by the fraudsters from a legitimate email from Google, it retained its DKIM signature. This isn't visible in the email but it's a security feature that proves the email is from where it says it's from – and so it passed Google's security filters.
- Which? contacted Google about this scam email and informed that it has shut down the mechanism that attackers are using to create the scam email. It also said that Google will not ask for any of your account credentials – including your password and one-time passwords. It also won't ask you to confirm push notifications or call you.
- Google also told Which?: 'We're aware of this class of targeted attack from this threat actor and have rolled out protections to shut down this avenue for abuse. In the meantime, we encourage users to adopt two-factor authentication and passkeys, which provide strong protection against these kinds of phishing campaigns.'

NIFC COMMUNITY AWARENESS UPDATE

KEY INFORMATION:

The future?: The above scams will continue to thrive, especially purchase scams and dodgy online shopping scams; already, millions have been lost to these scams this year. Always double-check an offer that seems too good to be true, especially if it's time-limited and rushing you to purchase. Always look at reviews across a few platforms before you buy and watch out for websites that are missing vital information about returns, contact details, location and T&Cs.

Stay ahead of the scammers: What if you could get scam warnings before they hit your inbox, your doorstep or your bank account? You can join almost half a million subscribers to Which? and get a trusted fraud expert in your inbox. The weekly emails give real-life examples of scams, the newest tactics being used and clear and simple tips on how to spot and avoid these scams. Sign up for free Which? Scam Alerts

Spotting and reporting scam emails: Sophisticated phishing emails like this one highlight the need to inspect suspicious emails thoroughly. To protect yourself, you should:

- Examine email headers – on Gmail, clicking on the arrow next to 'me' under the sender can show you the full email address that the email has been sent from.
- Hover over links to see if any of them could be suspicious. Pay attention to spelling errors or website addresses that don't quite match that of the organisation it claims to be affiliated with. The domain information checker Who.is will show you when the website was created – if the site was created recently, then it's likely to be dodgy.
- Be suspicious of emails trying to rush, pressure or scare you into doing something.
- Make sure you never click on links if you're suspicious about the email. You can report email scams by forwarding the email to report@phishing.gov.uk. You can also report emails to your email provider – select the 'Report Spam' on Gmail.
- If you lose any money to a scam, call your bank immediately using the number on the back of your bank card and report it to Action Fraud, or call the police on 101 if you're in Scotland.

Spotting and reporting purchase scams: Purchase scams typically start as ads and posts on social media or search engines. Some signs that a post, ad or website may be part of a purchase scam are:

- Discounts and offers that sound too good to be true - be wary of heavy discounts and claims of selling in-demand goods.
- Limited-time offers or any claim that gets to act with urgency, such as a closing down sale.
- Ads, posts and search results that aren't posted from a brand's official accounts or lead to websites that differ from the official website.
- Newly registered websites such as these could have been set up with the intention of scamming victims. Using a domain checker like who.is can tell you when a website was created.
- Negative reviews, especially if they're posted across multiple review platforms.
- Websites that don't feature 'contact us', 'about us' and terms and conditions pages.

To report a scam post or ad on Facebook or Instagram, select the three dots on the right-hand side of the page and click 'report'. Malicious websites can be reported to the National Cyber Security Centre. If you lose any money to a scam, call your bank immediately using the number on the back of your bank card and report it to Action Fraud, or call the police on 101 if you're in Scotland.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

NIFC COMMUNITY AWARENESS UPDATE

REPORTING:

- You can report scam texts by forwarding them to 7726.
- If you've lost money to a scammer, call your bank immediately using the number on the back of your card. Report the scam to Action Fraud or call the police on 101 if you're in Scotland.
- Scam emails can be reported by forwarding them to report@phishing.gov.uk.
- Malicious websites can be reported to the National Cyber Security Centre.
- You can report a WhatsApp message by selecting it in your conversation and tapping 'report'.
- To report the sender on WhatsApp, open up the chat, tap on the sender's contact details and select 'block and report'.
- To report a scam post on Facebook, select the three dots on the right-hand side of the page and click 'report'.

SMISHING SCAMS ARE EVOLVING:

A new report from cybersecurity firm Palo Alto Networks' Unit 42, the company's cybersecurity division specializing in threat intelligence and incident response, has uncovered that these scams are designed to steal sensitive information, including credit card and bank account details. What started as a scheme involving fraudulent toll payment notifications has now expanded to include fake delivery service alerts, tricking users into clicking malicious links. The scam appears to be operated by local cybercriminals using a toolkit developed by Chinese hacking groups. Notably, research from Unit 42 shows that many of the scam's root domains and fully qualified domain names use the Chinese .XIN top-level domain (TLD).

6 ways you can protect yourself from smishing scams:

- Verify before you trust: Treat unsolicited texts with caution. If a message claims to be from a government agency or company, don't click any links or act immediately. Instead, verify the claim by contacting the organization directly using an official phone number or checking their verified website.
- Avoid clicking suspicious links and use strong antivirus software: Scammers use links to direct you to fake websites that can steal your personal or financial information. Instead of clicking on any link in an unexpected text, manually type the known URL into your browser or search for the organization's official website.
- Keep your devices secure: Regularly update your devices' operating systems and apps to ensure you have the latest security patches. Consider installing reputable security software that can help detect phishing attempts and warn you about potentially dangerous websites or messages.
- Use a password manager: A trusted password manager can help protect your sensitive information by automatically filling in credentials only on verified sites. This minimizes the risk of entering details on fraudulent websites and can alert you if a site doesn't match what's expected. Get more details about my best expert-reviewed Password Managers of 2025 here.

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013

- Report suspicious activity: If you receive a text that seems off, report it immediately to your mobile carrier, local law enforcement or the FBI's Internet Crime Complaint Center (IC3). Reporting helps authorities track down scammers and prevent further attacks.
- Consider using a personal data removal service: Personal data removal services can help reduce your exposure to smishing attacks by removing your sensitive information — like phone numbers, addresses and email details — from data broker websites. Scammers often rely on these publicly available databases to target victims with personalized phishing texts. These services aren't foolproof, but they can make it harder for cybercriminals to find and exploit your information. While no service promises to remove all your data from the internet, having a removal service is great if you want to constantly monitor and automate the process of removing your information from hundreds of sites continuously over a longer period of time. Check out my top picks for data removal services here.

NIFC COMMUNITY AWARENESS UPDATE

STAY ALERT, STAY ALIVE:

The Counter Terrorism Policing message remains in that you should trust your instincts and report anything that doesn't feel right when you are out and about in the coming weeks.

Sadly, the threat from terrorism is a real one. Every year across the UK, Counter Terrorism Policing receives over 10,000 reports from the public and a fifth of those provide intelligence which is particularly useful to investigators. Since 2017, CTP, along with partners, have disrupted over 40 terrorist

Policing and security authorities encourage the public to trust their instincts and report anything that doesn't feel right to security or the police.

- You can help by sharing campaign messages for any events you are organising or supporting.
- You can increase your awareness by taking the free online ACT Awareness e-learning training.

Promoting the awareness and vigilance is also a powerful way of using communications as an extra layer of protective security. By supporting the campaign and using security-minded communications, you could help to deter hostile activity at major events.

We all have a role to play in keeping each other safe.

Wherever you are, whatever the situation….

If you see something, say something.
Stay Alert, Stay Alive!

Is it an emergency? Call 999

If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

If you want to report a concern anonymously, you can report it via the Crimestoppers website or via their hotline on: 0800 555 111.

NIFC (24/7): 01480 847013