NIFC COMMUNITY AWARENESS UPDATE

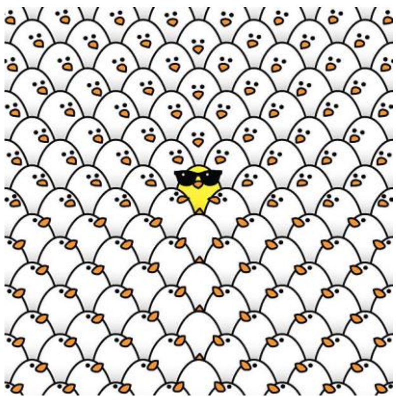
NIFC COMMUNITY AWARENESS UPDATE 12/24 (22 Nov 24)

(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.

CONTENT:

FESTIVE SEASON VIGILANCE:



If only the 'bad ~~chick~~ guy' was always this obvious!

Keep it in perspective, but remember that the 'bad guy', unless disrupted before they act, won't stand out until it might be too late.

With a winter season full of events, such as Christmas shopping, festive markets, pantomimes and concerts, we all have a role to play in keeping each other safe. As the festive period approaches, it is important to remember that the UK still faces a diverse and evolving terrorism threat; that's why the UK terrorism threat level remains at SUBSTANTIAL, meaning an attack is LIKELY.

We commend an understanding of, and applying risk mitigation, in line with Counter Terrorism Policing's Winter Vigilance Toolkit.

Is it an emergency? Call 999

If it is not 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

CRACKDOWN ON DRINK AND DRUG DRIVERS THIS CHRISTMAS:

The easy part is just advising you to never drink and drive; but human nature being what it is….

- Many police forces will be advertising the 'designated driver' scheme to support the crackdown on drink and drug drivers this Christmas – they need your help. 'I am DES' is a national initiative where licenced premises sign up to offer an incentive to encourage customers to have a 'designated driver' within their party. Locally, the campaign ran for the first time since Covid in Dec 23 across Cambridgeshire, with more than 60 businesses signing up in support (the most recorded to date!). Importantly, it saw a reduction in the number of people killed and seriously injured through road traffic collisions for that month compared with the previous year (with more than a 20% reduction).

- Business and venue locations will be included in a press release highlighting this year's police drink and drug drive campaign, and mentioning the 'I'm DES' initiative, where drivers within a group can benefit from a discount on soft drinks only. Members of the public can take part if they advise venue staff "I am Des" or words to that effect and show their car keys.

KEEPING IN THE 'FESTIVE' MOOD………….

Top 5 Christmas Cyber Scams:

- **Fake Delivery Emails:** The most popular type of seasonal phishing attack is linked to logistics. Scammers know that as Christmas approaches, people are sending lots of packages to friends or families or expecting the delivery of parcels themselves. Victims will receive an email from what appears to be a legitimate courier company informing them that they've missed the delivery of a parcel. The email will often be urgent in tone and warn the recipient that their package won't be delivered in time for Christmas if they don't act quickly. To select a new delivery time, they will be instructed to click on a link within the email, and upon clicking the link, they will be taken directly to a phishing website or their computer will be infected with malware.

- **Christmas eCards:** eCards have become a very popular and inexpensive way to send friends and families a card at Christmas. Scammers have been quick to take advantage of this online format and use it as a guise to trick victims into downloading and installing malware. As soon as you click on the link to view your card, there's a good chance you'll be downloading adware, spyware, or a Trojan virus onto your computer. Red flags that an eCard is malicious include; spelling mistakes, an unknown sender, suspicious link, or an attachment that ends with ".exe,". This can indicate an execute command which may install a virus onto your PC.

- **Seasonal Offers:** It can be hard to resist the lure of a discount online, especially at Christmas, but these too good to be true offers usually are! Cyber criminals will often create a fake URL page imitating well-known brand, then pretend to offer a real promotion. These scams are often set up specifically to harvest user data and will require the input of personal information.

- **Gift Card Survey Scams:** Fraudsters will often create Christmas promotion pages that claim to be associated with big brand names. The pages are full of offers to win expensive prizes, vouchers and gift cards. To be in with a chance of winning, all you have to do is like the page and share the promotion with your friends. This ensures the scam reaches as wide an audience as possible. The next condition of entry is to complete an online survey to verify your identity. This is just a cunning way for scammers to harvest your personal or financial details and commit identity fraud or sell your details on the dark web. Always be wary of any promotion that asks you to like and share material or participate in an online survey to enter.

