NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 7/24 (3 Jul 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.

CONTENT:

POTHOLES:

Potholes are the bane of motorists' lives. Not only do they make driving a challenge, but they can lead to repair bills of hundreds of pounds.

Encountering potholes is almost inevitable, especially after the last few cold wet months. The **RAC** report their patrols attended nearly 30,000 pothole-related breakdowns last year, up by 33% compared to 2022.

It can be tricky to navigate gaping holes in the road and can seem like a choice between swerving to avoid them, which could result in collisions with oncoming traffic, or risking serious damage to your car.

The motoring experts at Howden Insurance have shared tips on how to avoid potholes and what to do if you hit one.

- **Steps to take if you have hit a pothole:** Don't slam on your brakes: Although it can be a knee-jerk reaction to hit the brakes as soon as you hit a pothole, this may actually cause further damage. Try to reduce your speed slowly, before getting out in a safe place to assess your vehicle. By slamming on the brakes, you are putting more strain and compression onto the vehicle's suspension. This can cause misalignment, tyre and wheel damage and body or exhaust scrapes.

- **Check for damage:** Pull over, when it is safe to do so, and check your vehicle for any damage. Look for any dents, scrapes or visible damages to your wheels or tyres. When you get back into your vehicle, keep an eye out for any changes in the way it drives, such as any vibrations or if your car pulls to the side.

NIFC COMMUNITY AWARENESS UPDATE

- **Report the pothole:** Making an official report is easy to do, and may help it get fixed more quickly. If you were driving on the motorway when you hit the pothole, you should contact National Highways on 0300 123 5000 or visit **https://report.highwaysengland.co.uk**.

- You can report potholes on **FixMyStreet.com** who will forward details on your behalf.

- **Making a claim:** The insurance experts say you can make a claim for damage caused by a pothole if you have fully comprehensive insurance. You will need to take note of the where the incident occurred, as well as the date, time and weather conditions. The **RAC** say you may be able to claim compensation from the local authority or highways agency. Your chances of being successful will significantly depend on whether the pothole has already been reported. If they believe you have a valid claim, you will normally be sent a damage report form to complete and return. As well as basic information, they recommend including:
  - Copies of estimates or invoices for repairs to your vehicle.
  - A current MOT certificate.
  - Photos of the damage if you have them.

- The RAC stress that trespassing on a motorway is a criminal offence. Don't visit or try to photograph the location where your vehicle was damaged. Find out more **here**.

SUSPICIOUS EMAIL REPORTING SERVICE (SERS):

Over 32 million suspicious emails have been reported to the Suspicious Email Reporting Service (SERS), with more than a third of all emails reported in the last year.

The reports have led to more than **329,000 websites addresses being removed** by the National Cyber Security Centre. Action Fraud, the national fraud and cybercrime reporting service, launched a national phishing awareness campaign on 24 Jun 24, as reporting reached its highest level since SERS launched. New data shows a rise of 44% year-on-year, with almost 11,611,400 reports made to SERS in 2023, up from 8,074,200 reports in 2022.

Alongside emails, there has also been a huge number of text messages reported to 7726. In Mar 24, **more than 60,000 malicious websites were removed as a result of being reported using 7726**. This is a free service, offered by mobile network providers, allowing customers to report suspicious text messages in order to prevent other people from receiving them too.

Remember, if you think you have received a phishing email or text message, make sure you report it. You can forward emails to report@phishing.gov.uk, or forward spam text messages to 7726.

SERS was launched by the National Cyber Security Centre (NCSC) and the City of London Police in Apr 20, to enable the public to forward suspicious emails and report any malicious website links. Since its launch, more than 32 million reports have been made to the service.

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

What is phishing?

'Phishing', 'quishing' or 'smishing' is when criminals use scam emails, text messages, QR codes, or phone calls to trick victims. Whether it's an email asking you to "verify" your bank account details, or a text message claiming you've missed a delivery and are required to pay a redelivery fee, the goal is usually the same - to trick you into revealing personal and financial information.

