Information Alert – Test and trace scams – 4 June 2020

There have been many reports across social media of test and trace scams.

Please remember, genuine texts, calls or emails from the NHS service won't ask you for any personal details upfront.

You'll be given a unique ID number to log in to the NHS Test and Trace website. The **only** official web address for the NHS Test and Trace service can be accessed via the GOV.UK website.

Once you've logged in using your ID, you'll be asked to enter some basic information about yourself including:

- Your name, date of birth and current address
- The names of the people you live with
- Places you've recently visited
- Names and contact details of people you were in touch with around 48 hours before you developed symptoms

You won't be asked to share this information upfront over a call or text, so if someone is asking you for it directly, they are a scammer.

Contact tracers will **never**:

- Ask you to dial a premium rate number to speak to us (for example, those starting 09 or 087)
- Ask you to make any form of payment or purchase a product of any kind
- Ask for any details about your bank account
- Ask for your social media identities or login details, or those of your contacts
- Ask you for any passwords or PINs, or ask you to set up any passwords or PINs over the phone
- Disclose any of your personal or medical information to your contacts
- Provide medical advice on the treatment of any potential coronavirus symptoms
- Ask you to download any software to your PC or ask you to hand over control of your PC, smartphone or tablet to anyone else
- Ask you to access any website that does not belong to the government or NHS

Stay scam aware and report any suspicious approaches to us via our partners the Citizens Advice consumer helpline on **freephone 0808 223 1133.**

To find out more about the NHS test and trace service visit the GOV.UK website.

Rogue Trader Alert – Doorstep cold callers offering 'driveway work' – 3 June 2020

We are warning residents to be on their guard after received reports of doorstep cold callers in the Hethersett area offering driveways services.

This follows an incident in which a man cold called at a property claiming that 'as they were working in the area' he could offer 'discounted block paving or tarmac driveways for cash'.

The resident declined the offer and reported the incident to us.

Our advice is to **never** deal with anyone who cold calls at your property offering to do work on or around your property. It is possible these cold callers could move on to other areas within Norfolk.

Anyone concerned about doorstep cold calling activity in Norfolk can contact us through our partners the Citizens Advice consumer helpline on **0808 223 1133**.

Looking for a Trader you can Trust? Try a Norfolk Trusted Trader. To search our directory and read feedback from their customers visit www.norfolk.gov.uk/trustedtrader

Could your community help stop doorstep cold callers from targeting vulnerable people by becoming a No Cold Calling Zone? To find out more about the scheme or to apply visit www.norfolk.gov.uk/nccz

Scam Alert – Online scammers selling pets – 2 June 2020

Criminals continue to take advantage of the coronavirus pandemic to commit fraud, including scams involving the purchase of pets, such as puppies and kittens.

Scammers post adverts on social media, general online selling platforms and specific pet selling platforms with buyers being persuaded to place deposits for pets immediately to secure the pet of choice.

But the criminals posting these adverts never have any animals to sell. They use the COVID-19 and social distancing as a reason why the victim cannot come and see the animal first or pick it up.

After the initial payment more and more funds will be requested to cover insurance, vaccinations and even delivery of the pet.

To help protect yourself from scams like this:

- Do your research - Before purchasing anything online, including pets, look up reviews for the site, or person, you are buying from. If you're still not sure, ask a trusted friend or family member for their advice
- Trust your instinct - If you can't physically go to see the animal in person, ask for a video call. If the seller declines, challenge them on why. If you have any suspicions, don't go ahead with the purchase
- Choose your payment method wisely – if you decide to go ahead with the purchase, avoid paying by bank transfer as that offers you little protection if you become a victim of fraud. Instead, use a credit card or a payment service such as PayPal

More information is available on the Action Fraud website.

Rogue Trader Alert – Doorstep cold calling incidents – 1 June 2020

We are reminding residents to be on their guard to doorstep cold calling even if they are displaying a No Cold Calling sticker.

This follows a number of recent reports from residents who have had cold callers at their door despite displaying a sticker, with some reporting that the callers can be difficult to turn away and, in some cases, verbally aggressive when the presence of the sticker is pointed out.

Recently the ongoing COVID-19 situation has led to reports of doorstep cold callers claiming to be offering help to vulnerable residents or calling for health related reasons.

