The following is a Police Connect message.

Please find below the latest Consumer & scam alerts from Norfolk Trading Standards.

Kind regards

PC Pete Davison
North Norfolk Community Engagement Officer

Scam Alert – Social Media messages claiming to be from ‘Dominos’ offering ‘2 Large Pizza for Free’ – 26 May 2020

Be aware of social media messages claiming to be from Dominos offering ‘2 Large Pizza for Free’. It’s a scam.

Scammers are continuing to use the coronavirus pandemic to spam people with claims that these offers are ‘supporting the Nation’ during this time.

If you get a message like this, do not interact with it in any way and do not like or share on your social media profile.

Scam Alert – Facebook Messenger asking to borrow money – 22 May 2020

We are warning Facebook users to be aware of messages from existing Facebook friends sent via the Messenger service which asks to borrow money.

The message will give a reason why the money is needed ‘urgently’ and will be followed by further messages pressuring the recipient into sending the money.

These messages come from a Facebook friend’s account but are actually sent by fraudsters who have hacked the friend’s Facebook account and taken control of it.

If you receive this or a similar message via Messenger, do not interact with the message and contact the friend via another route if possible. Advise them their Facebook profile may have been compromised.

Find out more about keeping your Facebook account secure, including activating login alerts and two-factor authorisation.

Scam Alert – Further examples of scam text messages claiming to be from PayPal – 28 May 2020

With more people ordering items online, we are warning residents about scam text messages claiming to be from PayPal.

A recent example says that ‘you have (1) important unread message’. The message then provides a link to ‘view & resolve the current issue with your account’.

These text messages are not genuine and are not connected with PayPal.

If you receive this or a similar text message, delete it without clicking on any links.

If you are concerned about the security of an online account, contact the provider directly via their genuine website or app.

Never use links or details provided in a text message.

You can report suspected text message scams to us via our partners the Citizens Advice consumer helpline on freephone 0808 223 1133.

News Alert – Norfolk Against Scams Partnership launch anti-scamming campaign during Covid-19 – 21 May 2020

Agencies from across Norfolk have come together to warn residents to be extra vigilant of new and existing scams during the Covid-19 pandemic. A three-week campaign is being headed up by the Norfolk Against Scams Partnership, with a membership comprising Norfolk County Council’s Trading Standards, Norfolk Constabulary, the Office of the Police and Crime Commissioner (OPCCN), voluntary agencies, businesses and residents.

There will be a different focus on partners’ social media platforms each week, using the hashtag **#NorfolkScamAware**:

- **Trusted information** – to guide the public to useful information and support agencies.
- **Protect** – to give advice on how people can better equip themselves to identify the signs of scamming.
- **Watch Out** – to make victims aware of the Norfolk Scam Prevention Service and the new scams that have emerged due to the Covid-19 pandemic.

If you’re on Facebook or Twitter search for the hashtag #NorfolkScamAware and share some of the information with your family, friends, neighbours and in the community where you live.

Scam Alert – Emails claiming to be from ‘TV Licensing’ – 20 May 2020

There continues to be a range of emails circulating claiming to be from TV Licencing.

Recent examples have included emails claiming to be a ‘COVID19 Personalized Offer’ stating you are eligible for ‘1 x 6 months of free TVLicence’.

These emails are **not** from TV Licencing and any links contained within the message are likely to go to a genuine-looking fake version of the TV Licencing website which will attempt to gather personal and financial details.

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.

TV Licensing offer the following advice to help spot scam TV Licence emails:

- Check the sender's email address - TV Licensing will only send emails from donotreply@tvlicensing.co.uk (or donotreply@spp.tvlicensing.co.uk)
- Check how scammers address you - genuine TV Licensing emails will always use your title and last name. Scammers may simply use your email address, say 'Dear Customer' or nothing at all
- Check links in the email - do not click on links or attachments. If you're unsure, you can inspect links first. On a computer, hover over the link with your mouse (but don't click it). On a mobile or tablet, press down and hold (don't release while on the link)
- Check addresses of any websites it takes you to - scammers can't use 'www.tvlicensing.co.uk' for copy-cat sites. They'll try to disguise this so carefully inspect the full address in the browser bar

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

Information Alert – EasyJet Cyber Incident – 19 May 2020

EasyJet has confirmed that it had suffered a cyber-attack and is in the process of contacting affected customers following the incident.