In 2023, a doctor from London lost more than £150 to a fake email claiming to be from TV Licensing. The email claimed that they needed to renew her TV licence as soon as possible. What made the phishing email so believable was that the victim's TV licence had recently expired and the link in the email led to a fake TV Licensing website that replicated the real one.

Here's some practical advice you can follow when it comes to dealing with suspicious messages and calls:

- If you have any doubts about a message, contact the organisation directly using the contact details on their official website.
- Do not use the number or web address in the message. Your bank, or any other official source, will not ask you to provide sensitive information by email.
- Received an email that doesn't feel right? STOP! Report suspicious emails by forwarding them to: report@phishing.gov.uk. Send emails to this address that feel suspicious, even if you're not certain they're a scam – they will be checked.
- Always report suspicious text messages or scam call numbers, free of charge, to 7726. Your provider can find out where the text came from and block or ban the sender.
- To report a scam text, forward it to 7726 and then send the sender's number when prompted.
- To report a scam call, simply text 7726 with the word 'Call' followed by the scam caller's number.
- If you've lost money or provided financial information as a result of a phishing scam, notify your bank immediately and report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. In Scotland, call Police Scotland on 101.

SPEAR-PHISHING: ARE SCAMMERS TARGETING YOU?

How fraudsters use your personal information against you:

Personalised scam messages are much more convincing than generic ones – if a scammer can gather enough information on you, you're a target.

Spear-phishing is cleverly used by scammers to evade the usual evidence you count on to detect scams. When non-specific language is replaced with your name, address and date of birth, as well as something distinct, such as where you work or where you went to school, it's much easier to get conned by scam messages.

However, there are ways to scrutinise spear-phishing attempts and detect what's genuine and what isn't. Read the tips below to find out how.

NIFC COMMUNITY AWARENESS UPDATE

- **What is spear-phishing?** Spear-phishing uses information gathered on us to make scam messages more convincing. Generic emails, texts or messages saying that your bank account information has been compromised are transformed into eye-catching messages filled with your personal details, prompting you to take a second look.

- **The restaurant hack:** Chris received a call from Piccolino Restaurant in London saying the venue owed her the £30 deposit she supposedly made when booking via OpenTable. Although she did book the restaurant via OpenTable, she didn't recall making a deposit. The caller went on to tell her she could refund the deposit via a voucher – or reimburse it back to her card. Chris thought it didn't seem right for a member of staff to take card details over the phone. After Chris expressed her doubts, the caller's tone noticeably changed and became agitated. 'It's up to you if you want the deposit back or not'. Chris repeated her card number and expiry date. She was still suspicious but the caller reassured her: 'How would I know that you came into the restaurant at 5pm, left at 6.30pm and were celebrating a 60th birthday?' This was all correct, and Chris went on to give the three digits at the back of the card. After finishing the call, Chris descended into a complete panic as she knew something wasn't right. A few minutes later, she received another scam call purporting to be from her bank. Luckily, Chris realised this before it was too late, called her bank on a trusted number and cancelled her card.

- **What did the restaurant say?** The owner of Piccolino Restaurant, Individual Restaurants, said: 'One of our restaurants was subject to a phishing scam on 20 August 2023. It was an isolated incident during which a scammer was able to access the database for this specific restaurant, which contains phone numbers and booking details made via OpenTable. We responded promptly following notification of the incident and immediate steps were taken to close down access to the database, as well as contact any guests who may have been impacted. Further measures have been implemented internally, in partnership with OpenTable, to prevent future incidents.'

How do scammers get your data?

If you're wondering how a spear-phishing fraudster does their research, think back to that picture of your last holiday which you posted on Facebook or the work history in your LinkedIn profile.

In a survey where they delved into the social media habits of thousands of people in the UK, they found that on their public Facebook profiles:
- 68% of respondents share their names.
- 46% share their ages.
- 35% share their locations.

This can give a scammer some basic information to address you by name and include your location in a scam message.
- 21% of respondents share their places of work.
- 32% share their birthdays.
- 12% share their phone numbers and email addresses.

Now, a fraudster could call or email you, impersonating a colleague or offering you a job in your field.
- 18% of respondents share places they've visited

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

- 9% share their real-time location on their public Facebook profiles.

