NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 10/24 (4 Oct 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:

- **HARE COURSING**
- **ANTIVIRUS EMAIL SCAMS**
- **DO YOU KNOW WHO'S KNOCKING ON YOUR DOOR?**
- **COMMUNITY MEMBER CAUGHT OUT BY PARKING FINE SCAM**
- **FOUR WAYS ENERGY SCAMMERS COULD CON YOU:**
- **CRIME PREVENTION.**
- **STAY ALERT, STAY ALIVE.**

HARE COURSING:

There has been an increase in hare coursing following the recent wet weather. Hare coursing is the pursuit of hares with greyhounds and other sighthounds, which chase the hare by sight, not by scent.

Hare coursing is illegal in the United Kingdom.

If you see coursing, lamping or poaching in progress, it's a crime in action, so 999 it!

Where possible, please ensure you have the answers to the following questions:

- How many people and/or vehicles can be seen and what is their descriptions?
- Have any animals been seen to be pursued/chased or attempted to be pursued/chased?
- Are any people and/or vehicles believed to be trespassing on land?
- Why do you believe that these people and/or vehicles are involved coursing/lamping/poaching?
- Are the people and/or vehicles stationary or are they travelling? (Is there a What.Three.Words? What is the direction of travel?)
- Have any other offences believed to have been committed? (i.e. criminal damage to crops, dangerous driving, offensive weapons, public order)

Do NOT confront 'hare coursers' directly, call the police.

SCAM ALERT: ANTIVIRUS SCAM EMAILS TARGETING YOUR INBOX - IN RECENT WEEKS, SCAMMERS HAVE INCREASED EFFORTS TO TARGET INBOXES WITH DODGY EMAILS IMPERSONATING AVG ANTIVIRUS AND MCAFEE.

AVG Antivirus emails:

NIFC COMMUNITY AWARENESS UPDATE

- A dodgy email impersonating AVG AntiVirus. Emails claiming to be from AVG Antivirus tell you that your ‘AVG subscription has expired’ and that ‘you run the risk of viruses and malware.’ They also offer an 80% or 90% ‘renewal discount’ and give you a short deadline to claim this. You’re then prompted to scan a QR code or follow a dodgy link labelled ‘renew now.’ After following the link, you’re taken to the official AVG website.
- While this might seem strange, it means that the emails were most likely created and sent by a rogue affiliate. These are partner organisations that promote AVG’s products.
- AVG will only send emails from the AVG.com domain or, in some cases, GenDigital.com.

Emails impersonating McAfee:

- An email with an attached ‘invoice’ claiming to be from McAfee tells you that your purchase and registration of McAfee is complete and prompts you to review the ‘amended agreement.’
- The fake invoice begins ‘your payment to McAfee has been confirmed’ and asks you to call a number if you didn’t authorise the £799.99 fee.
- This number will put you through to a scammer who will try to get you to reveal your personal and financial details. They may also pressure you to download software to your device which will give them control of it.
- A second email impersonating McAfee tells you to ‘protect your device from dangerous threats’ with an ‘exclusive’ ‘90% discount’ on your McAfee renewal. It prompts you to follow a QR code or link to take advantage of this ‘deal’, but this leads back to AVG’s official website.

Spotting, reducing and reporting scam emails:

- If you receive an email you’re suspicious about, don’t click on any links in it or reply to the message. Instead, look out for these signs:
  - An unrecognisable or unusual sender's email address.
  - An impersonal greeting, such as ‘dear customer’.
  - Links that are different to the brand or organisation the email claims to be from - hover your cursor over the links to see where they lead.
  - Blurry or out-of-date branding.
  - Requests for personal information or bank details.
  - A tight deadline to take advantage of an offer.
  - Poor spelling, grammar and presentation.

