NIFC COMMUNITY AWARENESS UPDATE

NIFC COMMUNITY AWARENESS UPDATE 7/22 (8 Jul 22)

(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.)

A Bldg 407 'family' member recently encountered a doorstep scammer – albeit only a small financial loss, greater impact on well-being/safety. MO was to place a bag in the open doorway and then 'press' forward with other goods.

What is a doorstep scam?:

- A doorstep scam (or doorstep fraud) involves someone calling to your front door out of the blue, with the aim of tricking you out of money. There can be an added pressure when dealing with someone face-to-face. This can sometimes be even more challenging than dealing with other types of scams, such as phone scams or online scams. There are some honest doorstep sellers, but there is a fine line between a scammer and an unscrupulous trader. Scammers usually have the gift of the gab and will try to smooth talk you with a convincing story. Or they might be pushy and intimidating, trying to get you to sign a contract or buy something you don't want. Their main aim is to trick you out of money or gain access to your home to steal valuables. Either way, the key is not to let them in, and report them as soon as possible. Follow our tips below to prevent doorstep scams.

Common doorstep scams to look out for:

Rogue traders:

- **The scam:** a trader will come to your home and offer to do some work for you at a special rate – this might be new paving or a new driveway. Another common tactic is to claim that you have a hole in your roof or your damage to your guttering – usually something that you can't easily check yourself. They'll say that it's very urgent and put pressure on you to get the work done immediately.
- **The reality:** it's highly likely that they've made up the problem. They might pretend to fix it or do a shoddy job. They'll then charge you an extortionate amount for the 'work'.

Hard-luck stories:

- **The scam:** a stranger (who might seem perfectly respectable and friendly) will turn up on your doorstep pretending that, for example, they need to use the phone because their car has broken down or their pregnant girlfriend is ill – they need a glass of water – they've lost their dog in your garden.
- **The reality:** they'll say anything to make you feel sorry for them and will take advantage of your good nature to help them. While you fetch the water or go to get the phone, they might pocket your valuables. Or they might work in pairs – while one distracts you the other will gain access to your home.

Bogus officials:

- **The scam:** an official looking person with a uniform and ID badge turns up on your doorstep. They might say they are there to read the gas meter or conduct a survey for the local council.
- **The reality:** their ID could be fake. They want to get into your home or trick you into divulging personal information that can be used for ID fraud.

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

Nottingham Knockers:

- **The scam:** usually carried out by young men, who go door to door selling household products. They carry a fake ID and claim to be recently out of prison or on probation, and claim that this is a legitimate rehabilitation scheme.
- **The reality:** the household goods are supplied by a man (traditionally from Nottingham, hence the name) who employs them. A group of young men are dropped off to work an area, and then collected by the same man later that day. The knockers' role is to establish where elderly or vulnerable people live, and this information is then sold on to other criminals. If they come to your door, the advice from the police is to phone 101 to report them. However persistent they are with their hard-luck stories, do not buy from them.

Protect yourself from doorstep scams:

- **Be on your guard:** always be suspicious of anyone turning up at the door uninvited – regardless of their story.
- **Put up a sign:** place a sign in the window near your front door saying that uninvited callers are not welcome.
- **Keep your home secure:** don't let any stranger into your home. Keep your doors locked with the chain on.
- **Look for ID:** ask to see callers' ID cards and call the company to see if they are genuine. To be safe, look up the company number yourself rather than trust the number on their ID card. If you feel uncomfortable or have any doubts, don't let them in. It's your home. Tell them you're not interested or that now is 'not convenient' and ask them to come back at a different time (when you can have a friend or relative with you).
- **Set up a utilities password:** you can set up a password with your gas and electricity providers so that you can be sure callers (such as meter readers) are genuine – only genuine callers will be aware of your password. Call your utility company to arrange this. To activate the service they might need to put you on their Priority Services Register.
- **Nominate a neighbour:** if you have a relative or friend who lives close by, ask if they'd mind being on standby in case you get any suspicious callers. Before letting a stranger into your house, give your neighbour a call and ask them to pop round. If you don't know anyone nearby, contact your local Neighbourhood Watch Scheme or Safer Neighbourhood Team to find out if they can help.
- **Consider smart security devices:** smart doorbells incorporate a camera and can enable you to speak to a caller without opening the door; some can also send a message to a relative notifying them that you have a visitor. Find out more in our guide to smart security.
- **Take a photo:** if you're suspicious, ask the caller if you can take their photo on your mobile phone. Then send it to a close friend or relative. If the caller is genuine, they probably won't mind.
- **Call the police:** if a caller is really persistent and refuses to leave, you can call 999. If you are suspicious, but not in immediate danger, call 101, the police non-emergency number.

What to do if you're caught out by a doorstep scam?

- If you're caught out by a doorstep scam, there are several steps you can take.
- Report the incident to Action Fraud, the UK's National Fraud reporting centre, who monitor and investigate cases of fraud. Speak to an Action Fraud adviser directly on 0300 123 2040.Alert your local police or Neighbourhood Watch so they can warn other residents that the fraudster is in the area.