- **Charity Phishing Scam:** Cyber criminals are extremely devious and know that people will tend to be more charitable at Christmas and donate to those less fortunate. To exploit this goodwill, fraudsters will set up websites designed to look exactly like the genuine website of reputable charities. As soon as you enter the website, you will be asked to donate by providing your credit card details and personal information. The criminals will then use this data to steal your money or commit identity fraud. When donating to charity it's always best to go directly to the charity's website and never follow a link within an email.

How to Avoid Christmas Cyber Scams:
- Never click on links or download attachments from unknown sources.
- Always verify the security of a website.
- Pay close attention to the spelling of an email address, if there are any inconsistencies, delete immediately.
- Ignore and delete emails with poor grammar and formatting.
- If the email is threatening or urgent in tone, do not respond. This is a common tactic used to pressurise a victim into taking immediate action.
- If you get an email, phone call, social media message or text message about a parcel you weren't expecting, treat it with suspicion.
- Be wary of email offers – If an offer seems too good to be true, it usually is.
- Enable a spam filter on your email account.
- Back up data on a regular basis.
- Install the latest anti-virus software solutions on your work devices.
- Use strong passwords including email and social media accounts to reduce the chance of devices being hacked.

OTHER SCAMS….

Quishing scams:

Quishing, also known as QR code phishing, involves tricking someone into scanning a phony QR code with their phone or device. The QR code then takes the user to a fraudulent website that might download malware or ask for sensitive information. QR codes are often found on things like parking machines, charging points, emails, even restaurant menus and you may well use them even more this time of year as you dash between car parks to purchase presents and meet up with friends in cafes and restaurants.

NIFC COMMUNITY AWARENESS UPDATE

Prevention:

- Check… if the QR is on a poster in a public area, always check whether it appears to have been stuck over the poster, window or billboard. If the sign or notice is laminated and the QR code is under the lamination or part of the original print, chances are it's more likely to be genuine.
- If in doubt… download the app from the official Google or Apple store or search the website on your phone's internet browser, rather than scanning a QR code to take you there. It may take longer, but it's more secure.
- Trust your instincts, if something doesn't feel right, it probably isn't.

8 Nov: DVLA scams - Action Fraud has received 1,186 reports about scam emails impersonating the Driver and Vehicle Licensing Agency (DVLA). The messages claim that your vehicle tax payment has failed and includes a link to 'retry payment.' This will lead to a malicious website designed to steal your personal and financial information.

6 Nov: Portable heater scam email - A scam email advertising a portable heater; a dodgy email which claims to offer a portable heater for 30% off and says that the device is endorsed by Elon Musk. You're encouraged to follow a link to 'order now' which will lead to a malicious site that'll ask for your personal and financial data. This is yet another example of a celebrity scam advert.

4 Nov: Tesco voucher scam - A scam email impersonating Tesco; an email impersonating Tesco offers a non-existent voucher for £750. It includes a dodgy link to a phishing website which will try to get your personal and financial details.

You can report scams by forwarding them to report@phishing.gov.uk

Malicious websites can be reported to the National Cyber Security Centre

FALLING VICTIM TO A SCAM CAN BE DEVASTATING, BOTH FINANCIALLY AND EMOTIONALLY.

- Unfortunately, fraudsters are coming up with a growing number of ways to try to part us from our cash, increasingly using AI to help them, and these often appear totally credible. According to latest figures from UK Finance, more than £570 million was stolen by scammers in the first six months of 2024 alone. Below is a rundown of some of the different types of scams currently doing the rounds, and what you can do about them.

- If you're not certain whether something is a scam or not, you may want to consider signing up to Ask Silver, which is a free AI-powered scam checking tool designed to help you spot scams. You simply snap a photo or screenshot of any email, website, or leaflet you're worried about and send it to Ask Silver on WhatsApp. Ask Silver uses the power of artificial intelligence (AI) to spot any red flags and provides suggestions for next steps on staying safe, and if a scam is identified, you can Ask Silver to report the scam to relevant agencies on your behalf.

NIFC COMMUNITY AWARENESS UPDATE

TRENDING SCAMS AT THE MOMENT AND INTO 2025:

Parking fine scam: Growing numbers of people are reporting that they've received a notification about an unpaid parking fine. Victims are told to click on a link which takes them to a copycat site impersonating a government website. Upon entering your car registration details, you're told you've incurred a penalty and must enter your payment and personal details.

