



NIFC COMMUNITY AWARENESS UPDATE



NIFC COMMUNITY AWARENESS UPDATE 5/23 (20 Oct 23)

(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.

From ACTION FRAUD:

The internet's unequalled choice, 24/7 convenience and flexibility are benefits that suit people of all ages, wherever they live or work and whatever their circumstances. We've all either experienced at first hand or heard about negative experiences including online fraud or abuse which are, unfortunately, all too commonplace.

In order to go online with safety and confidence, it's important to get to know who and what you can trust ... and who and what you can't. And it's vital that everybody who uses the internet can do so with safety and confidence – regardless of gender, ability, appearance, background or beliefs – by being able to trust others' behaviour and behave responsibly themselves.

For more information about the internet and trust please read our latest advice here:

<https://www.getsafeonline.org/trust/>

Northants Police Reminders - Safety advice ahead of Halloween and Bonfire Night:

Links below contain safety advice ahead of Halloween and Bonfire Night. The seasonal Safety Newsletter is designed to help keep families safe across Northamptonshire (equally applicable to other areas) as they celebrate Halloween and Bonfire Night. We want you all to have lots of fun, but please don't forget about safety as you get swept along with the excitement of the season.

- [Be Bonfire Safe - NFRS.pdf](#)
- [Police and Fire Halloween & Bonfire Schools Newsletter 2023.pdf](#)

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



Received an email or text that seems suspicious? Report it. Your reports enable us to remove the emails and websites criminals use to commit fraud and cyber crime.

Forward suspicious emails to report@phishing.gov.uk . Send emails to this address that feel suspicious, even if you're not certain they're a scam - we can check.

Forward suspicious text messages to 7726 (it's free of charge). Your provider can find out where the text came from and block or ban the sender.

If you've lost money or provided personal information as a result of a phishing scam, notify your bank immediately and report it to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

Please note: Sometimes a forwarded email may not reach us because it is already recognised by spam detection services. You can also take a screenshot of the email and send it to report@phishing.gov.uk

Remember, scams are always evolving. Agencies need you to report scams so they can be prevented!

Wherever you are, whatever the situation....



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

Is it an emergency? Call 999

If it is 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



SCAMS

A recent survey by NatWest revealed that 74% of individuals have fallen prey to scams within the past year. The survey, which gathered insights from 2,000 participants across the UK in Sep 23 revealed some alarming statistics, highlighting the growing threat of digital and online scams. Among those surveyed, six in 10 (61%) said they now encounter more digital and online scams compared to traditional 'real-life' cons, like door-to-door bogus sellers. Eight out of 10 (80%) respondents said they worry that impersonation fraud may become harder to detect in the next five years, thanks to the rise of artificial intelligence (AI). Surprisingly, nearly a fifth (18%) admitted to responding to a message from an impersonator, initially thinking it came from a friend or family member. Furthermore, one in seven (13%) respondents stated they have previously lost money to fraud.

New parking app scam could cost you hundreds of pounds: The research conducted by One Poll also compiled a list of the top 10 scams people said they had been targeted with over the past year. These scams include:

- **Phishing scams:** Fake emails, calls, messages or websites that seem to be from legitimate organisations which ask you to provide personal or financial information.
- **'Trusted organisation' scams:** Fraudsters impersonate trusted organisations such as HMRC, energy companies or service providers, often claiming there is something wrong with your account or you owe a fine.
- **Refund scams:** Criminals impersonating trusted organisations offer bogus refunds and request personal or banking information.
- **Friend or family scams:** Messages sent to your phone or via social media claim to be someone you know asking for money urgently to pay bills.
- **'Get rich quick' scams:** Criminals claim people can make money quickly by investing in a company or goods.
- **Purchase scams:** Criminals place adverts for fake consumer goods and products online, on popular social media and even auction sites to gain money or information. Bogus offers may include games consoles, vehicles, concert and event tickets, designer clothing, pets or holidays.
- **Investment scams:** Criminals may encourage people to invest money in fake opportunities or pyramid schemes.
- **'Safe account' scams:** Criminals call pretending they are your bank or the police and that there has been fraudulent activity on your account, and to protect your funds you must move them to a new account to keep them safe.
- **Lottery cons:** Fraudsters claim someone has won a lottery prize, with a request to send over sensitive personal and/or financial information to claim it.
- **Befriending scams:** Criminals create fake accounts on social media and send connection requests, and after building up a friendship they ask for money, login information or other favours.

To safeguard against scams, the NatWest Fraud Prevention team shared some valuable tips:

- **Discuss scams:** Share information about scams you encounter with family and friends, helping each other stay informed about potential threats.

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



- **Honesty with your bank:** Never mislead your bank about the reason for a payment - if you are honest, the bank will be able to help you.
- **Be vigilant when buying:** When making purchases from social media or online marketplaces or considering online investments, conduct thorough research. Deals that seem too good to be true often are.
- **Protect your information:** Trusted organisations like your bank or the police will never ask you to transfer money for safety reasons or request your full pin, password or passcode.
- **Avoid unsolicited contacts:** Never respond to unsolicited calls, texts, emails, or social media messages or open suspicious attachments. These could be attempts to steal your personal information.
- **Check payment requests:** Always check your payment requests are going to who you meant them to and pay attention to the scam warnings on your texts and in your banking app.

An HMRC spokesperson said: “Take your time and check **HMRC advice on digital and online scams**. To help fight these crimes, forward suspicious texts claiming to be from HMRC to 60599 and emails to phishing@hmrc.gov.uk. Report tax scam phone calls to us on gov.uk. You can also contact HMRC directly but only use phone numbers from our contact details on gov.uk.

According to the National Cyber Security Centre - part of GCHQ - HMRC was the third most impersonated UK government body in 2022, behind the National Health Service and TV Licensing.

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