Is it an emergency? Call 999

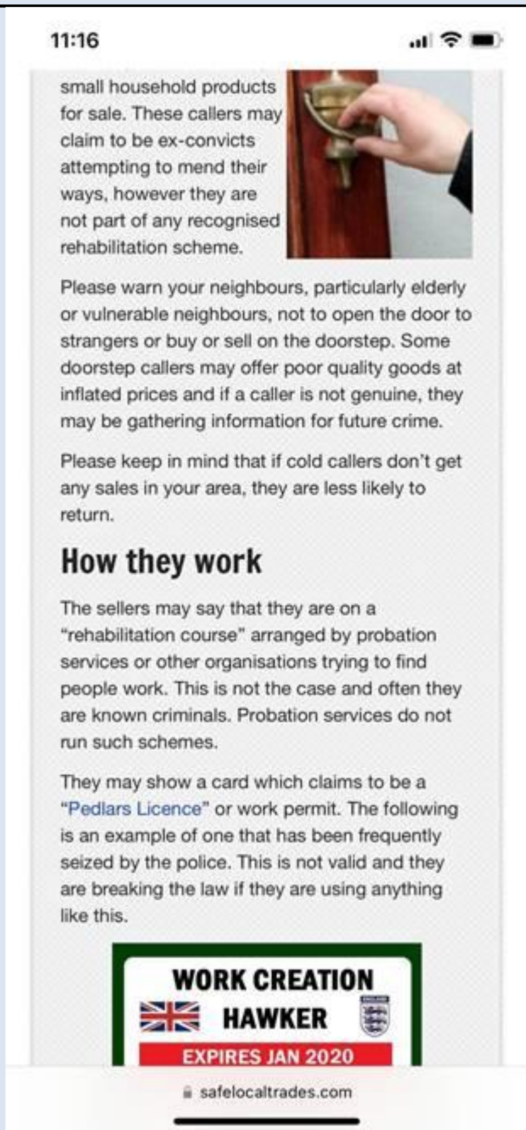
If it is <u>not</u> life threatening: Call 101 for the Civil Police; Call 111 for the NHS.

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

- Report dodgy salespeople to Citizens Advice (CA) (who can pass complaints to your local Trading Standards authority) if you believe they have sold you faulty, inferior or overpriced products or services. Call the CA Consumer helpline on 0808 223 1133 or chat with an adviser online.
- If you buy something as a result of an unsolicited visit to your home, you have a legal right to cancel – but be warned that you might not be able to track down a scammer.
- If you've paid by card or cheque, contact your bank to see what it can do. It should be able to offer advice on stopping the payment and keeping your bank account safe.

One of the current scams:	

11:16

small household products for sale. These callers may claim to be ex-convicts attempting to mend their ways, however they are not part of any recognised rehabilitation scheme.

Please warn your neighbours, particularly elderly or vulnerable neighbours, not to open the door to strangers or buy or sell on the doorstep. Some doorstep callers may offer poor quality goods at inflated prices and if a caller is not genuine, they may be gathering information for future crime.

Please keep in mind that if cold callers don't get any sales in your area, they are less likely to return.

How they work

The sellers may say that they are on a "rehabilitation course" arranged by probation services or other organisations trying to find people work. This is not the case and often they are known criminals. Probation services do not run such schemes.

They may show a card which claims to be a "Pedlars Licence" or work permit. The following is an example of one that has been frequently seized by the police. This is not valid and they are breaking the law if they are using anything like this.

WORK CREATION
HAWKER
EXPIRES JAN 2020

safelocaltrades.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

NIFC COMMUNITY AWARENESS UPDATE

COPYCAT WEBSITE SCAMS

Copycat Websites and Online Services

Copycat websites that appear to be legitimate government services and departments are regularly set-up by cyber criminals. They are designed to steal your personal data and payment details or charge extensive handling fees for tasks that are normally free or can otherwise be easily completed online using the actual relevant government website.

Cyber criminals often post fake links on social media or use sponsored ads and other techniques to get their sites to appear in your Google or other search results when looking for an official site covering: driving licences, passports, business grants, blue badges, etc.

Always use the **gov.uk** website portal to find the genuine HMG (UK) government service, department or information you need.

Other Phishing Sites

Similar techniques are used by cyber criminals to get you to visit fake but realistic logon pages or phishing sites to obtain your passwords, personal information and payment details. These may look identical to the genuine online store, social media site, payment service, customer support page or account logon you would expect to see.

Avoid clicking links received via email, text message or social media unless you have verified the source. Fake competitions, quizzes, surveys, discount vouchers and offers are also popular methods used by criminals to get you to click on a link to a phishing site.

- Enable your browser (**safebrowsing.google.com**) or security software web-safe (eg. Microsoft Edge SmartScreen) feature to help avoid known untrusted sites.
- A rudimentary but useful check using a domain/web address can be carried out on: **check.getsafeonline.org**
- Report suspicious websites so they can be checked and removed: **ncsc.gov.uk/section/about-this-website/report-scam-website**

For further cyber safety resources and advice contact:

CyberProtect@northants.police.uk

NorthantsCyber

Northamptonshire Police

Fighting crime, protecting people

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