- **What you can do:** Never click on any links in unexpected text messages or emails, and remember that all official government pages start with gov.uk. You should report scam websites to the National Cyber Security Centre and texts can be forwarded to 7726.

Booking.com scam: Booking.com customers have been warned by a cybersecurity firm that scammers are paying to steal their account details on the dark web. Scammers are specifically focused on customers of hotels that are signed up to use the site's services. They are sending phishing emails to customers that state payment information is required immediately to secure reservations. Since March this year, holidaymakers from a wide range of countries including the UK, US, Italy and Portugal have stated online that they have been a victim of fraud through Booking.com.

- **What you can do:** Be cautious of unsolicited emails or messages, especially those claiming to be from hotels or service providers. Go directly to the hotel through known contact methods before taking any action. Avoid clicking on suspicious links, particularly those received through emails or messages, to prevent malware downloads.

Vehicle scams: Fraudsters set up fake listings on online marketplaces or social media for vehicles that don't exist. When you get in touch, the fraudster asks you for a deposit to "secure" the vehicle and comes up with a reason why you can't see the vehicle in person beforehand. The fraudster might also pressure you to make a decision quickly by implying they have lots of other offers. After you send the money, they block you and delete their profile.

- **What you can do:** Always buy a vehicle from an authorised dealership if you can, as anyone can list anything online. If you are buying online, make sure you have seen and tested the vehicle yourself before handing over any money. Avoid paying by bank transfer and use a debit or credit card – that way, your money will be protected if something goes wrong.

Bogus giveaways: Scammers send emails, text or WhatsApp messages offering really appealing giveaways or deals. Consumer Group Which? flagged one that was sent out widely in 2022, claiming to be from Emirates Airlines offering free holidays. However, the particular brand or offer varies widely.

- **What you can do:** If you receive an offer via email or message that looks too good to be true and claims to be from a well-known brand, it's probably a scam. Links in scam messages are often shortened so they don't appear as the full, official website, and you don't know where they are taking you.

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

'Dieselgate' compensation scam: You might have seen adverts on social media promising compensation to people who owned vehicles affected by the 'dieselgate' scandal which emerged in 2015. This scandal primarily revolved around car manufacturers installing 'defeat devices' in cars between 2009 and 2020 which affected emissions tests so that these vehicles would meet legal standards. However, in reality emissions significantly exceeded permitted limits under normal driving conditions. Scammers are targeting motorists by promising high levels of compensation, usually in return for an upfront fee.

- **What you can do:** Steer clear of any requests for personal information which might be used to steal your identity. You should also be wary if you're told you're eligible for a very large amount of compensation, but only if you make an upfront payment. If you are keen to pursue a compensation claim, then you may want to consider using a legal service that operates on a 'no win, no fee' basis so that you only have to pay a fee if your claim is successful.

ENERGY-RELATED SCAMS - Steep energy bills in recent years have prompted fraudsters to expand the types of scams they are using to part victims with their cash.

Fake refund: Scammers pose as a major supplier and announce on email that you are entitled to a refund on your energy bills because of a "miscalculation". One version saw fraudsters posing as E:on claiming people were entitled to an £85 refund, with a link to enter bank details to get your money. Many who received it weren't with E:on so this raised red flags, but some were.

- **What you can do:** Check the email display name. Names reportedly used by scammers include eonhelp.com or Eon Winter Payment. You can always call your energy supplier using the number on its website. Also, check what your most recent bill says, and remember that in current times it's unfortunately unlikely that you will be due a refund. Your supplier would never contact you to request your bank details, as it already has these for your direct debit payments.

Debt collector scam: Fraudsters are taking advantage of customers whose energy suppliers have gone bust over recent years, with debt collector demands claiming they have an outstanding balance on their account. Emails may even be addressed by name, as customer information passes through many channels when a firm goes under, such as energy brokers, new suppliers, and debt collection agencies.

- **What you can do:** Contact aimed at collecting an outstanding balance or returning credit on your account should only be received several months after your supplier goes out of business. You should never receive a request years later, as has been the case for scammers who targeted Brilliant Energy customers. If you receive a request for a debt you were unaware of from a previous energy supplier you should contact Action Fraud either online or by calling 0300 123 2040.

Meter tampering scam: There have been claims made on social media that you could save money on energy bills by tampering with your meter, but doing so should be avoided at all costs. A man in Leicester was given a three-year prison sentence in 2018 for tampering with his meter, as this risked causing an explosion and endangering lives.