This information can allow fraudsters to develop seemingly uncanny messages that know where you are and where you've been.

What if you lock down your social media profile?

Even if you lock down the information you put out online, you can still be a target. Think of all the websites you visit and the ton of data you give away when you do. While this data isn't used for nefarious purposes, it can be if fraudsters are able to access it, and once data is breached, criminals can use it to create spear-phishing messages.

If you receive a message or phone call with information that only you would know, think about whether the details are truly exclusive knowledge and ask yourself: 'Is there any way someone could find this out?'

Who falls for scams?

The survey found that:
- 72% of Gen Z respondents have clicked on a link sent to them in a direct message from a friend or family member, compared to 57% of baby boomers.
- 15% of Gen Z respondents have clicked a link sent to them in a direct message from a stranger; only 3% of baby boomers had.
- 13% of respondents have provided personal information online as a result of clicking a link sent to them in a direct message. If we extrapolated that to the UK population, we're talking about 7.7 million people.
- 32% of respondents shared their birthdays on Facebook, and 14% shared them on public LinkedIn accounts.
- 20% shared their location on public Twitter accounts, and 15% shared their real-time location on public Snapchat accounts.
- 49% had private profiles on Facebook, 34% on Instagram, 19% on Twitter and 17% on TikTok.
- 24% shared images and or names of their friends and family on public Facebook accounts, 18% on public Instagram accounts. It's good etiquette always to ask before you share.

Six (6) ways to protect yourself against spear-phishing:

Every online or in-app click on your device takes you through page after page, capturing various data about you and your habits. Everything you type online puts more information about you onto the web.
Here are some methods of protecting yourself from scammers spying on you:

- **Temporary emails** - Register on websites with a temporary email address to protect yourself against potential email leaks. You can use services such as Temp Mail, Guerilla Mail or Apple's Hide My Email tool if you have an iCloud subscription.

NIFC COMMUNITY AWARENESS UPDATE

- **Check data leaks** - You can see if your data has been leaked at haveibeenpwned.com. Google users can visit passwords.google.com/checkup to see if any of their username and password combinations have been breached.

- **Protecting your devices** - In our survey, we found 55% have antivirus software installed on their laptops and 25% have it on desktops. Discover the best antivirus to protect your data.

- **Social media sharing** - Making social media profiles private keeps them away from potentially prying eyes. (Which? Tech subscribers should see our April issue, p16, to find out how you can lockdown your account.) You should also think twice about oversharing.

- **Suspicious messages** - Follow classic scam advice including being wary if you're contacted out of the blue or are offered something that seems too good to be true. Being asked to share personal and financial data or being pressured to make a decision are also red flags. And don't click on links in suspicious messages.

- **If in doubt, get in touch** - Not sure if a message is genuine? Go to the company's website. Don't click a link in an email or message to do this – use a search engine or type the URL directly into your browser. Then, check the website for the best way to contact the company. This may take a little longer, but you'll know you aren't being scammed.

How to beat cold callers:

Speak to your telephone network to see what call-blocking solutions may be available to support you or vulnerable friends and family.

You can also:
- Register landlines and mobile numbers with the Telephone Preference Service (TPS) free of charge. Then report marketing firms that breach this.
- Report nuisance calls, spam texts and breaches of the TPS to the Information Commissioner's Office (ICO) using its online reporting tool.
- Send the company a subject access request – via email is fine – asking it to supply you with copies of your data and proof that it had consent to contact you. It must reply within one month of receiving the request, and can be reported to the ICO if it doesn't.
- Refer to Action Fraud (in England, Northern Ireland and Wales) and Police Scotland (in Scotland) if you or someone you know has been the victim of fraud. Wider concerns about a business' practices can be referred to Trading Standards.

HOW TO SPOT A HOLIDAY SCAM:

From fake accommodation listings to dodgy reviews, here are our top tips to spotting the signs that a holiday offer is too good to be true.

NIFC COMMUNITY AWARENESS UPDATE

Incredibly cheap online deal?
If the price for your flight or holiday is considerably cheaper than the average cost elsewhere, you should be suspicious. Flight prices are largely set by airlines – with travel agents having some leeway – so, charging significantly less is often a sign that there may be a scammer behind the offer.