- If you do receive an email from a company you have an account with, contact them directly on a trusted number or log into your online account to verify the information in the email.
- It may not be possible to stop every spam email, but when you receive a dodgy email in your inbox, you should mark it as 'spam'. Doing this should encourage more of these emails to divert straight to your junk folder.
- You can report email scams by forwarding the email to report@phishing.gov.uk, and suspicious websites can be reported to the National Cyber Security Centre.
- You can also report emails to your email provider - select the ‘report spam’ on Gmail, the ‘report phishing’ button on Hotmail and send scam emails to abuse@yahoo.com if you use a Yahoo account.
- You can report fraudulent messages and scams impersonating McAfee to scam@mcafee.com.

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

- 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.

DO YOU KNOW WHO'S KNOCKING ON YOUR DOOR?

Cambs Police were recently called by concerned bank staff in Wisbech who had a woman in her 70s come in asking to withdraw £7,500. After bank staff spoke to her more, she confided that builders doing work opposite her home had knocked on her door and said she needed some work doing to her chimney.

They had quoted her £5,000 for the work, but while completing it had noticed other 'problems' including a crack on the roof – and increased the price of their work by £2,500.

The elderly woman said the builders would return to her home that afternoon to collect the cash, and confided in bank staff that she was frightened and the money was nearly all of her savings.

Officers took the woman home and tried to contact the builders to no avail, but advised the woman not to pay. An investigation has been launched with Action Fraud.

Top marks to the bank staff for contacting the police after noticing things weren't right.

Remember - rogue traders often offer gardening work or maintenance services at attractive rates but the quality of work is substandard, unnecessary or overpriced. They also use persuasive sales techniques to encourage you into making hasty decisions.

Doorstep selling is not illegal, but legitimate callers won't mind if you ask them to come back later while you verify that they are genuine. Ask them to leave their details and a quote and you can call them back once you've had time to decide whether you would like them to carry out the work. Also ask to see their ID.

COMMUNITY MEMBER CAUGHT OUT BY PARKING FINE SCAM:

A community member was recently caught out by a parking fine scam. You are reminded that the Driver and Vehicle Standards Agency (DVSA) issued a warning about parking fine scam text messages about fake DVSA parking penalty charges.
The text messages warn people that they have a 'parking penalty charge', and that if they do not pay on time, that they might:

- Be banned from driving.

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

- Have to pay more.
- Be taken to court.

The text message reads: "*Dvsa notice for you: You have a parking penalty charge due on 2024/9/30. If you do not pay your fine on time, Your car may be banned from driving, you might haeve to pay more, or you could be taken to court. Please enter your license plate in the link after reading the information, Check and pay parcking penatly charge. Thank you again for your copperation. Dvsa."*

The initial text message has been followed up with scam reminders: *DVSA Fixed Penalty Office: Today is the last day to pay your ticket due to your long term delinquency, if you do not pay your ticket on time you may be required to pay more in the future and we reserve the right to prosecute you. Please be patient and open the link below to process your ticket. Thank you again for your co-operation.*

Another scam reminder says: *DVSA Fixed Penalty Office last notification: You have not paid your ticket within the stipulated time. Today is the last time to notify you to pay. We will ban your car from driving on the road starting tomorrow and transfer your parking ticket to the court. Please wait until you receive the information. Process your ticket as soon as possible in the link.*

Another scam message says: *EWHC notice for you: We are preparing to prosecute you for the materials handed over by DVSA. Because you have not pay your parking penalty charge for a long time. Today is the last day for payment. If you do not pay within today, we will prosecute you. Please read the information and enter your license plate to check your parking ticket.*

DVSA does not issue or deal with parking fines.

What to do if you received a message:
- You can report scam text messages to the National Cyber Security Centre.
- Report a scam text message.
- You do not need to contact DVSA if you have received the text message.

If you've responded to a scam text message:
- If you've been tricked into sharing personal information with a scammer, you can take immediate steps to protect yourself.
- Find out what to do if you think you've shared personal information.
- If you've lost money or have been hacked as a result of responding to a suspicious text message, report it via: www.actionfraud.police.uk or call 0300 123 2040 (in England, Wales or Northern Ireland)

FOUR WAYS ENERGY SCAMMERS COULD CON YOU:

Fraudsters are poised to capitalise on confusion surrounding winter fuel payments. Changes to our energy bills offer a prime opportunity for scammers to sow confusion – and this year is no different.

