# NIFC COMMUNITY AWARENESS UPDATE

**NIFC COMMUNITY AWARENESS UPDATE 9/24 (22 Aug 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:***

- **FIVE (5) THINGS A SCAMS EXPERT WOULD NEVER DO.**
- **CAR PARK PAYMENT SCAMS ON THE RISE WITH FAKE QR CODES.**
- **DELAYS TO EU TIMELINE FOR NEW BORDER CONTROLS (EES and ETIAS).**
- **ONGOING SCAMS.**
- **PICKPOCKETS ON THE LONDON UNDERGROUND.**
- **CRIME PREVENTION.**
- **STAY ALERT, STAY ALIVE.**

## FIVE (5) THINGS A SCAMS EXPERT WOULD NEVER DO:

**Although nobody is immune to being scammed, no matter how intelligent, educated or financially literate they are, scam experts should have a better understanding but they acknowledge that scammers' methods constantly evolve to find new and nefarious ways to con their victims. Scam experts adopt some red lines – things they will just never do if asked – not without checking first.**

**Never buy from Facebook Marketplace without first inspecting the item in person.**

- In a cost of living crisis, buying second-hand furniture, clothes and children's toys can be a more affordable and sustainable option than buying new.
- Facebook Marketplace hosts listings for huge numbers of items, and normally the seller is local to you.
- The most common way to do business is to pick up from the seller's home and pay in cash on the doorstep. Doing it this way reduces the likelihood of being scammed.

**Never pay a stranger using bank transfer or PayPal's Friends and Family payments.**

- While a PayPal Friends and Family payment may save you a few pounds in fees, it means you have no recourse to PayPal's Buyer Protection scheme if the seller doesn't provide the goods.
- The same goes for bank transfers, which also lack protection. While there are some protections in place for scam victims who lose money through a bank transfer, getting your money back can be tricky.
- Scam victims who lose money this way often send funds, only for the recipient to break off all contact and block them.

**Never buy an unregulated investment.**

- The world is awash with exotic investment options – Scotch whisky casks, fine art, soybean futures and tropical island developments, to name a few. And of course, there's crypto.

- To the novice investor, the above might seem more exciting than the traditional options of buying stocks, shares and physical gold – particularly if the slick website or handout is promising you huge, inflation-beating returns.

But these types of investments are unregulated by the Financial Conduct Authority, meaning you have no recourse to the Financial Ombudsman Service if you're mis-sold.

And while some of these schemes are genuine (albeit very high risk), many are outright scams. That's why you should give them a wide berth and why the experts recommend any inexperienced investor to do the same.

No investment is completely without risk. However, it's far safer to take advice from a registered, authorised financial advisor and buy investments from a regulated firm, while physical gold should be bought from specialist bullion dealers with a well-established reputation, such as the Royal Mint.

**Never trust a call from the 'Fraud Department'.**

- If your bank detects a suspicious transaction on your account, it will freeze that transaction – and often the whole account – while it investigates the situation with you.
- Typically you'll receive a text message asking you to call the bank yourself. As long as you use the trusted phone number from your bank card or statement, this is safe.
- What isn't safe is answering a call from a human who claims to be from your bank's fraud team and then grills you for personal information or a one-time passcode.
- These calls come from scammers and you shouldn't hand over any details.
- Instead, hang up and spend a few minutes taking deep breaths to relieve any panic or stress, then use a different phone to call my bank using a trusted number to report what had happened.

**Never assume a loved one's cash request is genuine.**

- The now infamous 'Hi mum/dad' scam typically involves a WhatsApp message claiming to be from the new number of your adult son or daughter. 'They' quickly go on to request cash from you.
- This version of the con is easy to spot if you don't have an adult child. But if the message comes from, say, the genuine email address or Facebook profile of a friend, relative or even a colleague, would you spot it so readily?
- Your first instinct may be to help immediately and without question. But it's commonplace for social media and email accounts to be hacked by criminals who then bombard the victim's contacts with messages containing sob stories and pleas for financial help.
- The request may be for a bank transfer (to an account under a different name than your genuine loved one) or it may be for payment in gift cards.

That's why you should never send money or voucher codes on the strength of one of these messages. Always speak to the person to check the contents of the message, either face to face or by calling them on a trusted phone number that you have used before.

Not only could this save you from being scammed, it could also alert the person that they've been hacked, so they can take steps to recover the account.

## CAR PARK PAYMENT SCAMS ON THE RISE WITH FAKE QR CODES:

# NIFC COMMUNITY AWARENESS UPDATE

**Criminals are stealing money and personal data through 'quishing'; is there something suspicious about the QR code you are scanning?**

Fake QR codes are appearing on parking machines in UK car parks, allowing criminals to steal personal data and money. As digital payments for such things as car parking continue to grow, so do the opportunities for scammers to take advantage. Called 'quishing,' the scam directs victims to a fraudulent website where they are tricked into entering their payment card details, potentially costing them hundreds of pounds.

