JULY 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud newsletter for NHS staff. We hope that you find the contents useful. If you need any advice on fighting NHS fraud, you can find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.

IN THIS EDITION

Fighting Phishing

Many cyber fraudsters use phishing as an easy way to target lots of people at once. Phishing emails are usually designed to look as though they have come from someone you know or trust.

They will often contain a link to a malicious website that has been disguised with logos / branding to make it look legitimate.

Suspicious emails can be reported via the following routes:

- If the email has landed in your @nhs.net email account, please forward it as an attachment* to spamreports@nhs.net
- If the email has been sent to a non-NHS email account, please forward it to report@phishing.gov.uk

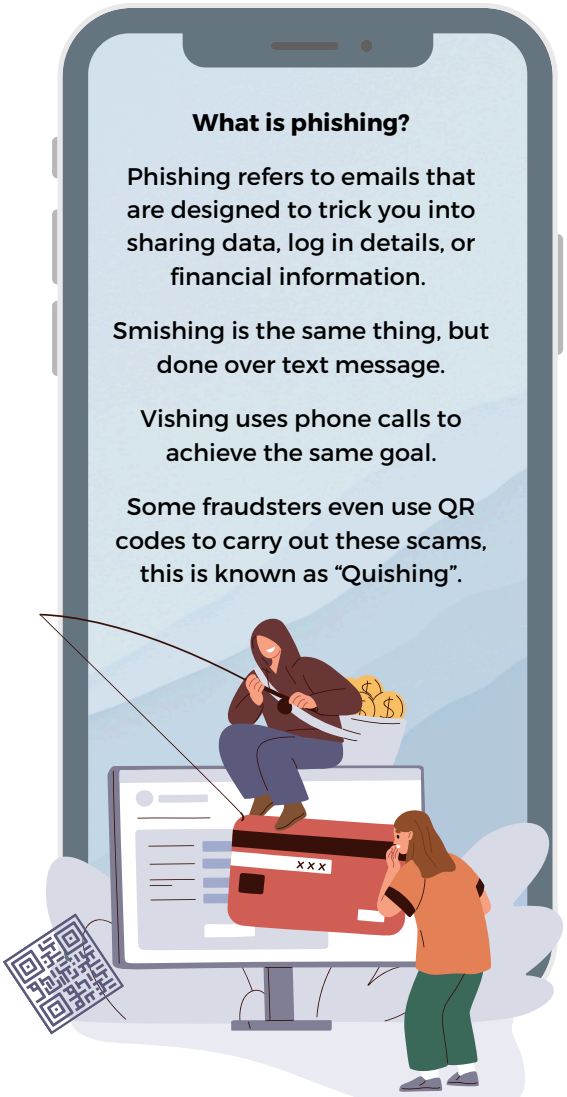
Action Fraud have recently announced that **over 32 million** dodgy emails were reported to the report@phishing.gov.uk service since it launched. A third of all reports were made in the last 12 months.

As a result of these reports, **329,000 malicious websites have been taken down** and prevented from claiming more victims.

Suspicious text messages can be forwarded to 7726, free of charge. Phone companies can then investigate the sender and block the number from targeting other people.

For more on this topic, please visit the Action Fraud website: https://www.actionfraud.police.uk/news/phishing

*For information on how to "forward as an attachment", see page 3,



Scam Trends

Courier Scams

Action Fraud have revealed that fraudsters stole over £28 million last year using courier scams. Victims lost **an average of £20,032** and the majority of victims were in their 80s. This scam tactic can be used against anyone.

Courier scams often begin with a cold call from a fraudster, who claims to be calling from your bank's fraud team, the police, or another trusted authority.

The caller will claim that there has been an unauthorised transaction on your account, that there is a current investigation that your help is needed with, or that your financial details have been compromised.

They will then talk you through steps they want you to take to "protect" your money. This may include withdrawing a large amount of cash, taking out foreign currency or purchasing a high value item. The cash or item is then collected by a courier and is ultimately handed over to the fraudster and their associates.

Some courier fraudsters have told victims to contact the phone number on the back of their bank card in order to verify that the call is genuine. However, these fraudsters used a piece of software to jam the victim's phone line - meaning what the victim thinks is a new outgoing call is actually connected to another fraudster.

Protecting Yourself and Others from Courier Fraud

Your bank and the police will never ask you to withdraw cash or purchase high value items.

To verify if a call is genuine, hang up and then either use a different phone or wait for 20 minutes before calling the number on the back of your bank card. This will help you to avoid line jamming software.

