FRAUD INSIGHT

JANUARY 2024

auditone

SCAM ALERT: EMERGING QR SCAMS

QR codes have become a popular way to open websites and pay for products and services. But not all of them are secure. Cyber criminals can use QR codes to steal personal and bank details. Here we tell you what you can do to avoid QR scams.

Warning Signs of a QR Code Scam

- **Poor Quality:** Poorly designed QR codes can be difficult to scan and may not even work at all. Additionally, a fake QR code may contain typos or other errors that make it difficult to read.
- **Unfamiliar Domain Name:** Most legitimate businesses will use their own domain name on the real QR codes, so if the URL associated with the code looks unfamiliar or suspicious to you, it's best to avoid scanning it.
- **Suspicious Content:** If you scan a QR code and are presented with content that seems suspicious or out of place, this could be another warning sign of a QR code. For example, if you scan a restaurant's QR code and are taken to an online casino site instead, this could be an indication of a fraudulent QR code.
- **Asking for Personal Information:** Legitimate businesses will never ask for personal information such as your credit card information, payment information, financial information, login information or any kind of sensitive information via a QR code scan.
- **Offers Too Good to Be True:** If you come across a website offering something that seems too good to be true after you scan QR codes (such as free money or products), this could also be an indication that the QR code is not legitimate.

How to avoid a QR scam

1. Before scanning a QR code, like in a restaurant or some other public space, check that it hasn't been tampered with or got a sticker placed over an original code.
2. Installing anti-virus software to verify original QR codes that do not contain malicious links will help you avoid having a virus or other malware downloaded onto your mobile.
3. Double-check the preview of the QR code link. When you scan a QR code, a preview of the URL should appear. Make sure the website address is legitimate. Look for a padlock symbol and an address that begins with "https://". Only those URLs are secure.
4. Think twice if the app or website you're being directed to asks you to provide personal details. If it does, make sure it's authentic.

NATIONAL CASES: DOCTOR SUSPENDED FROM PRACTICE FOLLOWING FALSE SICK CLAIMS

A Merseyside-based doctor who lied to bosses about being off sick pocketed almost £10,000 in pay she wasn't entitled to. The doctor told officials at St Helens and Knowsley Teaching Hospitals NHS Trust how between August and December 2020 she was unable to work due to illness. As a result, she was given requisite sick pay. At the same time, she undertook almost 40 shifts at hospitals more than 150 miles away while collecting thousands of pounds for being off work. At a Medical Practitioner Tribunal Service (MPTS) hearing, the doctor has since been suspended from practice for nine months.

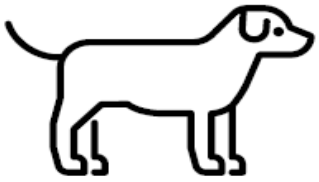
A report released following the completion of the hearing detailed how the doctor had been employed as a GP speciality trainee in St Helens and Knowsley, having joined the UK Medical Register in 2018. Concerns were raised with the General Medical Council following a probe by the trust. During the period August 25 to December 21, 2020 - amid the height of the Covid-19 pandemic, the doctor undertook a series of locum shifts for United Lincolnshire Hospitals NHS Trust. During this time she was paid almost £10,000 in sick pay. The tribunal was told the doctor eventually admitted to her misconduct. In evidence, she said a conversation she'd had with her former partner about being dismissed if she worked while claiming sick pay took place after the investigation had started. During an initial call in December 2020 with the trust's HR partner, when asked if she had been working while off sick, she explained that she was not in a position to talk due to the distress caused by recent life events. She explained that at that time she was not on sick leave and was asked by her lead employer to get a new sick note. The doctor said she knew she had acted wrongly but did not think it was correct to say that she did not correct her actions when she was made aware. During cross examination, the doctor accepted that the telephone attendance note made at the time by the HR business partner recorded that when asked if she had worked while claiming sick pay she had said no, which was a lie. The tribunal was told almost £3,000 had been re-paid by the doctor but she was having "some difficulties arranging to pay." In mitigation, the doctor said the incident occurred a while ago, and she has now had time to reflect on her actions and knew what she did was wrong.