**Top tips to help drivers spot these fake QR codes and avoid falling victim to the swindle:**

**Inspect the QR code closely:** Before scanning a QR code on a parking meter, it is essential to check that it has not been tampered with in any way. Look for peeling edges, unusual bumps in the material, and anything else that generally looks suspicious. If the corners of the code are peeling and you can see another code underneath, this can indicate that a fake code has been stuck over the original one. If the QR code is printed on paper, is unusually large, and covers all or part of the text on the parking meter, this is a tell-tale sign that it isn't legitimate. Scammers will often inflate the size of the QR code to make it more visually obvious, to encourage customers to scan it.

**Does the URL look genuine?:** When you scan a QR code, your phone allows you to preview the website's link before you click to visit the site. Use your judgment to assess the website URL and whether it matches up with the parking company's actual website. Some scammers will set up a copycat website using a domain name that looks similar but is slightly different from the real thing. Make sure that the website you are visiting on your mobile browser has a padlock symbol next to it and that the URL begins with 'https://' rather than just 'http://'. This ensures that the website is encrypted with a Secure Sockets Layer (SSL) certificate. Some phishing websites now also use SSL protection in an attempt to trick visitors, so this is a risk that should be taken into consideration when visiting the site.

**Suspicious website content:** If you click through to a parking service website with a QR code and the webpage content looks unusual or things feel out of place, this can be a sign you are not booking parking through the legitimate site. Some phishing websites can look quite sophisticated but there are some signs you can watch out for, such as spelling mistakes, lack of correct capitalisation, text being misaligned, and logos and graphics appearing pixelated or out of date.

**Personal information requests:** When paying online, parking services are likely to require your vehicle registration, your email address to confirm your booking, your card number, its expiry date, and the last three digits on the back of your card (CVV/CVC). If the site asks for additional information, such as your home address, phone number, or even your card's PIN number, this can be a sign that it isn't legitimate.

**Dedicated parking apps are best:** Popular parking services such as JustPark, Ringo and PayByPhone have their own dedicated app, which you can download directly from the Apple or Google Play store. Once you have the app downloaded, scanning the QR code should redirect you to the app to start your booking. If it doesn't, and you are directed to a site in your browser, it is likely that you could be dealing with a phishing website.

**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**

Alternatively, the car park should have a location code, which you can enter directly into the app if unsure about the QR code's legitimacy.

According to National Trading Standards, around 73% of UK adults have been targeted by scams, and 35% of people have fallen victim to the offence. With scams becoming ever more convincing, even the most technologically savvy among you remain at risk.

## DELAYS TO EU TIMELINE FOR NEW BORDER CONTROLS (EES and ETIAS):

**The latest update indicates that the EU's post-Brexit Entry/Exit System (EES) will launch on 10 Nov 24.**

The EES was first slated to launch in 2022 but has faced multiple setbacks due to IT issues and delays in installing the automated barriers required at all international land, maritime and air borders in the Schengen Area. When it becomes operational in autumn, non-EU travellers entering the Schengen Area will face new border controls.

The EES has two aims:

- To automate checks on entering and leaving the Schengen Area, which will detect overstaying.
- To enhance border security by registering fingerprints and facial biometrics of all third-country nationals crossing legally.

### Which travellers will need to use the EES?

- The Entry/Exit System will be an automated registration system for UK and other non-EU travellers who don't require a visa to enter the EU. Travellers will need to scan their passports or other travel document at a self-service kiosk each time they cross an EU external border. It will not apply to legal EU citizens or residents or those with long-stay visas. It will apply when entering all EU member states, apart from Cyprus and Ireland, as well as four non-EU countries in the Schengen Area: Iceland, Lichtenstein, Norway and Switzerland.
- The EES is being introduced to bolster border security and identify travellers who overstay their permitted time in the Schengen Area (90 days within a 180 day period).

### Will the EES cause travel delays?

- In the UK and elsewhere, there are concerns that the EES could increase delays at border checkpoints.
- French authorities will operate EES border checks at the UK's Port of Dover, Eurostar and Eurotunnel. They are currently working with the UK government to minimise the system's impact on border flows and traffic, but express concern about potential waiting times.
- Government agencies and representatives for the tourism industry have said that the EES will likely cause long queues for ferry traffic sailing from Dover to Calais.
- The scheme will have a "six-month soft launch" to make the process more simple. If the situation gets to a point where significant queues or delays are experienced, then there are provisions for precautionary flexibility measures to allow for much greater freedom of passage of vehicles, coaches, HGVs and cars.