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

- **What you can do:** If you are worried that a meter has been tampered with, you can make an anonymous call to Stay Energy Safe on 0800 023 2777. Turn off the gas if you smell gas, and open windows and doors, and leave the property. Call National Grid Gas on 0800 111999.

Energy saving device scam: Fraudsters recently marketed a device called Voltex, previously marketed under the name Motex. These were for sale on websites, Amazon and eBay, but none of these passed the Which? Basic safety test, and were at risk of causing fire or electric shocks. There was also no evidence that they would save money.

- **What you can do**: Beware of any extreme claims made by companies marketing 'energy saving devices' and look for a CE/UKCA mark to ensure it meets safety standards before using it. If you paid for a useless/dangerous device using a debit or credit card, you may be able to claim a refund using chargeback or Section 75 of the Consumer Credit Act.

Pre-payment doorstep scam: Households using pre-payment meters are offered reduced cost energy, according to Action Fraud, by scammers on their doorstep. For example, this may be £50 off an electricity meter top-up if you hand over £25 in cash. However, the scammers use cloned keys to top up energy credit illegally, which leaves you paying for the same amount of energy twice, as your supplier never receives the payment.

- **What you can do**: If someone knocks on your door offering a reduction in your energy bill, politely decline the offer. It's likely to be a scam, and call your supplier to report the incident.

Price comparison phone scam: Many of us are worrying about our energy bills, and would usually be able to fix our tariff to provide security and reduce costs. However, there are currently no open market fixes on the market that are worth switching to, unless you're willing to pay a fortune for price certainty. Even so, scammers are calling people saying they are from a well-known price comparison site that's offering a special offer for a limited number of customers. They'll stress that you must switch now to secure the deal.

- **What you can do**: Unless you've requested a call back, a price comparison site shouldn't cold call you. Never hand over any of your personal details if you receive a call like this, and refuse to engage in conversation.

Green home improvement grants scam: Scammers have been known to impersonate government schemes that offer energy-efficient grants and initiatives, such as the Green Homes Grant from 2020 to 2021. Be very wary of tradesmen claiming to install such measures, and wanting your personal details.

- **What you can do**: Don't sign up to anything off the back of a cold call or approach from a tradesman. Look into legitimate schemes, do your research, and get several quotes. You can use Which? Trusted Traders, for example, to find trustworthy tradesmen nearby.

NIFC COMMUNITY AWARENESS UPDATE

HOLIDAY SCAMS:

Holiday booking scams: Fraudsters set up fake websites or holiday adverts with the aim of stealing your money, and in some cases holidaymakers turn up to find the accommodation doesn't actually exist. Fake accommodation deals often pop up on social media and rental websites. They may offer, for example, a chunky discount on a beautiful holiday villa or country cottage, but you can only secure the property by paying a deposit through a money transfer service. Alternatively, you may be asked to pay the owner a deposit by bank transfer.

- **What you can do:** Avoid paying using a currency transfer service to pay for a holiday, as this is very likely to be a scam. If you're paying a deposit, use a credit card to get protection under Section 75 against a fraudulent holiday booking. But before booking, check online for other reviews that don't appear on the website, and that there are legitimate contact details for the property's owner or company.

Clone holiday booking websites: Fraudsters clone legitimate holiday booking websites and take your money and/or payment details. For example, scammers have been known to clone popular booking sites Airbnb (the official site is www.airbnb.co.uk) and Booking.com.

- **What you can do:** Check the website address carefully to make sure it's the official one, and avoid clicking on links that are sent in emails or text messages. If in doubt, type in the official website address yourself.

Fake cancellation refunds: A flight or hotel booking cancellation can ruin your holiday plans, and unfortunately, fraudsters are using these scenarios as an opportunity to offer fake refunds. For example, they may send fake emails asking you to provide your payment details to secure a refund, or call you claiming to be able to do this over the phone. Scammers are also creating fake social media accounts offering to help you with a claim or refund for a cancellation.

- **What you can do:** Never be pressured to hand over your details, and if you are at all concerned, don't proceed at all until you've checked out the firm involved. Don't click on links or emails and contact the holiday booking company or airline directly.

Investment/ financial scams - Always be very wary if you're contacted about a financial opportunity or investment that looks too good to be true – here are some to look out for.