Doctor took thousands in sick pay despite taking shifts 150 miles away - Liverpool Echo

SCAM ALERT: LOST PET SCAM

Criminals are targeting victims who have placed lost pet posts on Facebook. They are contacting victims claiming to be veterinary practices that their missing pets have been taken to and demanding payment for injuries.

If you having a missing pet and have posted on missing or lost pet sites on Facebook or other social media sites, be wary of this scam.



- **If in doubt, hang up and contact the veterinary practice yourself.**

If you believe you have been a victim of Fraud, contact your bank immediately and report the incident to Action Fraud https://www.actionfraud.police.uk/ or call 0300 123 2040

LOCAL CASES: CARLISLE NURSE STOLE MORPHINE FOR BACK PROBLEMS

A nurse who forged hospital colleagues' signatures to steal morphine has been convicted and sentenced to community service following an appearance at Carlisle Magistrates Court. The nurse used the drug to self-medicate for a back problem rather than seeking treatment stating their ward was busy and there were staff shortages.

Jeff Smith, mitigating, said the nurse acted "foolishly" because he was "not able to carry on". The nurse was reported to police in July 2022 following identified irregularities. The allegations included “forging other colleagues' signatures in order to sign drugs out," prosecutor George Shelley said. The nurse had also falsely indicated that certain patients required morphine when they did not. When interviewed, the nurse admitted he had been stealing morphine for about six months. He had suffered from a back problem for years and the low doses he took had increased and made him "feel good", the court heard. The nurse admitted one offence of theft and another of fraud, having falsified the names of doctors and staff as the drugs cabinet book had to be countersigned. Mr Smith said the nurse had worked for the NHS for 30 years. He should have taken time off to recover from his back problem but prioritised the NHS and patients over his own medical condition, Mr Smith added. "We all lose out as a consequence of what has happened, and no-one knows that more than him. Magistrates imposed an 18-month community order and he must also complete 200 hours' unpaid work.

Fake profiles are used by criminals to build a relationship with you on social media platforms, dating websites or gaming sites. They use information found on social media to create fake identities to target you. Once a relationship has evolved, they convince you to send them money.

They often go to great lengths to gain your trust and convince you that you’re in a genuine relationship before appealing to your compassionate side to ask for money. Criminals will use language to manipulate, persuade and

exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as claiming they need money for emergency medical care, or to pay for transport costs to visit you if they are overseas.

HOW TO SPOT THE SIGNS

- You've struck up a relationship with someone online and they declare their love for you quickly. Many fraudsters claim to be overseas because they work in the military or medical profession.
- They make up excuses as to why they can't video chat or meet in person and will try to move your conversations off the platform you met on.
- When they ask for financial help, it will be for a time-critical emergency, and the reason will be something that pulls at the heartstrings. They may get defensive if you decline to help.
- Their pictures are too perfect, they may have been stolen from an actor or model. Reverse image search can find photos that have been taken from somewhere else.
- They tell you to keep your relationship private and not to discuss anything with your friends and family.

HOW TO PROTECT YOURSELF

STOP: Take a moment to stop and think before parting with your money or information.

CHALLENGE: Is this person really who they say they are? Could it be fake? It's OK to reject, refuse or ignore any requests for your financial or personal details. Criminals will try to rush or panic you.

PROTECT: Contact your bank immediately if you think you've been victim of a scam and report it to Action Fraud.

PRESENTATIONS: CAN YOU HELP?

One of the best ways of helping the NHS prevent fraud is to know what to look out for in your day to day job. One good way of doing this is to arrange a fraud awareness presentation for your team, department/ward or directorate. Our team of trained counter fraud specialists will provide you with an interactive presentation focusing on real life fraud cases.

Why not add something different to the next team meeting?

