STAFFORDSHIRE POLICE

Cyber Champions Tips - January 2021

Vaccine Scams Soar in 2021

CITY of LONDON POLICE

POLICE - ALERT

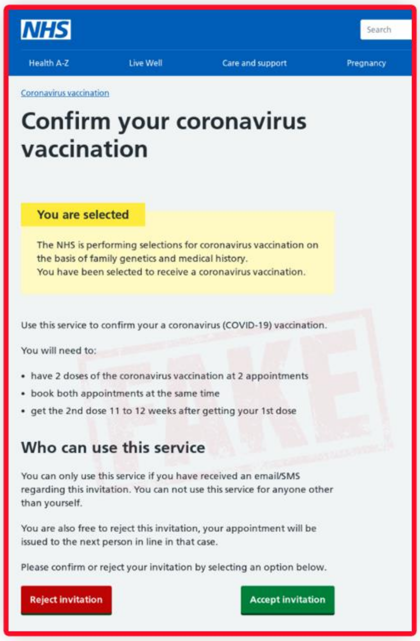
1,166 vaccine related scam emails reported in 24 hours

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Learn more: actionfraud.police.uk/vaccine

OFFICIAL

It is wonderful news to hear the roll out of the coronavirus vaccines are well underway, but we are in familiar territory concerning criminality who are seeking opportunities to exploit this positive step forward. News earlier this month reported the sad story of an elderly individual who had been victim to a **door step vaccine scam** and duped into receiving a 'fake vaccine', which was an unknown substance. This news was most shocking but highlights the lengths to which some criminally minded individuals will go to. The report also highlights the importance of looking out for those who are most vulnerable in our communities. Vaccine related phishing emails have soared this month, here are examples of phishing emails which have been circulating:



Coronavirus vaccination

Confirm your coronavirus vaccination

You are selected

The NHS is performing selections for coronavirus vaccination on the basis of family genetics and medical history.
You have been selected to receive a coronavirus vaccination.

Use this service to confirm your a coronavirus (COVID-19) vaccination.

You will need to:

- have 2 doses of the coronavirus vaccination at 2 appointments
- book both appointments at the same time
- get the 2nd dose 11 to 12 weeks after getting your 1st dose

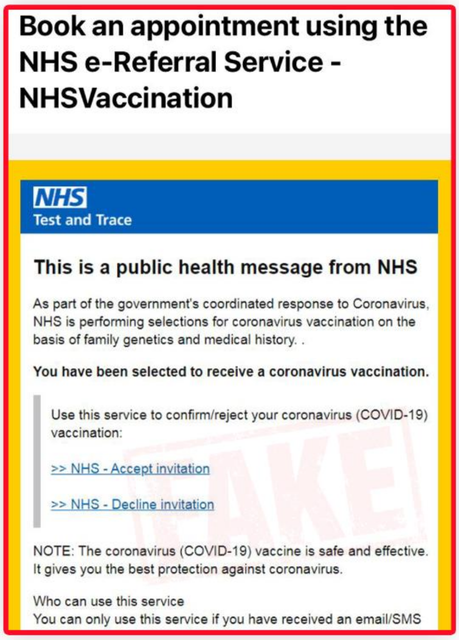
Who can use this service

You can only use this service if you have received an email/SMS regarding this invitation. You can not use this service for anyone other than yourself.

You are also free to reject this invitation, your appointment will be issued to the next person in line in that case.

Please confirm or reject your invitation by selecting an option below.

Reject invitation   Accept invitation



Book an appointment using the NHS e-Referral Service - NHSVaccination

This is a public health message from NHS

As part of the government's coordinated response to Coronavirus, NHS is performing selections for coronavirus vaccination on the basis of family genetics and medical history. .

You have been selected to receive a coronavirus vaccination.

Use this service to confirm/reject your coronavirus (COVID-19) vaccination:

>> NHS - Accept invitation

>> NHS - Decline invitation

NOTE: The coronavirus (COVID-19) vaccine is safe and effective. It gives you the best protection against coronavirus.

Who can use this service
You can only use this service if you have received an email/SMS

Signs to look out for:

Looks quite genuine at first glance

It's **'offering' something** – your vaccine invitation

The offer is something you may be anticipating/expecting – 'You are/have been selected'

'Accept' or 'reject' **icons inviting to click**

Links – 'Accept & decline' **inviting to click**

Takes you to a **convincing looking website** which when clicking through, **asks to enter personal and bank details**.

ALWAYS - TAKE FIVE

Advice - 'In the UK, coronavirus vaccines will only be available via the National Health Services of England, Northern Ireland, Wales and Scotland. You can be contacted by the NHS, your employer, a

GP surgery or pharmacy local to you, to receive your vaccine. Remember, the vaccine is free of charge. **At no point will you be asked to pay for a vaccine or hand over sensitive financial information:**

- The NHS will never ask you for your bank account or card details
- The NHS will never ask you for your PIN or banking password
- The NHS will never arrive unannounced at your home to administer the vaccine
- The NHS will never ask you to prove your identity by sending copies of personal documents such as your passport, driving licence, bills or pay slips

If you receive a call you believe to be fraudulent, hang up. If you are suspicious about an email you have received, forward it to report@phishing.gov.uk. **Suspicious text messages** should be forwarded to the number **7726** which is free of charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by calling 0300 123 2040 or visiting www.actionfraud.police.uk '*Action Fraud*

Other News

Fake National Insurance Calls - In just one week this month, Action Fraud reported they had received over 1000 extra calls from the public reporting a National Insurance scam. The calls are automated and encourage the pressing of '1'. People who press '1' are connected to criminals who try to steal personal details. The best thing to do on receipt of such a call is simply hang up and if worried, seek advice and additional information from a trusted source or from someone you trust, never provide personal or financial details to an unsolicited caller.