Fake WASPI compensation claim forms: The Women Against State Pension Inequality (WASPI) campaign has warned women not to be taken in by fake compensation claim forms which are being posted online by scammers trying to steal personal information. The Parliamentary Ombudsman in March said that the government should compensate women for not adequately informing them their state pension age would be increased, but it has yet to respond to the report. The fraudulent forms incorrectly state women affected by state pension delays can claim up to £2,950, when in fact no such amount has been confirmed.

- **What you can do:** Any form promising compensation to WASPI women is a scam, as compensation levels have not yet been confirmed. If you've already completed and submitted one of these forms, or received one, report it to the national fraud reporting centre Action Fraud and notify your bank immediately if you've handed over your bank details.

Scam HMRC text message promising cash: One scam text message claims to be from HMRC and says the taxman is issuing you with a tax refund. It then asks you to tap a link so that you can claim the payment. To do this, you must enter your banking details, which are then used to steal money from you.

- **What you can do:** Never click on any link, even if it looks authentic, or give out your bank details if requested by an email or text message. Instead, contact the organisation involved directly and see whether they have contacted you. You can report suspected phishing or spam texts to your mobile network provider by forwarding them to 7726 (these are the numbers on your telephone keypad that spell out the word 'SPAM'). Make sure you've installed the latest software and app updates to protect your devices from the latest threats too.

'Suspicious activity on your account' scam: You get a call or text message from someone pretending to be from your bank telling you there's been some suspicious activity on your account, which they will tell you has been frozen. They will ask for your banking details supposedly to confirm your identity and resolve the problem, but use these to steal from you. They may also try to direct you to a fake website to enter your information there. Often the number that appears on your phone looks legitimate, with scammers using technology to mask their actual phone number. In November 2022, the UK's biggest-ever fraud sting brought down a phone number spoofing site called ispoof.cc, which was responsible for selling this technology. Thousands of people called by criminals who used the site may be contacted by the Metropolitan Police and asked to contact the force to talk about their experiences, with fears that up to £48m might have been stolen.

- **What you can do:** Banks will never ask you for your PIN number or your online banking passwords, nor will they ask you to email or text your banking details, so hang up immediately if someone asks you for this information. If you want to check whether it really is your bank contacting you, end the call and telephone your bank from another phone number, as sometimes scammers will stay on the line, so that when you redial what you think is your bank, they reconnect with you. If they direct you to a website to enter your details, look at the link carefully and see if it looks vague or suspicious. If in any doubt, contact your bank directly and ask them to confirm.

'Payment attempted' scam: You receive a text message or call supposedly from your bank telling you that a payment was attempted from your account to a new payee. The message says that if it wasn't you, you should click on the link shown. This will take you to a fake website where you'll be asked to confirm your banking details. This information will be used to steal money from your bank account.

- **What you can do:** Never click on any link that is texted to you without first checking directly with your bank whether it's authentic, and remember that your bank won't ever get in touch asking for your bank details or passwords. Forward any suspicious or unsolicited texts to your network operator on 7726, so you'll no longer receive texts from that number.

NIFC COMMUNITY AWARENESS UPDATE

Ghost broking scam: You receive an email inviting you to buy car insurance, or spot an advert for competitive cover posted on social media, from a well-known insurance brand. Scammers will either forge insurance documents to persuade you the cover is genuine, or they will actually take out a real policy for you but then cancel it straight afterwards, pocketing your premium. Victims often don't realise they are without cover until they need to make a claim or are stopped by the police.

- **What you can do:** If you're offered an insurance deal that seems too good to be true, then it probably is and you should steer clear. If you are not sure whether the broker is legitimate or not, check on the Financial Conduct Authority or the British Insurance Brokers' Association website for a list of all authorised insurance brokers. If in doubt, you can also get in touch with the insurance company directly to verify the broker's details. If you think that you have been a victim of a ghost broker, you can report your concerns to Action Fraud at actionfraud.police.uk or on 0300 123 2040.

Pension review scam: You're contacted and offered a free pension review. This may be via text, email or you could spot a fake online advert. If you provide your details, you may receive a call or visit from a fraudster claiming to offer financial advice, who will recommend that you move your money into another scheme, or fake investments.

- **What you can do:** If someone contact you offering a pension review, ignore their approach. Keep your pension information to yourself, and don't share details with anyone you don't know. If you're aged 50 or over, you can also speak with Pension Wise on the phone, another government supported resource who offer free and impartial guidance about your pension options.