Presentation Request form - Click here >>>>>>

NATIONAL CASES: NURSE STRUCK OFF FOR CONCEALING SERIOUS CRIMINAL BEHAVIOUR

A nurse failed to tell her employers multiple times that she had been arrested in connection with a six-figure fraud scheme. The nurse from Bristol was questioned and later arrested after her husband received money payments from firms both in the UK and abroad, which were re-directed into his and her bank account between November 2019 and May 2020. The nurse, who was working at University Hospitals Bristol NHS Foundation Trust, failed to inform her line manager, senior management or the Nursing and Midwifery Council. A disciplinary hearing held in early September outlined how she had asked to leave work early to assist on a police matter. The report stated: "It is alleged that on December 8, 2021 you were approached by a senior employee at the trust who had been informed that you had requested to leave work early due to a matter involving the police. The report said that days before that,on December 3, 2021, she was charged with converting criminal property by money transfer totalling £114,945.95 between December 17, 2019 and January 4, 2020. She continued to keep quiet about the charge in a 121 meeting in January 2022 and declined to disclose any further information about the police investigation into her husband. Days later, she and her husband pleaded guilty to the fraud charges at Bristol Crown Court on January 10, 2022. Bristol Live's coverage of this brief court hearing caught the eye of senior staff at the NHS trust and the full-time nurse was questioned about the charge and the article. The panel heard she declined to give any information and she was promptly suspended by University Hospitals Bristol NHS Foundation Trust. The nurse referred herself to the Nursing and Midwifery Council in late January 2022, alongside a referral from the NHS trust. She was later given an 18-month prison sentence, suspended for two years, with 100 hours of unpaid work in March 2022. Her husband was jailed for 39 months for his fraudulent money transfers of £332,015.58. In mitigation, it was noted she had pleaded guilty to the charge and was identified by the judge as playing a secondary part in the fraud. The panel found that there were early admissions and engagement with the Nursing and Midwifery Council through-out the fitness to practise process and no patients were harmed.

HOW STRONG IS YOUR PASSWORD?

More and more victims are hacked, as the password they use is either easily hacked through information obtained through social media or the same password was used on other hacked accounts or websites. Try using Password Strength Meter (passwordmonster.com) to check how strong your password is or how easy it could be hacked and Have I Been Pwned: Check if your email has been compromised in a data breach to check when your email address has been in a data breach?

Both are free to use and will provide information on if you should change or strengthen your passwords.

NATIONAL CASES: NHS MANAGER SENTENCED FOLLOWING FRAUD INVESTIGATION

A senior manager at NHS Harrow Clinical Commissioning Group (CCG) was sentenced to three years and eight months in prison at Southwark Crown Court. The defendant pleaded guilty to a charge of Fraud by Abuse of Position at Willesden Magistrates Court in 2023.

The defendant stated that he knew what he was doing was dishonest and that he committed the fraud purely for financial gain and that fraud had become an addiction. He had attempted to cover up his fraudulent activities by sending an email to the CCG using the address of his deceased wife who had died in 2012, eight years prior to the email being sent. The lead investigator said: "he (sic) held a position of trust within the NHS, holding a budget allowing him to conduct this calculated fraud. He wanted extra cash to fund a lifestyle of expensive holidays and shopping which he and his husband couldn't afford. Not only did he steal money from the NHS which would have been used to fund care in the Harrow area, he used the names of family members and friends to facilitate the fraud including using the name of his deceased wife."

The fraud came to light when a colleague at Harrow CCG, where the defendant had been employed between April 2017 and December 2020 as the assistant managing director for planned and unscheduled care, queried invoices from a company called Tree of Andre Therapy Services Limited. Due to the unusual company name, checks were carried out. Searches could not find any web site for Tree of Andre, there was no trace of the company being registered on the Care Quality Commission (CQC) website and the company was shown as dormant on Companies House records. In his role at the CCG, he managed a team of staff and had a budget responsibility. He had authority and approval to sign off invoices up to a value of £50,000. Between August 2018 and December 2020, he authorised and approved invoices submitted by Tree of Andre for payment by Harrow CCG totalling £564,484.80. These were paid into a bank account registered to himself. He was the sole approver for all invoices submitted, and no services were delivered, or work conducted for the CCG by that company. The investigation established that Tree of Andre Ltd was registered to an address in Scotland, which would be too far away to provide services to Harrow CCG. Further investigation showed another company also registered at the same address, called Vesuvius Business Management Limited. This was the umbrella company used by the defendant to channel his NHS salary of £472 per day. In an attempt to cover up the fraud, he had sent an email in June 2020 purporting to be from Tree of Andre to NHS Harrow CCG providing anonymised patient details where care was shown to have been provided, as well as the GP practices concerned. The email was sent from the email address of his deceased wife.