Look out for logos:
Looking out for official logos is a good way to check the authenticity of holiday booking, travel agent and tour operators. Seeing the Atol logo in your travel company's brochures, adverts and websites should mean your holiday will be protected.

You can use the Check an Atol facility on the CAA website to check the Atol details of your travel company and the authenticity of any claims it's making.

If you have booked a holiday and have been assured you are Atol protected, make sure you are also given an Atol Certificate and know for sure that your holiday is Atol protected. The law says you should be given this certificate as soon as you have booked and paid money.

Key Information:

What Atol covers:
If you have booked an overseas air holiday booked with a UK travel company, Atol protection should apply.

Your holiday must be protected by law if you've booked it with a single travel firm that includes the following:
- Flights and accommodation (including a cruise).
- Flights and car hire.
- Flights, accommodation and car hire.

The scheme also applies when you book flights UK domestic or international flights, but don't get your tickets straight away.

Atol does not apply to holidays or flights directly booked with scheduled airlines or to flights booked with airline ticket agents.

You can also look out for any logos that the travel agent or tour operator is a member of a recognised trade body such as ABTA. This will also help you to identify if the company is legitimate.

If the company is a member of a recognised travel authority, you will have better financial protection and access to a complaints service should something go wrong.

If you're unsure, you can go on the ABTA website and verify the membership of the travel company.

Watch out for fake listings:
Popular holiday booking websites such as Airbnb and Holiday Lettings are a great place to find accommodation at a reasonable price.

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

Most listings are genuine, but scammers have figured out that they can use the popularity of these sites to dupe people and make some quick cash.

Scammers use these sites to set up fake listings with enticing deals for swanky getaways. A key tactic to look out for is that they will often try to get you to pay for your stay outside of the official website. Avoid any listing that asks you to pay by bank transfer or outside the internal system.

Don't be tempted to follow a weblink that arrives in an email, however good it looks. If you're prompted in an email to log in to your profile, go to the official site and do it from there.
If the email is genuine, the same message will be there. If you're already logged in and the message you received isn't on the internal system, then it's probably a scammer.

Before you book, sites such as Airbnb and Holiday Lettings ban direct contact outside of their mail system to deter fraudsters. So, if you see a listing with the host's email or phone name, be very suspicious.

Bank transfer the only option?:
If a bank transfer is your only option for payment, this should set alarm bells ringing. You should be especially cautious if you're asked to pay directly into a private individual's bank account. Not only does this show no bank is prepared to provide credit card facilities, but – if you're dealing with a scammer – it will be almost impossible to get your money back.

Paying by direct bank transfer means your money will be very difficult to trace should something go wrong and is not refundable. Wherever possible, pay by credit card or a debit card. If you feel confident it's not a scammer and you're willing to make payment to the individual, make sure you use a secure payment site like PayPal.

If you're on holiday booking sites such as Airbnb or Holiday Lettings, you should never pay by bank transfer. Always use the internal site system to pay.

Check online reviews:
Do a thorough search to check the company's credentials. Check multiple reviews for information on other people's experiences and take note of any warnings about the company.

If a company is defrauding people, there's a good chance you will find out pretty quickly by reading several reviews.

Make sure you check several online review sites before booking and don't just rely on one. There's a chance the scammer could have posted a few fake reviews to make them look better.

There are some tell-tale signs that a scammer may be behind one or several reviews, including the limited sharing of factual information. Make sure you read our full list of top tips on how to spot a fake review and stay alert.

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

Being offered a 'free' holiday?:
Getting something for free is incredibly rare and so if you're being offered a free holiday, you should be on your guard.

Many victims of timeshare scams were offered 'free' holidays to entice them into attending a seminar where they were then pressured into committing to a dodgy timeshare deal they later struggle to pay for or to sell to someone else.

You need to be on your guard against being talked into signing up for something you later regret. For example, closely study T&Cs, as well as receipts and invoices, when considering an offer and be very wary of any companies that don't provide any at all.

Before you commit to signing any type of contract, especially if the offer involves a holiday club or timeshare, it's a good idea to get it thoroughly vetted by a solicitor.

Key Information:

Beware high-pressure selling.

Timeshare agreements last for a long time and can be difficult to cancel, and some are sold in very high-pressure situations.

At these two to three-hour seminar sales pitches, you may be offered additional perks such as free alcohol and food to try entice you.

After saying 'no' to the first salesperson, often a more senior colleague will take their place, and so on. For every reason you give to decline, the salesperson will offer a sweetened deal or argument to try and convince you that your reason for saying 'no' to them is not a good reason.

Buy official:
If you're planning on going to a well-known religious pilgrimage, want to buy a ticket for a popular festival event or are desperate to go to a sporting game in high demand, you should try to buy through the official website and be careful of secondary ticketing sites.

Scammers know which events are popular and which have limited tickets, so will try and take advantage of people willing to pay high prices.

What to do if you've been scammed:

If you've sent your card details to a scammer, or lost money to a scam, call your bank immediately (using the number on the back of your card or on your statements) and report the scam to Action Fraud.

Giving away sensitive details, such as an email address, can be enough for a scammer to access your accounts. Be extra-vigilant in case you are targeted with more scams and increase your security by changing your passwords and setting up two-factor authentication.

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

You should also report the offending account to the relevant social media platform.

Frustratingly, this may not always result in its removal, but under the new Online Safety Act, tech firms including X could eventually be fined for failing to remove harmful and fraudulent content from their platforms.

To report something on X, click on the three dots and select 'report' from the dropdown menu. You can also report individual tweets, again by clicking the three dots above the tweet.

Seen or been affected by a scam? Help us protect others:

Sharing details of the scam helps us to protect others as well as inform our scams content, research and policy work.

BOOKING.COM WARNING

Booking.com is warning artificial intelligence (AI) is driving an explosion in travel scams.

The firm's internet safety boss, Marnie Wilking, said there had been "anywhere from a 500 to a 900% increase" in the past 18 months. She said there had been a particularly marked increase in phishing - where people are tricked into handing over their financial details - since generative AI tools like ChatGPT burst onto the market. "Of course, we've had phishing since the dawn of email, but the uptick started shortly after ChatGPT got launched," she said. "The attackers are definitely using AI to launch attacks that mimic emails far better than anything that they've done to date," she said.

Phishing attacks often try to convince people to hand over their card details through by sending them fake - but very convincing looking - internet booking links.

Scammers often target websites like Booking.com and Airbnb because they allow people to list their own places to stay. After someone pays up, the scammers either vanish without a trace - leaving the buyer without a place to stay - or even try to scam them out of more money through follow-up messages. These sorts of scams have been around for decades, though they often come with tell-tale signs of fraud, such as spelling mistakes and grammatical errors.

But - speaking at the Collision technology conference in Toronto - Ms Wilking said AI was making them harder to detect because it could generate realistic images and much more accurate text, in multiple languages. She is calling for hotels and travellers to use two-factor authentication - it involves an additional security check, such as inputting a code sent to you phone - calling it "the best way to combat phishing and credential stealing".

She also urged people to more vigilant than before when clicking on links.

But despite criticising how scammers are using AI, she said the technology was also allowing Booking.com to rapidly remove fake hotels that tried to scam people.

NIFC COMMUNITY AWARENESS UPDATE

ANTISOCIAL BEHAVIOUR (ASB):

In the National Crime and Community Survey 2023, respondents stated that antisocial behaviour (ASB) has been the most experienced, and the most feared, crime, over the previous 12 months. Although The Office for National Statistics (ONS) reported that crime rates dropped by 10% in 2023, the survey found that a staggering 37% of Brits experienced a crime in the last year, with 63% of those having experienced antisocial behaviour, followed by physical assault (25%).