Early access to your pension: Scammers tell you that you're free to access your retirement savings before the age of 55, but if you do this, you'll not only have to pay a hefty tax charge, at least 55% but sometimes as much as 70% of your pension pot, but you'll also have fees taken from your pension for the transfer, which can be 20% or more of your pension savings.

- **What you can do:** Remember that 55 is the earliest age you can take your pension benefits. If you have a regulated financial adviser, speak with them in the first instance if you need help with your pension or are wondering if you should access your retirement savings. If you don't have an adviser, the government-supported Pensions Advisory Service provides free independent and impartial information and guidance.

Loan fee fraud: Loan fee fraud is an increasingly common scam which is reported to the Financial Conduct Authority (FCA), with people losing £220 each on average. The 'loan provider' will tell you that your loan is approved and then ask you to pay an upfront fee before the loan amount can be released. They then take the payment but never provide you with the loan.

- **What you can do:** Always be wary of unsolicited approaches about loans and don't click on links offering them. It's also highly unusual to be asked to make a payment to a lender, before you've been given a loan. If you're considering taking out a loan from a company you've never heard of, check the FCA Register to see if the company you're dealing with is authorised and stay well clear if it's not.

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

'Get rich quick' schemes: You'll usually be cold-called or receive a letter promising generous returns from supposedly lucrative investments, such as diamonds or forestry. The golden rule with investing is that if it looks too good to be true, it almost certainly is, so steer clear of anyone promising you'll be able to get rich quick. If you're considering investing in anything, always take your time to verify and validate the investment and remember that legitimate organisations won't push you into making a decision – the financial services regulator doesn't allow them to.

- **What you can do:** Check the FCA Register to see if the company you're dealing with is regulated. If not, they may be on the FCA's Warning List of companies offering investment opportunities which are a scam. If the company is on this list, or you suspect they are trying to scam you, you should report it to Action Fraud either online or by calling 0300 123 2040.

Broadband and mobile deal scams: You may receive a call claiming to be from your mobile or broadband provider offering you an unexpected discount or deal. They might ask for your bank details, or your account information, claiming this is a normal part of the process. Remember that most providers won't get in touch with you this way, and they certainly won't ask you for sensitive information over the phone.

- **What you can do:** If you receive a call like this, hang up and contact your provider independently to report it.

Charitable donation scams and fake Ukraine fundraisers: Action Fraud received around 200 reports of fake requests to fundraise for victims of the Ukraine war, according to latest figures. Scammers attempt to con unsuspecting donors by wearing charity T-shirts, and fake stories about their families and victims. The run up to Christmas is also a prime time for criminals to attempt to pocket donations.

- **What you can do:** Never click on the links or attachments in suspicious emails or respond to messages which ask for your personal or financial details. You can find out if a charity is registered with the Fundraising Regulator here and you can check the charity's name and registration number at Gov.uk.

Loved one in need scam: You'll receive a WhatsApp message supposedly from a family member, saying that they've got a new phone number and need money to pay a bill urgently. Messages often start with 'Hello mum' or 'Hello dad'. They will then provide bank details for you to transfer money across to them. If you're contacted out of the blue from a number you don't recognise but the person is claiming to be someone you know and are requesting financial assistance – stop and think as it could protect you and your money. These messages may appear genuine but your money could end up in the pockets of a criminal, so it's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

- **What you can do**: If you're suspicious about a request for help you've received from a friend or family member, try and reach out to the person directly by another form of communication to confirm that their request for help is genuine. If you find out it is a scam, you should report it to Action Fraud either online or by calling 0300 123 2040.

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

Unpaid fines: Growing numbers of people are reporting scam calls that appear to be coming from numbers similar to their own. Commonly, the first seven digits (07nnnnn) match the victim's own number. The calls impersonate well-known government organisations, or law enforcement agencies, and will ask the recipient of the call to "press 1" in order to speak with an advisor, or police officer, about unpaid fines or police warrants. In May 2021, Action Fraud received 2,110 scam call reports where the caller's number matched the first seven digits of the victim's own phone number. Of these, 1,426 (68%) referred to HMRC or National Insurance.

- **What you can do:** Never agree to pay a supposed fine over the phone, as government and law enforcement agencies will not notify you about unpaid fines or outstanding police warrants by calling or texting you. If you receive a suspicious text message, you can report it by forwarding the message to 7726, and suspicious telephone/mobile calls can be reported to Action Fraud via actionfraud.police.uk/report-phishing.

