Counter Fraud Newsletter January 2024

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful.

Don’t Take the Bait

Have you ever heard of a scam called “baiting”? This scam involves placing USB sticks (the bait) in public places like cafes or car parks, hoping people will pick them up and connect them to their own devices.

Here's how it works: scammers leave USB sticks in public spots with tempting labels like "Free Music" or "Important Files."

When curious individuals pick them up and connect them to their computers, they unknowingly let harmful software in. This can lead to serious problems, like stealing personal information or installing ransomware.

To stay safe from baiting scams, remember these tips:

- Don't plug in unknown devices: avoid connecting random USB sticks or other gadgets to your computer.
- Turn off auto-run: disable automatic program execution when you connect external devices to your computer.
- Educate your team: make sure your colleagues know about the risks of connecting unknown devices at work.
- Follow company rules: stick to your workplace's IT policy, and report any suspicious devices to your IT department.
- Update your security software: keep your antivirus and anti-malware tools up-to-date for added protection.
- Report strange devices: If you find a USB stick in public, don't connect it. Instead, tell the authorities or the place's management.

By being careful and following these tips, you can reduce the chances of falling for baiting scams and keep your devices and information safe.

You can read more about baiting here: https://www.makeuseof.com/what-is-a-usb-drop-attack/

Current Scam Trends

Salary Sacrifice Scam Alert

The Counter Fraud Team have been made aware of a scam where a fraudster used stolen NHS staff credentials to buy items through a salary sacrifice scheme. Goods were purchased without the staff member’s knowledge, and payment was taken from their monthly salary. The items ordered were delivered to the fraudster, so the victim only found out when they checked their pay slip and spotted unexpected deductions.

Thankfully this has only happened a few times, but it does highlight the importance of checking your pay slip even if you’re not expecting to see a different amount.

- Never share your ESR / email log in details with anybody else.
- Make sure to use strong and unique passwords for different accounts - including your email and ESR accounts.
- If you take advantage of a salary sacrifice scheme, have yet another password for that system. For more on this, please see the password advice article on the next page.
- Check your pay slips monthly and report anything unusual.

- If you print your pay slips out, shred or destroy them before discarding them to prevent anyone stealing your details.
- If you email your pay slip to yourself, we advise that you password protect it so that nobody else can open it.
- If in any doubt, please speak to your Local Counter Fraud Specialist (our contact details are in your organisation's Anti-Fraud, Bribery and Corruption Policy).

Lottery Scams

Lottery scams are also known as prize draw or sweepstake scams. This type of scam usually starts with a letter, email or phone call claiming that you have won a substantial amount of money in a lottery.

Common lotteries named in this scam are Australian, Spanish or Canadian. The caller will usually say that they are an official at the lottery and will try to put you under a lot of pressure to act straight away or risk losing your winnings.

The scammers will either ask you to send them a copy of your passport or other personal information for 'proof of identity', and / or ask you to pay some kind of fee before they can release your prize.

If you do make a payment, the criminals will often ask for more, coming up with excuses for each charge. In some cases where banking details have been requested, instead of crediting the victim's account with the prize fund, the account has been emptied.

To prolong the crime, if a person has been coerced into handing over money or their details, the scammers will sometimes then pretend to be from their bank or law enforcement and offer to help them recover the lost money. Throughout this phase, the fraudsters may encourage the victim to transfer their remaining money into a "safe account" which is controlled by the criminals.

It is often easy to spot this as a ruse if you haven't actually purchased a lottery ticket. You can't win a competition you haven't entered.

However, if you do enter lotteries or online competitions, it is harder to spot this type of scam. If you are contacted by someone claiming you have won a prize, be very wary and do not share your financial information.

Contact your bank immediately if you are concerned you've shared your bank details with a fraudster. You can find more information and advice on this type of fraud on the Action Fraud website.

Cyber Security

Setting Good Passwords

The start of a new calendar year can be a great time to start fresh and update your passwords. You'll often hear the Counter Fraud Team advising that you need to make sure you use strong and unique passwords.

Why do passwords need to be unique?

A survey run by Google in 2019 found that 65% of people were reusing the same password for multiple accounts. When you consider how many different systems and services we log into, it's understandable that people often find it easier to rely on a single password that they are really familiar with. However, this is a big risk.

The danger comes when one of your accounts is breached. If a company that holds your data is targeted by cyber criminals, your log in credentials could end up being stolen and sold on. If you rely on a single password, accounts you hold elsewhere can also be hijacked.

For example, let's say that Company A is hacked, and your username and password are stolen. The cyber-criminal is able to log into your account with Company A to look for more information - such as the email address linked to your account.

They try your password to see if they can get into your emails. If they get into your email account, they can go round lots of other services and reset your password, locking you out of your accounts. If you don't have the same password for your emails, you might think they'd just give up and move on.

However, they haven't quite finished. They will try logging into popular services - such as Amazon, PayPal, eBay, social media platforms etc. using your email address and the password that Company A lost.

Any account which they manage to access gives them an opportunity to gather more information on you. Some accounts will also contain saved payment information, which can be used to place unauthorised orders.

For example, if they get into your Amazon account they can use your saved details to place high value orders which they could arrange to have delivered to Amazon lockers. They would also be able to steal your address which may help them to carry out identity theft.

Hopefully this example highlights why having unique passwords is so important.

How do you set a good password?

Three is a Magic Number. The National Cyber Security Centre recommends that you use three random words to make strong and unique passwords. Doing this makes your password much longer (and therefore harder to guess or break), but keeps it easy to remember. If picking three random words is proving tricky, you could use a favourite song lyric or phrase that you find memorable.

Don't make it personal. You should not use any personal information in your passwords - things like your pet's name, your middle name, the place you were born etc. can be tracked down on social media and your online footprint. Even if you think your privacy settings are pretty good, friends and family who you are linked to online may be less diligent.

Characterful passwords. If you need to include special characters in your password, it is often tempting to replace letters that look similar (e.g. password becomes p@$sw0rd!) - however this tactic is well known to fraudsters. Instead, think about adding them in between your three random words : e.g. balloonhooklamp could be changed to @balloon?hook!lamp.

Take a strength test. To explore how small changes can increase your password strength, have a look at How Secure is My Password. This is a website where you can type in potential passwords and it tells you how long it would take a computer to crack them. For example, balloonhooklamp is estimated to take 1 thousand years to break, but adding symbols in increases that to 80 trillion years!

Don't recycle. Reusing passwords is risky - it's always safest to come up with a new password rather than slightly tweaking one you have used before.

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS.
You can contact the Counter Fraud team using our details below. You can also report your concerns to the NHS Counter Fraud Authority via their online reporting tool or hotline. If you making an anonymous report please give as much detail as possible as we won't be able to contact you for more information.

I have a concern that fraud may be being committed against the general public.
These concerns can be reported to Action Fraud (0300 123 2040). If someone has been actively defrauded it may also be appropriate to report to the police. If it is suspected that the victim's bank account has been compromised, they will need to speak to their bank as a matter of urgency.

I have received a suspicious email to my NHS.net email address.
Do not click on any links or attachments. Forward the suspect email as an attachment to spamreports@nhs.net. To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".

I have received a suspicious email to another email account (not NHS.net).
Do not click on any links or attachments. Forward the email to report@phishing.gov.uk. You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

I have received a suspicious text message.
Do not click on any links in the text message! Forward the text message to 7726.

I have come across something and I'm not sure whether or not it is fraud related.
You are very welcome to contact your Local Counter Fraud Specialist for advice and support, our details are below.

How to Contact Your Local Counter Fraud Specialist:

Your Local Counter Fraud Specialist is: