Devon & Cornwall Police

Neighbourhood Policing newsletter (Summer 2020)

Reducing Opportunities for Crime

Doorstep Crime is the name given to crimes carried out by bogus callers and rogue traders who call uninvited at **your** home under the guise of legitimate business or trade. The phrase 'doorstep crime' includes distraction burglary, bogus callers, rogue traders and unscrupulous sales people.

Most people who knock on your door or ring your doorbell are genuine, but some are not. A friendly face and a warm smile is not always what it seems. Always be on your guard.

The Home Office definition of distraction burglary is 'Any crime where a falsehood, trick or distraction is used on an occupant of a dwelling to gain, or try to gain, access to the premises to commit burglary. It includes cases where the offender first enters the premises and subsequently uses distraction burglary methods in order to remain on the premises and/or gain access to other parts of the premises in order to commit burglary.

What can YOU do yourself to reduce the likelihood of it happening?

People that commit these types of offences may say they are from the water, gas or electric company or the local council. They may ask for a glass of water, or to wash their hands or claim to have lost a pet. They will use ANY STORY to get into YOUR HOME. They can be young (even children) or old, male or female, and might work alone or in teams. They often target the elderly and/or vulnerable.

YOU can KEEP THEM OUT if you have any doubt at all:

Lock – your doors and windows, even when you're at home.
Stop – are you expecting anyone, do they have an appointment? Make sure the back door is locked – some thieves work in pairs with the other one sneaking in the back while you're at the front door.
Chain – put the door bar or chain on before you open the door.
Check – check their identity carefully. Don't be afraid to ask for ID.

More information: dc.police.uk/home-security

Courier Fraud

What is courier fraud?

Fraudsters telephone a potential victim, claiming to be from their bank, the police or another law enforcement authority. They then trick the person into revealing their PIN and agreeing to hand over their debit or credit card.

What should I look out for?

Calls where someone claims to be from your bank or the police. They may say that a fraudulent payment has been spotted on your card, or that someone has been arrested using your details and cards.

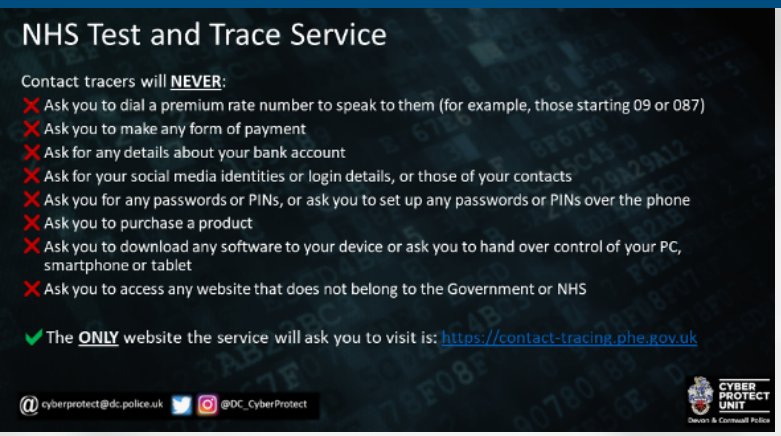
They may then ask you to ring back using the phone number on the back of your card. This is to make you believe that the call is genuine. But the fraudster keeps the line open at their end, so you are actually connected straight back to them or an accomplice.

They will ask for your PIN, or sometimes ask you to key it into your phone's handset. You should never give this to anyone.

The scammer then sends a courier or taxi to pick up your card from your home. It is possible the driver does not know they are being used as part of the scam.

Once they have your card and PIN, the scammer can spend your money.

COVID-19 Phishing Scams



How to recognise and avoid phishing scams

Phishing is where people try to get hold of sensitive information such as usernames and passwords by pretending to be from a trustworthy source. Hackers are becoming more sophisticated and the spoof emails can look very convincing.

Spear phishing pretends to come from a person or business that you know. They will use information they can find online (often on social media) to target you.

How to avoid becoming a victim of cybercrime and phishing:

Cyber Aware is the UK government's advice on how to stay safe online during coronavirus.

1. Avoid having the same password for all your accounts, create a separate password for your email.
   Your email contains lots of information about you. If your email is hacked all of your other passwords can be reset.
2. Make you password strong by using three random words.
   Weak passwords can be hacked easily, use a sequence of three random – *but memorable* – words you'll remember.
3. Save your passwords in your browser
4. Turn on two-factor authentication
5. Update your devices
   Ensure you have the latest software updates, which have improved security features.
6. Turn on automatic backup
   To protect your personal data from being, lost, damaged or stolen.

https://www.ncsc.gov.uk/cyberaware/home

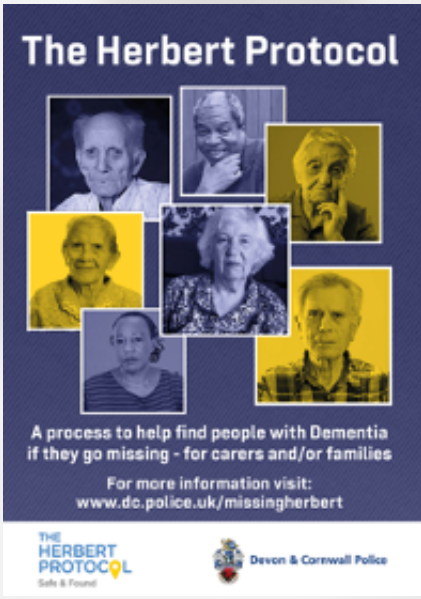
If you have received an email which you're not quite sure about, forward it to the **Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk**

How to protect your family and friends:
Anyone can fall victim to a scam, but older people can be at greater risk because scammers tend to target people who:

- Live alone
- Are home during the day
- Have savings or valuables in theiR homes
- Due to loneliness or isolation they may be more inclined to talk to people they don't know.

Look out for the signs of having been scammed:

- More post/letters lying around the house.
- More phone calls from strangers or companies.
- Large unexplained cash withdrawals/ cheques
- Having less money than expected.
- More anxious or upset.



Discuss this newsletter with your loved one. Help them make their property more secure. The Police can help with this. Help them be secure on the internet.

Report any potential fraud to Action Fraud

Call 999 in an emergency or report via 101 or online

Useful websites

- dc.police.uk
- actionfraud.police.uk
- ageuk.org.uk/

Devon & Cornwall Police