July Cyber Scam Update

Beware of ticket fraud as restrictions ease

Data from Action Fraud reveals that 1,085 reports of ticket fraud have been made so far this year, equating to an average loss of £850 per victim. Almost two thirds of victims (61 per cent) were aged between 20 to 49 years old. Action Fraud received 374 reports of ticket fraud in March this year – the highest number of reports received since March 2020 when lockdown restrictions were first implemented. Victims reported losing over £200,000 in March this year alone.

One victim lost £200 after posting on Twitter asking if anyone had tickets for sale for a concert. The victim was messaged by someone who claimed they had a number of tickets for sale and the suspect claimed they would transfer the tickets to the victim as soon as payment was received. The victim sent the payment via PayPal and once the suspect had received the payment, they blocked the victim.

Another victim lost almost £250 after joining a Facebook group where they saw someone selling two VIP tickets to a festival. The victim contacted the person selling the tickets and was informed that they only accepted payment a digital wallet provider. The suspect claimed they would transfer the tickets to the victim as soon as payment was received, but went on to block the victim and continued to advertise the tickets on the same group. Another victim lost more than £3,500 after purchasing tickets for a rugby tour via what appeared to be a legitimate ticket website. The victim attempted to obtain a refund due to the uncertainty around travel, but was unable to contact the company. The company has since been dissolved and a number of other victims have reported suffering a similar fate.

Action Fraud has launched a national awareness campaign today (Monday 14 June 2021) to remind the public to take extra care when booking tickets online, as it is anticipated that increased demand for tickets following restrictions easing will lead to more unsuspecting victims being targeted.

Spot the signs of ticket fraud and protect yourself:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal give you a better chance of recovering your money if you become a victim of fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

Scams warning for tax credits customers

Anyone doing their tax credits renewal who has received a tax or benefits scam email or text might be tricked into thinking it was from HMRC and share their personal details with the criminals or even transfer money for a bogus overpayment.

Many scams mimic government messages to appear authentic and reassuring. HMRC is a familiar brand, which criminals abuse to add credibility to their scams.

If customers cannot verify the identity of a caller, HMRC recommends that you do not speak to them. Customers can check GOV.UK for HMRC's scams checklist to find out how to report tax scams and for information on how to recognise genuine HMRC contact.

HMRC's advice:

- Stop: Take a moment to think before parting with your money or information. Don't give out private information or reply to text messages, and don't download attachments or click on links in texts or emails you weren't expecting. Do not trust caller ID on phones. Numbers can be spoofed.
- Challenge: It's ok to reject, refuse or ignore any requests - only criminals will try to rush or panic you. Search 'scams' on UK for information on how to recognise genuine HMRC contact and how to avoid and report scams.
- Protect: Forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599. Report scam phone calls on GOV.UK. Contact your bank immediately if you think you've fallen victim to a scam, and report it to Action Fraud (in Scotland, contact the police on 101).

July Cyber Scam Update

Warning about scam calls from "matching" mobile phone numbers

The National Fraud Intelligence Bureau (NFIB) is warning the public to be vigilant of scam calls that appear to be coming from numbers similar to their own. Commonly, the first seven digits (07nnnnn) match the victim's own number. The calls impersonate well-known government organisations, or law enforcement agencies, and will ask the recipient of the call to "press 1" in order to speak with an advisor, or police officer, about unpaid fines or police warrants.

In May 2021, Action Fraud received 2,110 scam call reports where the caller's number matched the first seven digits of the victim's own phone number. Of these, 1,426 (68%) referred to HMRC or National Insurance.

Victims have also reported receiving these types of calls, and messaging, via widely-used messaging apps, such as WhatsApp.

Protect yourself - What you need to do:

- Government and law enforcement agencies will not notify you about unpaid fines or outstanding police warrants by calling or texting you. Do not respond to any calls or texts you receive about these.
- Always take a moment to stop and think before parting with money or your personal information, it could prevent you from falling victim to fraud. Remember, it's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- If you receive a suspicious text message, you can report it by forwarding the message to 7726. It's free of charge.
- Suspicious telephone/mobile calls can be reported to Action Fraud via their website: https://www.actionfraud.police.uk/report-phishing

MONTHS TOP TIPS:

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the real world.

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook**: www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**: @SafeInWarks

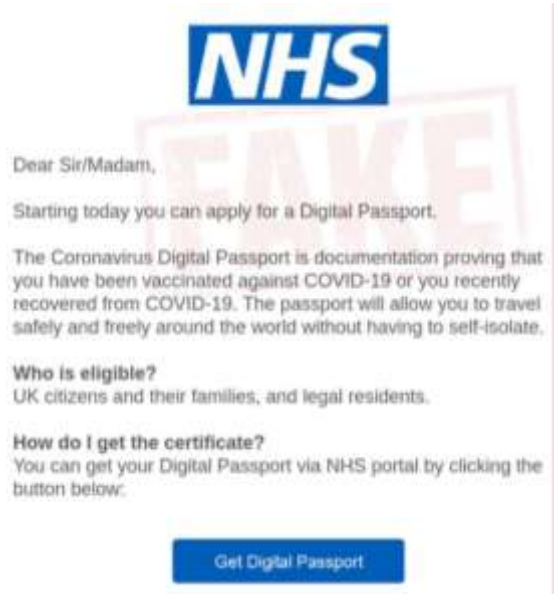
Visit our **site**: www.safeinwarwickshire.com

3 2040 or http://www.actionfraud.police.uk

crime, contact Victim Support on 01926 682 693.

Vaccine passport scam emails reported over 370 times

Action fraud have received over 370 reports scam emails regarding vaccine passports.



TOP TIPS:

- Remember, the NHS would never ask for your bank details as your vaccination status can be obtained for free through the official NHS app, NHS website, or by calling the NHS on 119.
- If you received a suspicious email, you can report it by forwarding the email to **report@phishing.gov.uk**. Your reports will help Action Fraud remove the fake websites used in these scams.