NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 6/24 (7 Jun 24)

(The Community Awareness Update provides general information to enable personnel to keep up-to-date with routine 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.

MOST CONVINCING SCAMS TODAY:

Hijacked holiday bookings:

- Weak hotel email and booking systems are being targeted by hackers to send troublingly plausible messages to holidaymakers. Once they've gained access to the systems of hotels and B&Bs, they're armed with guests' contact and booking details, and can send fake messages, texts or emails. The most dangerous appear in the 'secure' internal messaging platforms of genuine sites.

- Booking.com scams are one of the most reported, e.g. Action Fraud recorded 20 reports in 2023 and already recorded 40 reports in the first three months of 2024.

- Typically, messages claim there's a problem with your payment, before asking you to 'verify' or 'update' your card details on phishing sites designed to look like Booking.com.

Fake phone and broadband providers:

- Threatening calls and poorly written messages claiming to be from your phone or broadband provider are easily dismissed, but perfectly timed impersonation scams are more likely to slip through. You may be told you're owed a refund, offered new equipment to fix non-existent connection issues, or enticed with offers to upgrade your package, reduce bills or claim loyalty deals. A nasty trick is to ask you to share your screen, by downloading 'remote access' software.

- Bad luck can play a part, as you may be having genuine issues when scammers contact you. They might even have got information through hacking your emails. One victim said that a 'Sky' employee called to say they had booked an engineer due to a problem with their wi-fi, which had been playing up. The 'employee' said that he had checked the speeds via the PC, said it was slow and that a refund was due as they had been paying for a wi-fi boost for over a year. The 'employee' said a refund would be processed via an external app. Unfortunately, a genuine call from Sky the day before made it seem above board. The 'scammer' took £250 as gift cards from the credit card.'

NIFC COMMUNITY AWARENESS UPDATE

Fake ads and rip-off subscriptions:

- You might be bombarded by sneaky subscriptions hidden in misleading ads.
- We've heard from hundreds of people in the past year who discovered unwanted and often extortionate recurring payments.
- Some victims were paying as much as £50 a month to companies they had never heard of. Many have faced a battle to get a refund from their card provider, because payments appeared to be 'authorised'.
- One tactic is to place stickers of fake QR codes over genuine ones found in car parks, restaurants and posters. Malicious QR code scanner apps have also been blamed for directing users to scam advertising.
- Another ploy is to pay advertising platforms to target victims at scale, notably by impersonating parking apps such as JustPark, PayByPhone and RingGo. Which? has found repeat offenders on Google – despite it telling us that it had taken action.
- A Google spokesperson said: 'Protecting users is our top priority, and we have strict ads policies that govern the types of ads and advertisers we allow on our platforms. We enforce our policies vigorously, and if we find ads that are in violation, we remove them. We continue to invest significant resources to stop bad actors and we are constantly evaluating and updating our policies and improving our technology to keep our users safe.'

Your bank account drained in minutes

- Which? was the first to sound the alarm in March about e-money firm Revolut and account takeover fraud (when criminals hack into financial accounts to make unauthorised transfers).
- All the victims were experienced business owners, including one who lost £165,000 in an hour and another who lost £40,000 in 10 minutes. None has been reimbursed.
- The scammers created a fake email address and copycat webpage to impersonate Revolut. They were even able to pass 'selfie' security checks (a photo of the account holder).
- Then they contacted victims, claiming to be from the Revolut fraud department to obtain security codes. Once unleashed, the speed at which they drained the accounts is truly shocking.
- A spokesperson for Revolut said: 'We are aware of a recent increase in advanced account takeover scam attempts across the industry.' They added: 'We are continuously strengthening our fraud controls to stay one step ahead of this trend, introducing further direct interventions and sharing educational materials with our customers so they are able to spot the social engineering tactics of criminals.'

