North Yorkshire Police Monthly Fraud Newsletter

Hello and welcome to August's monthly fraud update newsletter for North Yorkshire. Apologies this month is a little late and yes I acknowledge that it is now September!

We've had a couple of scams see a resurgence in our region these last few weeks so you'll find warnings about them below, along with some advice to keep yourself and your loved ones safe.

If you have any suggestions for future content you think would be useful in these newsletters or general feedback then we'd really like to hear from you! You can email: Carys.Samuel@northyorkshire.police.uk

Scams of the month

Gift card scam

An email is received which appears to be from a friend or colleague asking you to buy a number of gift cards - Google or Apple Pay. The email will usually be from someone you know (their email may have been hacked) and explains they can't buy the gift cards themselves because they are in a meeting or can't get to the shop but that they will pay you back as soon as they can.

The email will also likely ask you to photograph the cards once purchased and send them photos of the unique codes printed on each card.

This allows the scammer to use the gift cards to make online purchases and needless to say you will never see your money again.

Typically the value of the gift cards is around £500.

If you receive an email like this, do not purchase any gift cards. If it is from someone you know, ring them to check if the request is really from them and if not then they need to be alerted their email may have been hacked.

Phishing email scam targeting businesses in our region

A phishing email scam is currently in circulation which indicates the recipient has files to download and that they should login using their employee credentials to

access the files.

The emails reported so far appear to be from one of a number of law firms but could appear from any organisation which may have been compromised so please be very cautious.

If you receive any email which asks you to login to a system to view or download files, don't click the link without considering:

- Were you expecting this email or has it come out of the blue, even if it is from a known sender?
- Have you ever previously been asked to login to a system to view/download files?
- Are you able to verify with the sender by phone or in person that the email is genuine?

If you receive a phishing email at work, you should notify your IT department. If you don't have an IT department you can forward phishing emails to report@phishing.gov.uk

If you think you may have received an email like this and provided your credentials by logging in to a system, let your IT department know immediately. Reset your password and if you can, enable two/multi-factor authentication (2FA/MFA) on your account as this will help to protect you if your details have been compromised.

You can find more information on keeping your details and your business safe by visiting the National Cyber Security Centre: www.ncsc.gov.uk

If you have been a victim of a cyber-attack, call us on 101.

Counterfeit vaccine passports

Now that travel and entertainment venues are opening up again, many places require proof of vaccination status in the form of an NHS Covid Pass. These can only be obtained via the NHS website, NHS app or by calling 111.

We've heard some reports from around the UK that fraudsters have been posing as NHS employees and offering fake Covid 'passports' in return for a fee. People have been contacted by email with a link redirecting you to a fake but convincing 'NHS' website where you're asked to put in your personal details.

One of these fake websites has been taken down but you can be fairly sure this scam will rear its ugly head again so be vigilant and if you receive an email like this, delete it immediately.

This month, learn how to: keep safe from holiday frauds

The school summer holidays might be coming to a close but many of us will still be looking to get away from it all, whether booking for the coming weeks or planning

ahead to October half term.

Here's some tips on making sure you keep safe and your dream holiday doesn't turn into a nightmare:

- Don't reply to unsolicited emails, texts, social media or calls with holiday offers. Links and attachments in emails may lead to malicious websites or download viruses.
- Book a holiday directly with an airline or hotel, or through a reputable agent. Check whether they're a member of the Association of British Travel Agents.
- If you decide to deal directly with the property owner or a letting agent, ask them questions about the booking, room, location and area.
- Don't book on websites that don't have a padlock icon (https) in the address bar, and be extra cautious if you're asked to pay using bank transfer or cash; pay by credit or debit card if you can.
- Check reviews before you book, you can search online for these. If a holiday destination doesn't have any independent reviews, be very suspicious and do your best to conduct further checks before booking.

If a deal looks too good to be true then it probably is! Trust your instincts.

Ways to get involved
If you are organising an event and would like our police volunteers to attend to give fraud prevention advice and materials, please email Andy Fox on andy.fox@northyorkshire.police.uk

Can you share our safety posters? You can download them from our website here: https://northyorkshire.police.uk/stayingsafe/fraud/22887-2/ or email carys.samuel@northyorkshire.police.uk if you need printed copies.

If your community organisation or group would like to arrange a virtual fraud prevention talk then email our Financial Abuse Safeguarding Officer, Andy Fox on andy.fox@northyorkshire.police.uk and he will be happy to help.

If you know anyone who would like to be added to our distribution list please email: carys.samuel@northyorkshire.police.uk

As always, if you need to report a crime or scam please call 101 or 999 if it is an emergency.

Message Sent By
Carys Samuel (Police,Corp Comms Manager,North Yorkshire)