Counter Fraud Newsletter – April 2022

Welcome to the April 2022 edition of our Counter Fraud Newsletter for NHS staff. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, you will find our details on the last page.

Current Scam Trends

Energy Bill Scam Warning

As we all face rising energy bills, there is a likelihood that fraudsters will look to exploit the situation. These scams often begin with a phishing email which claims to be from an energy company.

The email may look convincing and feature the company's normal logo and branding, along with a link which it claims will take you to their official website. The email may try to lure you into following the link by promising a refund or rebate on your bill, or try to panic you by saying there's a problem with your payment method and penalty fees are about to be applied.

If the link is followed, the recipient will be asked to enter personal and financial information on the fake website in order to log into their account or to prove their identity. Once the fraudster has collected this information, they can then use it to try and take money from your account.

In some scams, the fraudster will contact the target after a few days or weeks, claiming to be from their bank's fraud team. They will even reference the dodgy email and claim that the customer now needs to move their money into a "safe account" to protect it from fraud. They may even use spoofing software to make it look like they're calling from the bank's customer services number.

Please remember to treat unsolicited emails with caution, even if they appear to be coming from a real company that you have a relationship with. It is worth taking time to check that the email has come from a genuine account, but do remember that official email accounts can be impersonated or hijacked.

Martin Lewis has recently advised people to look out for similar scams using the Council Tax rebate as a hook to lure victims in. The best way to verify that an email is genuine, is to contact the company or organisation using their official customer services number. Which have published an interesting video which shows their reporter dealing with an energy scammer on the phone.

WhatsApp Voicemail Phishing Email

A phishing campaign which impersonates WhatsApp's voice message feature has been spreading information-stealing malware. The attack starts with an email claiming to be a notification from WhatsApp of a new private voice message. The email contains a creation date and clip duration for the supposed message, and a 'Play' button.

The identity 'Whatsapp Notifier' masks a real email address belonging to a Russian road safety organisation. As the address and organisation are real, the messages aren't flagged as spam or blocked by email security tools. Armorblox, who discovered the scam, believe the Russian organisation is playing a role without realising.

The 'Play' button will take the email recipient to a website which then asks them to click 'Allow' in an allow/block prompt to 'confirm you are not a robot'. Once 'allow' is clicked, the browser will prompt to install software that turns out to be information-stealing malware. Please be cautious when using WhatsApp or any other software and be on the lookout for unusual messages.

National Cyber Security Centre Advice

The National Cyber Security Centre (NCSC) has published some very useful advice on spotting scam messages after Cadbury's warned of an online scam. Look out for these warning signs:

· **Authority -** does the message claim to be from someone or an organisation that you trust?

· **Urgency** - does it imply that you need to respond within a limited amount of time, or immediately?

· **Emotion** - does the message make you feel panicked, fearful, hopeful, or curious?

· **Scarcity** - does the message claim something is in short supply in order to make you fear missing out?

· **Current events**— does the message refer to current events in order to seem more convincing?

Any of these tactics can be used to try and manipulate you into doing something you wouldn't normally do. Fraudsters simply adapt their established scams to fit whatever is in the press — e.g. energy price rises, global unrest, emerging Covid variants/changes to restrictions and testing routes etc.)

Sensitive and Personal Phishing Emails

As people become more aware of phishing tactics, fraudsters are upping the ante to coerce you into parting with your hard earned wages.

A member of staff at one of our organisations has received an email in which the sender claims to have downloaded spyware onto her computer. They claim that they have evidence of the staff member viewing websites of an adult nature and have images taken of her doing this. They threatened to expose this to her contacts unless she contacted them. The sender also included links to alleged videos as 'proof'. Scammers of this nature will tend to try and add credibility to themselves by providing technical details.

Some of the more sophisticated scams of this nature have recently included the receiver's password to make them believe that they have had access into their devices. The passwords have likely been obtained in a previous data breach.

Had she made contact, it is likely that the sender would have made extortionate financial demands in exchange for destroying the evidence. Previous similar cases have shown that if a payment is made, they will continue to ask for more and more. The sender is relying on the receiver to feel too embarrassed or ashamed to report this, even if they haven't been accessing inappropriate sites.