Your bank may also offer a web-chat function where you may be able to get some quick advice without using the phone.

If the caller claims to be police, ask for their name, collar number and which force they work for. End the call, wait for 30 minutes or use a different phone to call 101. You can ask to be connected to any police force which will allow you to check if the call was genuine.

If you have vulnerable friends or family members, consider encouraging them to sign up to the Telephone Preference System and installing a call blocker to manage unsolicited calls.

Call Forwarding Scams

Scammers are adding another layer of misery to victims of fraud by setting up call forwarding services on their mobile phone. In this fraud methodology, it is likely that your details will have been stolen in some other kind of fraud, usually one which has allowed the fraudster to access your bank account.

The criminals will then phone you up, pretending to be from your bank. They will tell you that you need to enter a code into your phone in order to continue to receive information from them. This code is commonly seen to be *21* or *401* followed by several other numbers. This will enable the fraudster to set up a call forwarding service and answer any future calls pretending to be you.

With the information they already have, they will make some transactions out of your bank account. Unfortunately, when your bank calls to check if you have authorised the payments, the call goes to the fraudster who tells them that they are legitimate.

If you receive a call from a bank asking you to input a number into your phone, end the call, then use a different phone or wait 20 minutes, then call your bank using a number you know to be them, such as from your bank card or their internet site, to check that if the call was genuine.

This scam has also been seen in fake failed delivery phone calls, where somebody will call you pretending to be from a delivery company customer services asking you to input a code to receive delivery updates.

Warning about Fake Police Scams

We often refer to the lengths which scammers will go to in order to fool us. If you missed the article on BBC news about fraudsters masquerading as Chinese police, it's worth a read. The article can be found on the BBC news website here - Scammed by the fake Chinese police. We have summarised the key points of the article below.

A British-Chinese woman was contacted by the fraudsters who initially told her that an illegal package had been stopped in customs with her named as the sender. She was then told she was being investigated for fraud.

The scammers sent her 'evidence' which allegedly proved her involvement in the crime. They then video called her and the fraudsters were wearing official uniforms and even took her on a virtual tour of a supposed police station.

The unscrupulous conmen told the victim that she wasn't to mention this to anybody or she would serve an additional 6 months in prison. They made this appear to be official by making her sign a confidentiality agreement. Additionally, they made her download an app so they could monitor her phone remotely.

To avoid being imprisoned in China, she paid them her life savings as 'bail'. However, they then demanded a further £250,000 to avoid her extradition to China.

It was when she tried to borrow money and confided in her daughter that she was made aware that this was a scam. Luckily her bank has refunded her.

In other cases, it has been reported that victims have been told to fake their own kidnappings to raise ransom money from their families.

The Chinese Embassy have issued worldwide warnings about not sending information or money if you are accused of a crime you haven't committed. Australian police have also issued warnings about cyber kidnappings.

Reminder

If you are in doubt about whether a phone call is genuine, hang up. Fraudsters who call potential victims are often very well-practiced and can go to significant lengths to trick you into moving money or sharing info.

After you have hung up, use a different phone to call your bank or Action Fraud for advice (0300 123 20 40)

Cyber Skills - How and why to "forward as an attachment"

If you are using an @nhs.net email address, and receive a suspicious email, you can forward it to spamreports@nhs.net.

This is a central inbox which is managed by NHS Digital. When you send a suspect email to this address, the team ask that you forward the email "as an attachment".

Doing this means that the NHS Digital team get all the data behind the dodgy email (such as the sender's IP address). This gives them as much information as possible to take effective action.

NHS Digital can take action such as blocking the sender from being able to contact @nhs.net email addresses or adding phrases / links to the filters. This greatly reduces the risk of another member of staff being caught out.

Forwarding an email as an attachment is easy once you get the hang of it! There are a few different ways of doing it, depending on which version of Outlook you are using.

If you use the desktop version of Outlook:

- Select the suspect email in your inbox.
- At the top of your screen you will see your Response Options - Reply, Reply All and Forward.
- Just to the right of these is a small button marked "More" or an icon that looks like this:

- Click the button and select "Forward as Attachment"
- Send the email to spamreports@nhs.net.

If you use the webmail version of Outlook::

- Select the suspect email in your inbox.
- At the top of your screen you will see arrows representing your Response Options - Reply, Reply All and Forward.
- To the right of these is a small drop down button:

- Click the button and select "Forward as Attachment"
- Send the email to spamreports@nhs.net.

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy,.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.