We are asking residents to report ALL doorstep cold calling incidents to us, especially if their property is displaying a No Cold Calling door sticker of any type. We are also offering the following advice:

- If someone cold calls at your property, remember it is your doorstep so your decision whether you even answer the door. If you can, check through a spy hole or look from a window to see who is there
- Think about your home security, make sure other doors to your property are locked before answering the front door
- If the person is offering services or trying to sell something politely but confidently say you are not interested and close the door

- If the person is claiming to represent an authority, organisation or charity ask to see ID. If ID is offered, ask if you can take it to check its validity. If you are given the ID close the door and contact the company or organisation on the ID by a number you find online or in the phone book, **do not** use information on the ID, it could be fake

If no ID is offered, the caller refuses to let you check it, or you cannot verify it is genuine, politely but confidently say you are not interested and close the door.

As the cold caller leaves, if you can, safely from inside your property watch and see:

- Do they go to call at neighbouring properties
- Do they return to a vehicle, is it sign-written, can you see the make, model, colour and registration plate
- Are they alone or working with others

Note down a description of the cold caller, why they were calling and who they said they were representing – all of this information is very useful to us and the police when looking at cold calling incidents

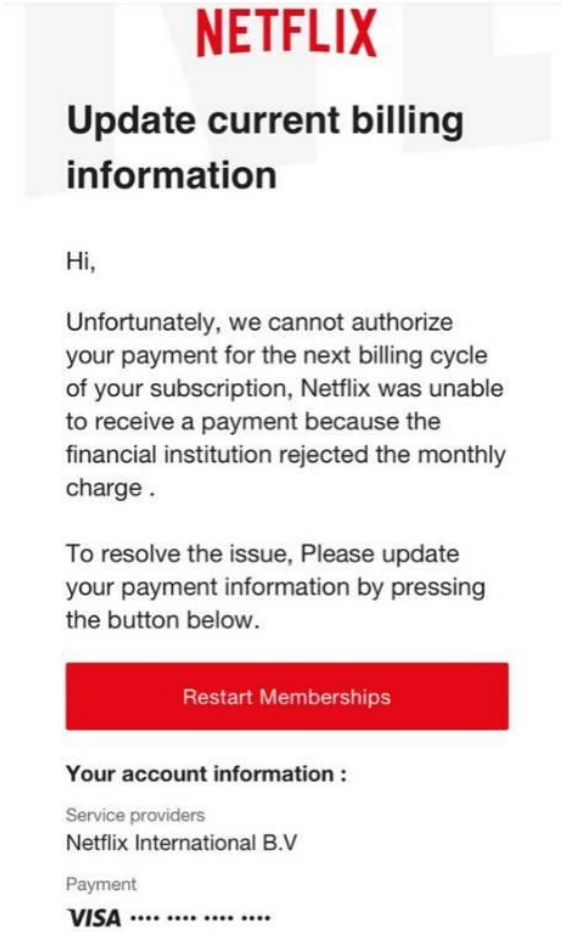
You can report doorstep cold calling incidents to us via our partners the Citizens Advice consumer helpline on **freephone 0808 223 1133** or to Norfolk Constabulary on **101**. In an emergency always dial **999**.

If you would like one of our No Cold Calling door stickers call our customer service centre on **0344 800 8020**.

Why not consider setting up a No Cold Calling Zone in your community? You can find out more about our scheme at www.norfolk.gov.uk/nccz

Scam Alert – Emails claiming to be from 'Netflix' – 29 May 2020

Since the beginning of lockdown, scammers have been exploiting the popularity of streaming services, and the increase of those that have signed up to the many services available.



There has been a dramatic rise in suspicious domains impersonating a variety of streaming giants, with a great many phishing emails, text message and fake adverts pointing to them to attempt to steal your money.

The data harvested on these spoof websites includes names, addresses and other personal information, as well as stealing credit card or banking details for financial gain.

Our advice is **always** be wary of claims made in unexpected email approaches and **never** click on links or open attachments if approached in this way.

Netflix offer the following advice regarding scam emails:

How do I know if an email or text is actually from Netflix?

Keep the following in mind to determine if it's from us:

- We will never ask for your personal information over email. This includes:
  - Credit card number
  - Bank account details
  - Netflix password
- We will never request payments via a third party vendor or website

What should I do if I received a suspicious email or text?

Scammers can’t get any information from you unless you give it to them.

If you received a suspicious email:

- **Don’t click** any of the links or open any of the attachments
- **Forward** the email to phishing@netflix.com
- **Delete** the email

You can report suspicious emails received to us via our partners the Citizens Advice consumer helpline on **freephone 0808 223 1133**.