This kind of scam is not new but it is the first which has been seen by the Counter Fraud Team sent to a work email address. Remember that you are a victim and the sender is relying on creating a sense of panic to get you to engage with them. They do not know what activities you have been up to, but just one person taking the bait will be a very good pay day for them.

If you receive an email of this kind at work, please contact your IT department immediately.

You can check whether your passwords have been breached here: Have I Been Pwned: Check if your email has been compromised in a data breach. You can find out more about this methodology, which is also known as "sextortion" below.

Sextortion (webcam blackmail) - National Crime Agency

Sextortion emails: how to protect yourself | Action Fraud

Cyber Security – Remote Access Software Warning

Action Fraud have advised that **more than £50 million** was lost last year to scams where victims were tricked into handing over control of their computer or smartphone to criminals**. 20,144** people fell victim, with an average loss of **£2,868** per victim.

Remote Access scams could start with a browser pop-up saying that your computer is infected with a virus, or you may receive a call from someone claiming to be from your bank saying that they need to connect to your computer in order to cancel a fraudulent transaction on your account.

The fraudster's goal is to steal your money or access your financial information to obtain goods or services for themselves. They do this by persuading you to let them remotely access your device using Remote Access Software (such as Team Viewer, AnyDesk, Remote PC etc.).

These Remote Access programmes are really helpful if you have a genuine problem with your device and you're speaking to IT, for example. It enables those with the technical know how to fix issues from a distance.

Unfortunately, fraudsters are very good at impersonating trusted organisations, such as banks, or IT support companies. They also use the same legitimate software to facilitate their crimes. Once they have remote access to your device, they can deploy malicious software directly onto your computer. They may also persuade you to log into your online banking so that they can "check" for evidence of fraudulent activity. They then use the access to empty your accounts.

- Remember, a bank or service provider will never contact you out of the blue requesting remote access to your device.
- If you feel that you have been targeted contact your bank or the service provider immediately on a different device from the one the scammer contacted you on.
- Only use existing contact information from genuine documents or following a Google search (don't rely on any contact info given by the fraudster). Your bank will have a 24 hour helpline so that you can contact them outside of normal hours. This is usually found on the back of your bank card.
- You can also report attempts to use this tactic against you to Action Fraud on 0300 123 2040 or via actionfraud.police.uk.

In the Press

Practice Manager admits fraud after paying herself £18k in unauthorised overtime

Julie Ann Stevenson was the practice manager for a GP surgery in Neath. Over a period of around two years, she had accessed the practice payroll system and made £18,000 worth of unauthorised overtime payments to herself. The fraud was uncovered when the practice found that they had insufficient funds to be able to pay staff wages. It was also found that she had raised her own rate of pay several times over the same time period. Stevenson has been issued with a suspended sentence and has also been ordered to pay costs of £1,000.

Fraudulent practice manager brought to justice by NHS counter fraud investigation. (cfa.nhs.uk)

Jail sentence issued following £80k worth of false expense claims

Tanya Tucker worked for the NHS and Unison, and falsely submitted a large number of expenses claims. She has been found guilty of 7 fraud charges after a two week trial, and has been sentenced to 28 months imprisonment.

Tucker claimed identical expenses from both her NHS employer and the union and signed off cheques made out to herself by forging her colleagues signatures. She spent the money on a car, meals out, holidays, beauty treatments and to pay for her honeymoon.

'Brazen' Bishop Auckland Unison official jailed for £80k con - BBC News

Bribery conviction for Chief Information Officer who abused his position (non NHS)

Brian Chant worked as Chief Information Officer (CIO) at an Oxfordshire-based company. Chant used his role to push for a £22 million contract to be awarded to a specific IT company.

A HMRC investigation identified that the IT firm had reclaimed VAT for services from a company called "Chant Consulting Ltd.". It was also uncovered that Chant was a director of the consultancy firm. This prompted further investigation due to Chant's role in promoting the firm for the high value contract.

A review of Chant's computers, emails, and bank accounts highlighted that Chant had orchestrated the contract being awarded and had received over £474,000 in payments from the IT company. He has been found guilty of bribery and false accounting, and has been sentenced to six years imprisonment.

Former executive officer jailed for £22 million IT contract plot | City of London Police