Ticket fraud: Ticket fraud involves scammers advertising tickets to popular events such as concerts and plays, often on social media. Once you've paid for the tickets, they never materialise and the scammer blocks you from making further contact. A spokesman for Action Fraud said; "One victim lost £200 after posting on Twitter asking if anyone had tickets for sale for a concert. The victim was messaged by someone who claimed they had a number of tickets for sale and the suspect claimed they would transfer the tickets to the victim as soon as payment was received. The victim sent the payment via PayPal and once the suspect had received the payment, they blocked the victim. "Another victim lost almost £250 after joining a Facebook group where they saw someone selling two VIP tickets to a festival. The victim contacted the person selling the tickets and was informed that they only accepted payment a digital wallet provider. The suspect claimed they would transfer the tickets to the victim as soon as payment was received, but went on to block the victim and continued to advertise the tickets on the same group."

- **What can you do:** You should only ever buy tickets from the venue's box office, official promoter or agent, or a legitimate and well-known ticket site. Never purchase them from someone you don't know by bank transfer. If you think you've fallen victim to a ticket fraud, contact your bank immediately and see if they can stop your payment and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

Shopping and postal scams - If you shop regularly online, always check that your payment details are kept safe and be suspicious of any offer which seems an incredible bargain. Here are some of the shopping and postal scams to watch out for.

Fake websites: Unfortunately there are always plenty of fraudsters operating fake shopping websites designed to part you from your cash, so make sure you're on your guard when buying online. These sites try to pass themselves off as the real thing, so you'll order and pay for items which then never arrive. You should only ever buy from websites with 'https' preceding the website address, as this means the site is a secure connection. If it's a retailer you haven't heard of, check customer reviews on sites such as Trustpilot to get an idea of whether they are reputable and trustworthy. You should also make sure you choose strong passwords for any shopping site where you're signing up for an account or providing credit card details. Ideally you should choose a combination of upper and lower case letter, numbers and special characters and make sure you choose a different password for each account you set up. Using different passwords for each account means that if one retailer suffers a data breach and usernames and passwords fall into fraudsters hands, your passwords with other websites remain safe.

- **What you can do:** If you're not sure whether a website is real or fake, get in touch with the retailer directly and check you've got the right URL. If you think you've fallen victim to an online shopping fraud, get in touch with your bank immediately and see if they can stop your transaction. If you have been defrauded or experienced cyber-crime you should report it to Action Fraud either online or by calling 0300 123 2040 so they can monitor reports of fraud and act quickly to stop it.

DPD scam: Recently there's been a spate of scam text messages and emails sent out, purporting to be from delivery company DPD. The message says something along the lines that you've missed a delivery, or an additional fee is payable if you want the parcel to be delivered. You're then directed to a fraudulent site which requests personal information such as your address or payment details. DPD says that fake or scam emails are nearly always sent from a private email address and not from an official DPD one. Often they are forged and look different from a dpd.co.uk, dpdlocal.co.uk or dpdgroup.co.uk address. If you're in doubt, don't click on any suspicious links and check whether you're actually expecting a parcel.

- **What you can do:** If you think you've received a fraudulent message which is pretending to be from DPD, you can report it at report@phishing.gov.uk.

Amazon scam: Watch out for fake automated phone calls claiming to be from Amazon, telling customers their Prime subscription is due to expire, and that payment will be automatically taken from their account to renew it. The recorded message then asks you to press one to cancel or two to speak to customer services. The call then goes through to an individual who 'requires' your personal details to access your account and will use this information to take money from your account. There are a number of variations on this scam being reported, including for example an automated fake call from Amazon saying 'your £500 Iphone is being shipped, please press one to cancel or two to speak to customer services'.

- **What you can do:** If you receive an automated voice recording pretending to be from Amazon, simply hang up and report it both to Action Fraud and Amazon.

Royal mail scams: There are several Royal Mail scams doing the rounds at the moment, so be on your guard if you receive an email, text message or call claiming to be Royal Mail which you think might be fraudulent. These will often state that a delivery was attempted which needs to be rescheduled and asks you to click on a 'bit.ly' link, which takes you to a scam site asking for payment. Alternatively, you might receive a message saying that postage has been underpaid, and your package will only be delivered once you've paid the required postage.

- **What you can do:** If you receive a suspicious email, text message or telephone call which you think is fraudulent, please report it to reportascam@royalmail.com. Don't click on any links or attachments and then delete it from your inbox. If you have clicked on a link and provided any personal data like your bank account details on a website or over the phone, or you're concerned that you've been compromised, you should report the scam to Action Fraud and notify your bank immediately.