The National Cyber Security Centre (NCSC) has issued the following advice for EasyJet customers:

- Anyone who thinks they have been a victim of online crime can report a cyber incident using Action Fraud's online fraud reporting tool anytime of the day or night or call 0300 123 2040. For further information visit www.actionfraud.police.uk
- If you're an EasyJet customer, we recommend changing your password on your EasyJet account – and if you know you've used that password anywhere else, change it there too. The best way to make your password long and strong is by using a sequence of three random words you'll remember

There is more information on the NCSC website:

- Now would also be a good time to check if your account has appeared in any other public data breaches. Visit haveibeenpwned.com, enter your email address and go from there
- Two-factor authentication (2FA) is a free security feature that gives you an extra layer of protection online and can stop cyber criminals getting into your accounts - even if they have your password. If it is available, then we suggest using it on all your important accounts
- If your account has been compromised, your personal details may be used to help craft more convincing scam emails. If you believe you have received a suspicious email then you can report it to the NCSC using the Suspicious Email Reporting Service (SERS) but the NCSC has produced advice which will help you spot the most obvious signs of scam emails
- EasyJet confirmed that 2,208 credit card details were accessed in this incident. If you were one of them, you should be notified of this by EasyJet. We advise that you monitor your accounts for any unusual activity and if you're worried, get in touch with your bank's fraud department. There is more information on the NCSC website

Scam Alert – Further reports of telephone cold callers claiming to be police officers – 19 May 2020

We have received a further report of a Norfolk resident receiving a telephone cold call claiming to be from a police officer.

In this incident, the male cold caller claimed to be a police officer from the 'Met Police' and stated he was calling

about the resident's bank card which 'had been breached'.

During the call the male also mentioned 'the Serious Fraud Office' and 'the Flying Squad' as being involved. He then said the resident should 'call 999 immediately' to 'verify his information'.

Courier fraud happens when a fraudster contacts a victim by telephone claiming to be a police officer, bank or from a government department, among other agencies. Several techniques will then be adopted in order to convince the victim to hand over their bank details or cash, which may then be passed on to a courier.

Residents are reminded that neither your bank nor the police will **never** ask you to withdraw money or purchase items.

If you receive this or a similar call **do not** follow the instructions given. Instead:

- Hang Up
- Either wait five minutes for your phone line to clear, use a mobile phone or a different phone line; and
- Call and report to Norfolk Police via 101

In an emergency always call **999**.

Please continue to share these warnings and advice with family, friends and anyone within your community who could be vulnerable to this type of approach.

Scam Alert – Text messages regarding ‘Cervical Screening’ – 18 May 2020

We are again highlighting a warning after some women reported being contacted by text message, with the sender claiming to be from the ‘call and recall service’ to advise that ‘they are overdue for screening’.

The message then states you need to call a mobile number and provide personal details.

These messages are **not** from the NHS Cervical Screening Programme. If you receive this message **do not respond or call the number**.

Contact when it is time to book your cervical screening appointment will be sent by post. This letter will tell you where you can go for cervical screening and how to book.

Speak to your GP surgery if you have questions about cervical screening invitations, results or any symptoms you have.

You can report suspicious text messages to us via our partners the Citizens Advice consumer service on freephone **0808 223 1133**.

Scam Alert – Telephone cold calls claiming to be from ‘Amazon’ – 18 May 2020

We are again warning residents to be on their guard for telephone cold calls claiming to be from ‘Amazon’.

This follows a report from a Norfolk resident who received a call which delivered a recorded message stating, ‘this is Amazon’. The message then went on to say that ‘your Amazon Prime is about to be renewed and a payment of £79.99 will be taken from your bank account’. The call then claimed that you could ‘Press 1 to speak to an Amazon Service Manager to discontinue this’.

These calls are a scam and are **not** connected with Amazon in any way. If you receive this or a similar call our advice is **do not** interact with the call and hang up.

If you have received a telephone cold call which you believe to be a scam you can report it to us via our partners, the Citizens Advice consumer helpline on freephone **0808 223 1133**.

To manage your contact details, additional information and subscriptions, please login through the member portal.