Changes like this can provide an easy cover story for scammers. Be extremely wary of calls, texts and emails claiming to be from your energy supplier, the government or Ofgem.

NIFC COMMUNITY AWARENESS UPDATE

If you're in any doubt, avoid clicking on links in messages and contact your supplier directly using the details on your bill – or go to Gov.uk for more info.

Read on to find out about the energy scams to be aware of amid stretched household budgets, and how to protect yourself.

Ofgem impostors:

- Brazen fraudsters have repeatedly posed as the energy regulator, Ofgem, to offer free boilers, cheaper tariffs, grants or energy efficiency upgrades.
- Victims typically receive a cold call, email, text or doorstep visit from someone claiming to represent the regulator and asking for bank details.
- In 2023, Ofgem identified an impostor website that it warned could have had 'disastrous implications for customers, if it hadn't been shut down quickly'.

Top tip - Never hand over your personal or bank details without stopping to think first about how to verify what you've been told using verified contact details. A genuine representative wouldn't mind you doing this. Contact the organisation they claim to be representing directly before you go any further.

Fake pre-payment offer:

- If you had a knock on your door from someone offering half-price energy on your prepayment meter, would you be tempted?

- Action Fraud has warned that gangs of criminals are cloning prepayment meter keys with, for example, £100 of credit on them, before selling them door to door for just £50. Sometimes the criminals even pose as energy company employees.

- This may seem like a good deal, but it can backfire spectacularly months – or even years – down the line. Eventually, your legitimate supplier realises you're not buying enough energy to be consistent with normal use, and investigates you.

- You may then find yourself paying again for the energy used – this time at full whack – so you end up paying more than if you'd paid the honest way.

Top tip - Never engage with or purchase any goods or services from doorstep salespeople, because you may struggle to locate them again and obtain a refund if you have problems with your purchase. Don't let anyone into your home unless you were already expecting them.

Solar scammers:

- Solar panels have become more common in the UK, although some households have had them in place for a decade or more. These systems require maintenance and repair and, in a few cases, the firms that originally installed them have stopped trading.

- Customers of those defunct firms have reportedly been approached out of the blue and offered a free check of their installation. This is often accompanied by a high-pressure attempt to sell a maintenance contract or a forceful suggestion that the system needs expensive repairs.

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

- If you are in this situation, ask the company how it got your contact details and confirm whether it has consent to contact you. If it's cold calling you and behaving disreputably from the outset, that's a major red flag.

- At best, services could be overpriced, with shoddy workmanship; at worst, a scammer could take your money and run.

- As with the purchase of the solar panel systems themselves, you should not feel pressured into signing a contract without having all the information you need to make the decision. Ideally, you should see clear calculations from the new company, demonstrating how their services will increase the benefit you get from your solar panels, set against its cost.

Top tip - Do your homework before signing up, obtain several quotes and check websites and reviews carefully. Read our advice on solar panel cold calls to watch out for.

Meter tampering:

- In June 2023, research from the insurer Direct Line revealed that 30% of electricians and gas engineers had spotted signs of meter tampering while on call-outs.

- Bypassing a meter or removing pipework might save a few pounds, but it can be exceptionally dangerous – not just for the perpetrator, but for unsuspecting neighbours.

- In 2021, toddler George Arthur Hinds died in a gas explosion at his family home in Heysham, near Morecambe, because the next-door neighbour had removed a length of gas pipe with an angle grinder to sell it for scrap, and had bypassed his gas meter to steal gas.

Top tip - If you suspect a meter has been tampered with, you can report it anonymously to Stay Energy Safe on 0800 023 2777. If you smell gas, open the doors and windows, turn off the gas (if you can do so safely), exit the property and call the National Gas Emergency Service on 0800 111 999. Calls to these numbers are free.

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 <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