NIFC COMMUNITY AWARENESS UPDATE

Coupon scams: Most of us are looking to save money as the cost of living soars. However, if you receive links for coupons or special deals via a text message or WhatsApp, be wary. These may be discounts off money spent at your favourite retailers, or supermarkets, but are really attempting to access your accounts and personal information.

- **What you can do**: Think twice before clicking on any links without verifying they are a legitimate offer. Scam links can lead to malware or other issues that may try to access your accounts, and cause problems with your mobile phone. Don't open any links on WhatsApp from people you don't know, or click on any links in text messages. Remember that anyone can message you if they have your number, which makes this route a popular one with scammers.

Job-related scams: Scams against job seekers are becoming increasingly common, and as with most scams, the fraudsters can often appear highly credible. They may put pressure on you to act quickly or pretend they know who you are and that they've found the perfect job opportunity for you. There are several types of employment fraud out there, but here are three common scams to be aware of:

- Fake job offers, advising you that you need to pay for security checks, online training, visas or insurance upfront
- Requests for you to call a premium rate phone number for an interview, racking up hundreds of pounds of call charges when there is no interview, or vacancy
- Work-from-home scams, which essentially con you into money laundering.

You should never pay any money up-front, or call a company for an interview. If it doesn't feel right, the chances are it isn't.

- **What you can do:** To find out more about employment scams or to report a scam, visit the website Safer Jobs, a non-profit organisation created by the Metropolitan Police to raise awareness of, and to combat job and employment- related fraud.

Computer service software fraud: Victims of computer service software fraud typically receive a call from a well-known broadband provider, who claims there is an issue with their service which they are going to resolve. The caller talks you through the supposed problem and asks you to log on to your computer or mobile and connect via a Remote Access Tool, which means they can then access your device. Some reports also state that fraudsters have been using browser pop-up windows to make contact with victims. You're then either persuaded to log into their online banking to make a payment for the service you've supposedly received, or you're told you need to log in so you can receive a refund from the broadband provider as a form of compensation. This enables the scammer to then transfer money from your account.

- **What you can do:** You should never install any software, or provide anyone who has cold-called you with remote access to your computer. If you've already done this, seek technical support to remove any unwanted software. If you need tech advice, look for reviews online first or ask friends for recommendations. If you think you've been a victim of fraud, report it to Action Fraud.

Romance scams: Romance fraud, as the name suggests, is a type of scam where fraudsters develop fake romantic relationships with people, both online and in person, with the aim of either stealing their money or personal information. According to UK Finance, the first half of 2023 saw a 29% increase in romance scams, with about £18.5m lost this way. Romance fraudsters may spend weeks, months, or even years, wooing an unsuspecting victim and convincing them they are in a real relationship. Once they've gained the trust of their victim, the fraudster will create a scenario where they need a large sum of money, for example, they might claim they need to pay for medical treatment or to travel to see an unwell relative and will use their relationship along with manipulative and coercive language to pressure them into giving them cash.

- **What you can do:** If you match with a scammer online, one of the most common things they are likely to do is ask you to take your conversations off the site and talk via text, WhatsApp or phone call, so there isn't a trace of them asking for money on the site, so keep your conversations on site if possible. If someone asks you for money or personal information on a dating site, you should let the platform immediately so they can prevent the fraudster from targeting anyone else.

Who to contact if you're a victim of fraud:

Contact your bank immediately if you think you've fallen for a scam.

If you have been defrauded or experienced cyber-crime you must report it to Action Fraud either online or by calling 0300 123 2040.
You should also report what's happened to the Financial Conduct Authority either online or by telephoning 0800 111 6768.

CRIME PREVENTION:

Beware of pickpockets:

The one thing you will not be at a Christmas Market is… alone; and this is the perfect scenario for pickpockets to operate. Crowds going in various directions – pushing, shoving, distracted by stallholders and vendors…

Keep your wallet and valuables close to you at all times. Pickpockets may try to distract you or physically bump into you, especially in crowded places. If you realise you have been pickpocketed, shout out to warn others.

You can review a wide range of Crime Prevention tips via:

https://www.cambs.police.uk/cp/crime-prevention/

NIFC COMMUNITY AWARENESS UPDATE

STAY ALERT, STAY ALIVE:

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!

…and don't forget basic crime prevention:

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