What do you do if you think you may have provided personal details to someone over the phone you now believe could be a scam?

Advice:

- 'Contact your bank/building society/credit card provider immediately and report to Action Fraud www.actionfraud.police.uk or call 0300 123 2040
- **Protective Registration** - You can also contact CIFAS to apply for protective registration. This means extra checks will be carried out when a financial service, such as a loan, is applied for using you're address and personal details, to verify Its you and not the fraudster.' *Action Fraud*

Scam guises currently circulating include:

- HMRC TAX
- Amazon
- Health providers, vaccine
- Police and bank personnel

Phishing methods used:

Phone - Vishing
Texts - Smishing
Emails - Phishing

NCSC NEWS

Public Being Urged to be Aware of Post Data Breach Scams - New National Cyber Security Centre (NCSC) guidance is now available to help people stay safe online by understanding how cyber criminals use information from data breaches to try and steal sensitive personal data. 'With nearly half of UK businesses reporting a cyber breach or attack in the past year (46%), the National Cyber Security Centre (NCSC), a part of GCHQ, produced guidance to help individuals and families stay safe in the aftermath of a breach. Criminals can use information taken from a breach, such as email addresses, to send phishing messages to try and trick people into handing over sensitive personal data like credit card details' *NCSC.* Further information and new guidance can be found here: National Cyber Security Centre

Purchasing Second Hand Devices - Do you consider security when purchasing second hand devices? Lives are lived revolving around the usage of digital devices these days and lots of personal data is stored on them; but what do we do when we change our tech; selling, buying new or purchasing preowned? The second-hand market has an abundance of older tech on offer which can suit many budgets and is often an affordable way for people to access newer technology; but we need to consider our data security when either exchanging, giving, buying or selling. The NCSC has issued new guidance for consumers who are buying or selling preowned connected devices. The guidance contains information about things such as erasing data, choosing second-hand devices and things to do before using a second-hand device, it is well worth a read and you can see the full guidance here: National Cyber Security Centre

New NCSC Vulnerability Scanning Tools & Services:

Audience - SME's, Large Organisations & Public Sector

The NCSC has issued guidance which offers advice on the choice, implementation and use of automated vulnerability scanning tools for organisations of all sizes. 'Vulnerability Scanning is a broad term, used to describe the automated process of detecting defects in an organisation’s security program. This covers areas such as the patch management process, hardening procedures and the Software Development Lifecycle (SDLC). Services or products that offer vulnerability scanning are also commonly known as Vulnerability Assessment Systems (VASs). As part of an effective Vulnerability Management Program (VMP), vulnerability scanning solutions can be an affordable way to automatically detect security issues within an organisation’s networks. The benefit of vulnerability scanning 'affords an organisation the ability to keep pace with individuals and groups intent on compromising systems, many of which use similar tools and techniques to discover security flaws' *NCSC*. This useful guidance can be found by visiting here: Vulnerability Scanning Tools and Services - NCSC.GOV.UK

January NCSC threat reports here:

8th January 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-8th-january-2021

- HMRC warn of COVID-19 scam text messages
- PPE company’s operations disrupted by former employee
- Hackney council cyber attack update

15th January 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-15th-january-2021

- Vigilance urged following COVID-19 vaccine scams
- Capcom releases new update on ransomware attack
- Billions in Bitcoin residing in inaccessible wallets
- Sports clubs gather for summit on cyber security

22nd January 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-22nd-january-2021

- Ongoing threat of ransomware
- Fake apps responsible for rise in attacks targeting remote devices

29th January 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-29th-january-2021

- Facebook members' telephone numbers for sale
- 2 million+ pieces of personal data leaked from dating site hack

West Midlands Regional Cyber Crime Unit (WMRCCU):

The WMRCCU website has a host of information to help boost your cyber awareness and help keep you informed, take a visit where you will find tips, information, advice and subscription to the Cyber Crime Sentinel, check it out here: https://www.wmcyber.org/

WMRCCU Podcasts deliver regular non-technical cyber news, advice and discussions about current threats and issues we are facing, well worth a listen and can be accessed here: https://cyberthreatweekly.buzzsprout.com/

Reporting

Report cyber-crime and fraud to Action Fraud: actionfraud.police.uk

Businesses suffering a live cyber-attack can call: 0300 123 2040

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Received a phishing email?

Forward suspicious emails to: report@phishing.gov.uk

Received a suspicious text message?

You can report fraudulent texts by forwarding to: **7726**

If a scam text claims to be from your bank, you should also report it to them

Further advice can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

takefive-stopfraud.org.uk

ukfinance.org.uk

staffordshire.police.uk