In November 2021 he was arrested at his home in Scotland. When interviewed by NHS CFA investigators, he confirmed that Tree of Andre was a ghost company he had set up some months after he began his contract with Harrow CCG. He had registered the company online in the name of family members who had no knowledge of the

fraud. He confirmed he had set this company up to facilitate the fraud and that no services were ever provided by it. He confirmed the payments made by Harrow CCG were made into his bank account. Sentencing him to three years and eight months in prison Judge Vanessa Francis said: "You have worked in the NHS all your life, you are clearly someone who clearly cares deeply about helping others. Yet you used the system to systematically defraud those who had employed you to the tune of over £565,000.

For an NHS department already in deficit, what you did was take away the opportunity for people to be treated, for people to be helped and get what they needed. It meant in practical terms the vulnerable people who needed care did not get as much care as they needed, and you are responsible for that. You abused the position of responsibility that you were given and in a relatively planned and sophisticated way."

NHS Counter Fraud Authority Head of Operations, Richard Rippin said:

"We are delighted with the sentence given out today, and I commend the work undertaken by our NHSCFA investigators and the Crown Prosecution Service who have brought this case to court. This was a deliberate and calculated attack on the NHS, with the sole purpose of using money originally intended for patient care to live a lavish lifestyle at the expense of the taxpayer. There is a counter fraud response working across the NHS to identify and pursue offenders like this and protect those funds needed for patient care. Work now continues to recover the monies taken and return them to the NHS in Harrow."

Since the beginning of December 2023, Action Fraud and the Suspicious Email Reporting System (SERS) have received over 180 reports concerning the impersonation of National Crime Agency (NCA) agents. The victims describe receiving an email purporting to be from the NCA. The email states that the NCA has evidence that the recipient has accessed and viewed "child pornography" or other "illegal pornographic content." The emails demand that the recipient make contact within a specified deadline. If they do not, the email claims that a warrant will be issued for their arrest and that the recipient's details will be added to the sex offenders register, quoting legislation in an effort to make the threat sound legitimate. It is assessed that the intention of the email is to prompt the victim into initiating communication with the suspects so that personal information can be disclosed to be used for blackmail or to commit fraud. Unlike other emails which impersonate law enforcement, there is no up-front demand for money however, where victims have engaged with the suspects, they have demanded money at a later stage. The use of such threatening language creates a significant and emotional impact upon the recipient. The time pressure that is applied encourages victims to panic and act without thinking, unknowingly exposing themselves to compromise and blackmail.

The NCA will not send unsolicited correspondence requesting money or bank details.

If you have doubts about the authenticity of a message received from the NCA, please call 0370 496 7622. Remember, your bank (or any other official source) will not ask you to supply personal information over email. If you think an email is suspicious, you can report it by forwarding the email to: report@phishing.gov.uk.

Victims reported losing a total of £15,319,057, a 41 per cent increase on last year's results, which amounts to an average loss of £2,372 per victim. From May – August 2023 alone, more than £4.6m was lost. With the summer months seeing the highest levels for holiday fraud reports, Action Fraud has launched a national awareness campaign to urge the public to think twice before booking a holiday, so consumers don't get burnt before they are on the beach. Pauline Smith, Head of Action Fraud, said:

"With summer only just around the corner, we enter a period where fraudsters ramp up efforts to catch out unsuspecting members of the public. Scammers prey on people wanting to find a good deal online – whether that's cheap flights, great hotels close to the beach at discounted rates or package holidays that undercut well-known travel operators and brands, people are more than willing to snap up a deal which sometimes comes at a heavy cost. When booking a holiday here or abroad, it's important to do your research before handing over any money and to double check any website. To avoid the wave of crime this summer we encourage people to stop, check and research before paying. If it sounds too good to be true – it most definitely is."

Anna Bowles, Head of Consumers and Enforcement at the UK Civil Aviation Authority, which runs the ATOL financial protection scheme, said:

"Before booking any trip abroad it is always worth doing some homework before you part with any money to make sure you limit your risk of being impacted by fraud. Make sure you research the company you're booking through - check reviews and ensure that your booking includes all the extras you're expecting, such as baggage allowance and transfers. We also recommend some simple measures to financially protect your well-earned holiday, including using the atol.org website to check your trip is financially protected by ATOL, consider paying by credit card and taking out travel insurance as soon as you book. This will add extra layers of protection against anything going wrong with your booking."