RECOGNISE:

Recognising what ASB is and what ASB isn't can be difficult. What constitutes ASB is extremely subjective and whilst we have examples of behaviour, what you may consider to be antisocial behaviour another person may not. Have a look at our guides to help you identify ASB. Antisocial behaviour is a range of behaviours that can cause nuisance and annoyance or harm and distress to a person in their home, neighbourhood or community. It is a wide range of unacceptable activities such as:

- **Noise nuisance** including loud music, banging, DIY at unsocial hours, loud parties and frequent visitors at unsocial hours.
- **Household disputes** including shouting, swearing and fighting.
- **Harassment and intimidation** including intimidation through threats or actual violence, abusive behaviour aimed at causing distress or fear to certain people, e.g. elderly or disabled people, and verbal abuse.
- **Environmental antisocial behaviour** including dumping rubbish, animal nuisance, including dog fouling and dogs barking, vandalism, property damage and graffiti, antisocial drinking, driving in an inconsiderate or careless way, for example, drivers congregating in an area for racing/car cruising, and arson (secondary fires).

There is a fine line between antisocial behaviour and neighbour disputes which can often begin over relatively minor inconveniences, such as parking. However, if they persist, they can potentially become antisocial behaviour.

Antisocial behaviour is not parking (including badly parked vehicles), children playing, neighbours doing DIY (at reasonable times of the day), groups of young people in the street or in parks unless they are being rowdy, abusive, causing damage or committing other crimes, noise caused by everyday living, religious or cultural practice, one-off parties, or general living noise.

RECORD:

It is important to keep a record of the incidents and the behaviours as this will be of great help in investigating the behaviour and tackling it. It can also help you to get some perspective on how often it happens. If you decide to take formal action at some stage, it can help others see an established pattern of nuisance over time.

Use an ASB diary to record events over a period of **14 continuous days**. You can ask someone else (a neighbour or visitor) who witnesses the nuisance to sign the entry in the "names & addresses of any witnesses" column. Return your completed diary to your ASB team at your local authority. If you live in private accommodation, or if you live in a local authority or housing association property, return it to your housing officer.

REPORT:

Antisocial behaviour can ruin lives and devastate communities. Reporting antisocial behaviour early on is important to prevent it from escalating.

The Local Authority, Social Housing Landlords & the police all have powers to deal with antisocial behaviour. It is important that on reporting anti-social behaviour to your local authority, police or housing provider that you detail the **impact that it is having on your health and wellbeing being**.

If the antisocial behaviour is serious, criminal or causing a risk to a person report it to the police in the first instance:

- If it's an emergency and the crime is still taking place, call 999 and ask for the police
- If it's not an emergency, call the non-emergency number 101 instead.
- For more ways to report to the police, see our reporting page.

Secondly, contact either the Local Authority or your Social Housing Landlord.

If you are a **tenant or a leaseholder of a Social Housing Landlord**, contact your landlord to report the issues. Landlords should take complaints seriously and act professionally. If you ask, they must publish and provide documents that set out the types of behaviours they can help to tackle. Your landlord should clarify what information they need from you and what help they can provide and keep you updated until your case has been closed. They should also tell you about the help available from other agencies with different powers and responsibilities, such as your local authority or the police, and support you to approach them. They should also put you in touch with services such as Mediation and Victim Support if needed.

If you are in **private rented accommodation or a homeowner**, contact your local authority who will have dedicated personnel who deal with antisocial behaviour.
If the antisocial behaviour is not serious, criminal or causing a risk to a person, you should contact either the Local Authority or your Social Housing Landlord in the first instance, then the police.

SOME INFO FROM OUR COLLEAGUES AT SAWDEY SOLUTION SERVICES:

Seven (7) Essential Summer Safety Tips For All Ages:

It's summer (?), and we have a few more weeks to soak up the sun and the outdoors before the weather cools down. But summer adventures aren't without some risks, from damage and injuries caused by the sun and heat to water-related and environmental accidents.

Whether you're spending the summer months at the pool, tackling yard work, or traveling to new destinations for a beach vacation or hiking, knowing how to stay safe is vital for all ages. Here are our top safety tips for keeping everyone in your family healthy and happy this summer.

NIFC COMMUNITY AWARENESS UPDATE

Remember these summer safety tips.

1. Be prepared for anything by checking the weather before you head outside:
The weather can be unpredictable, but thanks to our smartphones, we can access weather predictions anytime, anywhere, even for impromptu trips. It's important to adequately prepare for the weather and your surroundings, especially if you are traveling or far from home. (And, keep that cell phone nearby in case of an emergency!) When you know the approximate temperature, you can plan to dress accordingly. Knowing what the weather will be like can also help you determine what to bring to help keep you safe, protected from the sun, and hydrated.

It's also good to stay on top of something called the UV index, which indicates how much ultraviolet (UV) radiation is expected from the sun. The higher the UV index, the more at risk you are of overexposure and sun damage. This is important to know because the UV index can be surprisingly high on cloudy days when the sun is out of view. If the UV index is over three, you should take additional precautions to protect your skin from the sun, like wearing sunscreen and sun-protective clothing, hats, and sunglasses.

2. Lather on sunscreen anytime you're outdoors:

Unprotected skin can quickly burn in the sun, which can cause immediate and long-term damage. Sunburn is a common summer injury, but early and frequent exposure to the sun can also lead to skin cancer, including melanoma, which can be deadly. Wearing sunscreen is one of the best summer safety tips to ensure you stay healthy now and in the future.

For the best protection, you should apply a shot-glass-sized amount of sunscreen 30 minutes before going outside, and reapply every two hours or sooner, if you are sweating or swimming. This recommendation applies to people of all skin tones and ages, as anyone is susceptible to sun damage. Even if you don't burn easily, the sun can cause other skin damage, including wrinkles, photoaging, and sun spots.

Choosing a sunscreen for babies and kids:

When choosing a sunscreen for kids, consider selecting one that is a physical or mineral sun blocker. These use zinc oxide or titanium dioxide rather than chemicals and are less likely to cause a reaction.

If you have a newborn or infant, you may have noticed that the back of the bottle recommends asking a doctor before applying sunscreen to babies under six months of age. That's because babies especially should be kept out of the sun, as early overexposure significantly increases the risk of skin cancer later in life. However, it's a myth that you can't apply sunscreen to your little ones. Try to keep them in the shade and/or covered with clothing and hats, but definitely apply sunscreen to any areas of exposed skin, like the face, if you are out walking or otherwise can't avoid the sun.

3. Wear the right clothing and accessories:

Where you're going should affect what you choose to wear. What you'd wear to the beach should be different than what you'd wear on a summer hike on a hot day. In either case, you may want to wear more than you think you'd need. Many people wear less clothing in the summer sun, but it's a good idea to opt for more skin coverage when possible. Many articles of clothing now have a UPF rating, which indicates they provide additional skin protection from the sun. Light-coloured and lightweight clothes can also help reflect the sun, keeping you cool and safe.

You should also wear a hat that has a UPF rating and is wide-brimmed, protecting the face and neck. In addition, sunglasses offer important eye protection from the sun. We often think about sunglasses as a fashion accessory but they're actually very important for minimizing long-term vision problems. We recommend choosing shades that provide 99-100% UVA and UVB protection.

4. Pack a refillable water bottle and first aid kit:

Staying hydrated is extremely important, especially with increased outdoor activity over the summer. Drink plenty of fluids, regardless of how active you are, especially in dryer climates or higher altitudes. Don't wait till you are thirsty to drink, as that's a sign you're already low on fluids. In addition, avoid surgery or alcoholic drinks which can actually cause you to lose more body fluid. Don't forget to keep your pets hydrated too, giving them plenty of fresh water and shade.

It's also a good idea to pack a personal first aid kit to help tend to common summer injuries. You can buy a pre-assembled first aid kit online or build your own with:

- **Soft gauze, tape, and antibiotic ointment** for minor cuts and scrapes
- **Sunscreen** for frequent application in the sun
- **Bug spray** to ward off mosquitoes and bug bites
- **Aloe vera** to soothe sunburns
- **Hydrocortisone cream** to ease itchiness and irritation from insect bites or poison ivy

5. Be vigilant about water safety:

It's not just the pool and open water at the beach that can cause drowning. The majority of drownings for kids between one and four actually happen during non-swimming times, like at a backyard barbecue where someone has a fountain, pond, or baby pool. For that reason, it's important to always be aware of your surroundings, and if you have a child that is not a strong swimmer, always practice "touch supervision." In other words, stay within arms-length of your toddler or young child anytime you are in or near water. If you are with a group of people, you can also assign an adult (who isn't drinking alcohol) to be the designated "water watcher."