# NIFC COMMUNITY AWARENESS UPDATE

**Is Electronic Travel Information and Authorisation System (ETIAS) still on track?**

- Roughly six months after the launch of the EES will see the introduction of the European Travel Information and Authorisation System (ETIAS). This new scheme obligates non-EU citizens who do not require an EU visa to gain travel authorisation to enter the bloc (as opposed to the EES which is a monitoring system of border crossings by third-country nationals). The visa waiver will be mandatory for anyone wishing to visit the Schengen Area short term.
- ETIAS was originally set to be operational from November 2023. However, the European Commission now states that it will come into force in 2025. While an exact date is not provided, the EU has previously indicated that it will be introduced five to six months after EES. There may be an implementation period where it is gradually introduced alongside the Entry/Exit System.
- Travellers will be able to apply for ETIAS online before their trip at a cost of €7. Once approved, the electronic travel authorisation will be electronically linked to their passport and will last for three years.

**ONGOING SCAMS:**

**Card fraud**:

- Losses of £551.3million in 2023.
- Card fraud covers loads of things, including spending on lost or stolen cards, cards that get stolen before you receive them, fake and counterfeit cards and remote purchase fraud (where fraudsters steal your card details and use them to shop online, on the phone or through mail order).
- There's also card ID theft, where fraudsters use data harvested online or through hacking to either apply for a card using your details, or to take over your account after finding a way to break in to it.
- Finally, there are the face-to-face scams. This is where scammers "shoulder surf" to spot your pin, then steal your card. Alternatively there is the "Lebanese loop" or "card entrapment" scam, where a fake ATM cover is attached over a genuine machine, allowing them to steal the card.

**Unauthorised remote banking fraud:**

- Losses of £151.8million in 2023
- Remote banking simply means financial services that you don't have to be physically present to use. These are: internet, telephone and mobile banking services. Remote banking fraud exists in a wide range of formats, but mainly refers to attempts by scammers to get their hands on your log in details or accounts by tricking you in to handing the information over.

**Other scams:**

- It's not just the method of fraud that matters, sometimes it's the different categories of scam that you need to watch out for. These include:
  - Romance scams. Where fraudsters pretend to be a potential partner to get you to send money.
  - Investment scams. Where you are cold-called and pressure sold a ropey or non-existent form of high-risk investment, from cryptocurrency to investing in land abroad.
  - Advance fee scams. Where you are persuaded to pay a fee to gain access to a much bigger sum of money or goods.
  - Invoice or conveyance scams. Where people are tricked in to handing over sums of money after the fraudster hacks and email or website and changes the payment details for invoice payments. Sadly, there are many, many other scams to watch out for.

**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

## PICKPOCKETS ON THE LONDON UNDERGROUND:

Pickpocket thefts on the London Underground remains an issue, with the Central line being one of the worst hit across the network.

Today, statistics indicate that train-related theft is at a higher rate than pre-pandemic levels - on trains, platforms and at station entrances and exits – moving swathes of people; people in a hurry; people pressing up against other people, etc.

The Westminster area is a favourite spot of pickpockets – central point for tourists.

Pickpocketing covers theft of items directly from the victim, but without the use of physical force and so easily accessible items like mobile phones and wallets tend to be the most targeted. Keep an eye on your bags and any other valuables and be vigilant around other passengers.

It's also important that victims and witnesses contact the police as soon as the robbery occurs. The first hour after the incident takes place can be critical to catching the suspect.

Statistically, you would be unlucky to be caught-up in a criminal act but it could happen and it will ruin your visit, day, week……..; if it does happen, report the incident without delay, and cancel any cards, etc., if they have been stolen.

Here are some additional tips from the Metropolitan Police to help avoid being a victim of pickpocket theft.
- Carry bags in front of you or diagonally across your chest
- Return cards to your purse or wallet quickly and zip it up or button it before concealing it
- Use a purse that's difficult to open. One that zips or snaps shut is best
- Use a money belt if you're carrying a significant quantity of cash
- Keep a list, separate from your wallet and phone, of contact numbers, in case your phone is stolen
- Keep a photocopy of your airline tickets, passport, credit cards and any other documents that would be impossible or inconvenient to replace if stolen

## CRIME PREVENTION:

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

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

## STAY ALERT, STAY ALIVE:

This summer has seen millions of people across the UK and Europe enjoying themselves at major events such as music festivals, sporting events (Euros, Olympics), bank holidays, etc.

Unfortunately, whilst trying to keep it in perspective, the terror threat hasn't gone away. The threat to the UK from terrorism is SUBSTANTIAL, meaning an attack is likely. We know that the large audience participation events and venues could be attractive targets for terrorist activity. That's why UK Counter

# NIFC COMMUNITY AWARENESS UPDATE

Terrorism Policing collaborates with event organisers and businesses across the UK to help keep the public safe.

**You can play your part by promoting the campaign using the new toolkit launched today on ProtectUK**

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 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**