Data revealed that the top 10 hotspots of people being caught out by holiday fraud in the UK were as follows: London, West Midlands, Greater Manchester, Thames Valley, West Yorkshire, Hampshire, Essex, Sussex. Avon and Somerset and Kent. Interestingly, people in their 20s and 40s who reported losses accounted for 44 per cent of all reports, further dispelling the myth that only older people are targeted by fraudsters. Holiday fraud encompasses many different tactics employed by criminals to dupe unsuspecting members of the public. The most frequent frauds are clone comparison websites, airline websites and holiday websites. At a quick glance it would appear you are on a trusted site, whereas in reality the URL has been changed. Here, victims assume they are on the genuine site and willingly hand over money at a great cost. Fake confirmation emails or booking references are even sent, which has resulted in some cases of victims only realising they have fallen victim to fraud when they are at the airport to check in for their flight to be told that their booking does not exist.

An emerging trend is fraudsters using counterfeit Air Travel Organisers' Licensing (ATOL) protect numbers on their fake webpage. All credible and trusted companies are provided with a number that shows the company has passed the regulatory checks by ATOL, with this number being unique to the website. Recently, fake websites have used duplicate or fabricated numbers which have been edited onto an ATOL logo. ATOL recommends double checking all numbers on websites and checking travel operators before handing over any money. If you do pay, use a credit card as this can offer greater protection should you lose your money.

Top tips to avoid falling victim to holiday fraud

- **Do your own research:** Booking your trip via a company you haven't used before? Do some research to check they're legitimate. Read feedback from sources that you trust, such as consumer websites. You can find a company's official website by searching for them on Google or another trusted search engine
- **Look for the logo:** Check whether the company is an ABTA member. Look for the ABTA logo on the company's website. If you have any doubts, you can verify membership of ABTA online on their website. If you're booking a flight as part of a package holiday and want more information about ATOL protection, or would like to check whether a company is an ATOL holder, visit the ATOL or CAA website.
- **Pay safe:** Book your holiday with a credit card, if you have one. Most major credit card providers protect online purchases, and are obliged to refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected
- **Secure your email:** If your email is hacked, it could allow a criminal to access information about your holiday booking. Use 3 randoms words to create a strong password for your email that's different to all your other passwords. If you're offered 2-step verification to protect your email and social media accounts, always use it

For a full list of tips to avoid becoming a victim of fraud, please visit https://www.atol.org/about-atol/how-to-check-for-protection/ or https://www.abta.com/tips-and-advice/planning-and-booking-a-holiday/how-avoid-travel-related-fraud.

MEET THE COUNTER FRAUD TEAM

Rebecca Napper

Head of Operations (Proactive)

T: 07980 726 508

E: rebecca.napper@audit-one.co.uk

Michelle Watson

Head of Operations (Reactive)

T: 07580 589 024

E: michelle.watson@audit-one.co.uk

Laura Fox

Counter Fraud Manager

T: 07976 759 637

E: laura.fox@audit-one.co.uk

Kathryn Wilson

Counter Fraud Specialist

T: 07973 814 205

E: kathryn.wilson@audit-one.co.uk

Gemma Collin

Counter Fraud Support

T: 07920 590 180

E: gemma.collin@audit-one.co.uk

Martyn Tait

Counter Fraud Specialist

T: 07976 433 667

E: martyn.tait@audit-one.co.uk

Steven Sherwood-Hodgson

Counter Fraud Specialist

T: 07977 065 338

E: steven.sherwood-hodgson@audit-one.co.uk

Stephen Veitch

Counter Fraud Specialist

T: 07973 814 475

E: stephen.veitch@audit-one.co.uk

Simon Clarkson

Counter Fraud Specialist

T: 07980 729 654

E: simon.clarkson@audit-one.co.uk

Sarah McCloud

Counter Fraud Specialist

T: 07979 814 713

E: Sarah.mccloud@audit-one.co.uk

Michelle Acuna-Ocana

Lead Investigation Officer

T: 07974 096 752

E: michelle.acunaocana@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060