Investment fraud:

- Squeezed households are being drawn to bogus investments and 'get-rich-quick' schemes run by criminal gangs netting horrifyingly large amounts of money.
- Investment scammers stole an average of nearly £13m per week from almost 100,000 victims in 2020-23, according to data from Action Fraud. More victims came forward in 2023 than any other year.
- Too many people blame victims, calling them greedy or sloppy, yet Which? regularly comes across cleverly cloned websites claiming to be regulated companies, sometimes using glossy, professional-looking brochures making false claims about enticing rates and how your money is protected.

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

- Misleading profiles on LinkedIn and Companies House can also add an air of legitimacy.
- Sickeningly, victims are often retargeted by recovery scammers – sometimes claiming to be from legal firms, auditors and regulators – falsely promising to help recover their losses, for an upfront fee.

Ten (10) ways you can protect yourself from scams:

- Use expert tips to stop scammers from stealing your data and money.
- Never share your password, Pin or security codes, even if a caller or message claims to be from your bank or another trusted company.
- Have the most up-to-date security software on your phone and PC. See our expert pick of the best antivirus software.
- Only download apps from official Apple, Google Play or Amazon App stores.
- Ads on search engines have been used by scammers in the past, so pay close attention to the web address if you click on one.
- QR codes can also be used by scammers – pay close attention to the web address if you use one, and never use a QR code scanner app as it increases the risk of downloading malware. Instead, use your phone camera. Find out more about QR codes.
- Be suspicious of companies contacting you, even if they seem to know about you – this could be taken from your social media profiles or leaked data. Get in touch with the company using a trusted method to check it's genuine.
- Never pay for a holiday outside a trusted booking system; ideally, pay with a card to ensure you benefit from chargeback (debit and credit cards) or Section 75 protection (credit card only). Use our free tool to make a section 75 or chargeback claim.
- Ignore unexpected investment offers, whether that's via cold calls, ads, emails or through the post. These are likely to be scams.
- Avoid entering your details on social media sites and unknown sites, particularly those advertising on search engines. You risk being targeted with endless scams.
- Sign up to the free Which? scam alert emails to outsmart the fraudsters.

HOW TO GET YOUR MONEY BACK AFTER A SCAM:

Here's what you can do to try and recover your money if you've lost out to a scam.

How did you pay?

How you go about getting your money back, and how successful you're likely to be, will depend on how the money was paid.

Debit card:

- If you used a debit card, you may be able to ask your bank to get your money back through the chargeback scheme.
- Chargeback is not enshrined in law but is part of Scheme Rules, which participating banks subscribe to.
- It applies to all debit card transactions including goods costing less than £100, although exact rules may vary between the American Express, Maestro and Visa networks.
- But, there are no guarantees your bank will be able to recover the money through chargeback.

- Chargeback also applies to credit card transactions where goods cost less than £100, so section 75 doesn't apply.

Bank transfer:
- A bank transfer scam, also known as an authorised push payment (APP) scam, occurs when you - knowingly or unwittingly - transfer money from your own bank account to one belonging to a scammer.
- If you've been caught out by a complex and convincing scam which has resulted in you transferring your money into another bank account, then you should contact your bank immediately.
- Tell the bank what happened, and let it know the bank account number your money was sent to.
- The bank can try and recover the funds once it has been notified.
- If your bank is signed up to the voluntary Contingent Reimbursement Model (CRM) code, it has to take a number of steps to protect customers and reimburse blameless victims of APP scams.

Credit card:
- If you've paid for goods or services with a credit or debit card, you have greater protection if things go wrong under Section 75 of the Consumer Credit Act or by using chargeback.
- But whether you can make a claim or not depends on the type of scam you have fallen for.
- An example of a scam where you could use Section 75 or chargeback would be a scam where you paid for goods or services and it turned out these were either never available or the 'seller' disappeared.
- Credit cards have the greatest protection, as you can make a claim against your card provider under Section 75. Under Section 75, the credit card company is jointly and severally liable for any breach of contract or misrepresentation by the company.
- For Section 75 to apply the item or service you bought must have cost more than £100 and not more than £30,000.

Paypal:
- **Order not delivered**
  - If the scammer took payment for an item through PayPal but failed to send it, you should be covered by PayPal Buyer Protection. However, there are some exceptions and time limits on lodging a claim.
  - In some cases, scammers set up convincing fake PayPal payment forms which actually just gather your bank details.
- **Fake PayPal payment page**
  - This is when the scammer has used PayPal branding to make fraudulent activity look legitimate.
  - As PayPal isn't part of the transaction, you won't be able to claim your money back via PayPal Buyer Protection.
- **Seller protection**
  - Sellers can be scammed when a fraudster pays for an item via PayPal. The scammer may say that they didn't receive the item and make a claim through PayPal Buyer Protection or Section 75.
  - If you're caught out by this scam you'll probably want to make a claim under PayPal Seller Protection.
  - But this has conditions and requirements - particularly around the delivery address that's used and the seller having proof of delivery.
  - As long as you've met all of the criteria you should be protected.

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

- In some instances, the scammer will be aware of these rules and will specify a different delivery address or collect in person.
- In these scenarios, you wouldn't be covered by seller protection as you didn't meet the condition of posting the item to the account holder's registered address.

Cash, vouchers or gift cards:

- Unfortunately, it can be very difficult to get your cash back after a scam.
- This is also the case if the scam involved gift cards or vouchers. Make sure you never share the numbers on the back of gift cards or vouchers with people you don't know.
- Report the fraud to the police and Trading Standards to see if they can take any action.
- Talking to others about what's happened, and hearing about the experiences of others who have been through the same experience can help. You can get in touch with support groups through charities such as Citizen's Advice, Victim Support and Age UK.

Money transfer wire service:

- Unfortunately, it's not always possible to get your money back if you paid via a wire service such as MoneyGram, PayPoint or Western Union.
- All of these services provide advice on how to avoid fraud and scams, so it's a good idea to read their guidance to safeguard yourself against future scams.

I didn't authorise the payment:

- If there is a transaction on your card that you don't recognise, you can make a claim to your bank.
- If you've handed over your card to have a particular amount debited from it, and then you find more money has been taken without your permission, or a sum has been taken by someone else, you can make a claim for this additional amount.
- The Payment Services Regulations and the Banking Conduct of Business rules place obligations on banks and building societies to provide a refund in these circumstances.
- Make sure you report the unauthorised transaction as soon as you become aware of it.

STAY ALERT, STAY ALIVE:

This summer will see 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 summer events and venues could be attractive targets for terrorist activity. That's why UK Counter Terrorism Policing is collaborating with event organisers and businesses across the UK to help keep the public safe this summer. In France, the policing and security measures for the Olympics are second to none.

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.

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

- 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 summer campaign 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

NIFC COMMUNITY AWARENESS UPDATE

DRINK AND DRUG DRIVING SUMMER CAMPAIGNS

- The ‘summer’ campaigns by police forces are already in place in a bid to crack down on those who think they can drink or take drugs and drive and get away with it
- With hopes high for a long hot summer, drivers are reminded to enjoy the long evenings, but not to drink and drive.
- Police officers will be out in force during the campaign in a bid to crack down on those who think they can drink or take drugs and drive and get away with it.
- Summer is a time for socialising and having fun and this year will be no exception, particularly with some of the major sporting events taking place.
- The message is clear, have fun, drink if you want to, but don’t then get behind the wheel and drive. If you take that risk you will be caught.
- Drink and drug driving are serious offences and drivers should be in no doubt that if they are caught behind the wheel under the influence this summer they risk losing their licence as well as facing a fine and even a prison sentence.
- The number of drink driving deaths has fallen by more than 75% since 1979. But drink and drug driving still kills hundreds of people, that is why the police take tough action to tackle these reckless drivers.

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