The best thing you can do to protect your child from the dangers of water is by getting them swim lessons, if they're over the age of one. If your young child cannot swim or is not yet a proficient swimmer, definitely consider a well-fitting life jacket that is coast-guard approved anytime you are around water, whether you're boating or at the beach or pool. A foam noodle or pool-floatie should not be a replacement for a life vest.

6. Know the risks and signs of heat exhaustion:

Heat-related illnesses, like heat exhaustion or heat stroke, occur when the body can't properly cool itself. During extreme heat, a person's body temperature can rise faster than the body can cool it down, leading to damage to the brain and other vital organs. Older adults, young children, and people with chronic diseases are at the highest risk of heat exhaustion, although it can also happen to young, healthy people who are participating in strenuous activity in the heat.

Warning signs can vary but may include feelings of:

- Dizziness
- Muscle cramping
- Weakness
- Fatigue
- Confusion
- Heart palpitations
- Nausea

If you notice any of those and generally feel unwell, go indoors immediately. Rest in a shady or air-conditioned place, drink water, and blot your skin with cool water to help lower your body temperature.

7. Never leave your pets or children unattended in a car:

It only takes about two minutes for cars to heat up to lethal levels, so it is critical that you never leave a young child or animal alone in your vehicle at any time. We're all capable of making mistakes or forgetting where we're going or why, but there are a few things you can do to remind yourself that you bring everyone with you. If you have children in car seats, one thing you can do is put something you need, like your purse, wallet, phone, or shoes, in the backseat next to your child. This will help you remember to check the backseat and bring your children with you. It may sound silly but if there's a family emergency or a change in routine, it could help save a life.

Finally, sun and heat-related illnesses and injuries are especially common when families are traveling in new, unfamiliar environments. So it's always a good idea to know your limits, use common sense, and be aware of your surroundings, wherever you are. Don't wait until you have an emergency to prepare—know your emergency plan ahead of time, stay cool, and stay safe!

Five Tips for A More Sustainable Summer:

Summer is the perfect time to go green! Check out these five sustainability tips for the warm season ahead.

NIFC COMMUNITY AWARENESS UPDATE

- **Eat Seasonally & Locally (& Go Heavy on the Veggies):**
  Show seasonal produce some love! Treat yourself to nutritious vegetables and fruits that benefit your health, while also supporting local farmers and the planet.

- **Unplug:**
  Get outside! Breathe in some fresh air and enjoy the beauty of Wisconsin. Go for a bike ride, take a walk, listen to live music, or even take a camping trip with friends. Whatever you do, put down your electronics for a while every day and engage with your natural surroundings. Before you leave the house, remember to defeat phantom energy by making sure chargers, adapters, and small appliances are unplugged.

- **Stay Hydrated with A Reusable Bottle:**
  Hot summer days can get quite dehydrating, especially after a long hike or bike ride. Make sure to quench your thirst using a reusable water bottle rather than a disposable one. While you're at it, consider using reusable containers and utensils for picnics and barbecues, too!

- **Sun-Dried Savings:**
  Take advantage of the sunny skies and warm breezes by air drying your laundry outside on a clothesline. Simply string up a line between two trees or two posts outside your house in the sun, get some clothes pins, and pin wet laundry to the line. It'll save energy as well as money on your next electric bill.

- **Close Your Shades:**
  Temperatures are getting warmer and air conditioners are constantly on—but that doesn't mean you have to do the same. Before you spring for the AC, consider a more sustainable option. You can keep the temperature down in your home by opening windows at night to let in the cooler air, then closing them first thing in the morning and lowering your shades to block the hot sun and take advantage of your house's insulation. If your house is not well insulated, you can open the windows during the day to create a cross-breeze.

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

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

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 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