Fraud Information Alert 10

MIAA Anti-Fraud Service

December 2020

Fake IDs, Vaccination Frauds & Electronic Skimming

Crime fighting agencies are predicting a change in the MO for fraudsters and cyber criminals coinciding with the release of the COVID-19 vaccines. PPE scams are expected to be replaced by COVID-19 vaccine and treatment scams. This is likely to take all forms of cyber-crime activity from emails, to texts and phone calls.

Fake NHS IDs & Theft of Supplies

Due to the high demand for medical supplies across the EU, medical premises including pharmacies are becoming increasingly vulnerable as targets for thefts. Be on the look out for obviously false IDs. Be alert to tailgating. If you don't feel comfortable challenging an individual whom you suspect may possess a false NHS ID in a sensitive or restricted area, do at least report your concerns promptly to line management or security (if available).

Fake Patient Fraud – COVID-19 vaccinations

There is the potential that some individuals may falsely represent themselves as an NHS employee to receive the COVID-19 vaccine in advance. With the online sale of fake NHS IDs and lanyards, there is the potential for fraudsters to purchase these in an effort to appear as a legitimate member of NHS staff when attempting to obtain a vaccination. A fraudster could use the name of a genuine medical professional along with their own image, even if identity checks were conducted prior to the vaccination available records don't always include images to compare.

Online Shopping - Electronic skimming

NHS staff must be cautious when purchasing office supplies for homeworking, there is the potential that Electronic skimming (e-skimming) could occur.

Due to the rapid increase in people working from home as a result of COVID-19, over seven million people are believed to have purchased office equipment. Cyber-criminals have been known to target some retailers (particularly smaller ones) in order to harvest customer details due to limited online IT security provisions. Don't forget:

- Choose carefully where you shop
- Use a credit card for online payments
- Only provide enough details to complete your purchase
- Keep your accounts secure
- Watch out for suspicious emails, calls and text messages
- If things go wrong let your bank know straight away

National Cyber Security Centre advice - shopping online securely - https://youtu.be/PtHfFP9-8d0

For some further seasonal fraud advice, visit: https://www.actionfraud.police.uk/campaigns

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

MIAA IA 20/21 10

For further information on MIAA's Anti-Fraud Service visit miaa.nhs.uk

CONTACT: Action Fraud to report any suspicious calls or emails.

For further information or to report NHS Fraud contact:

Darrell Davies

Assistant Director (Anti-Fraud)

0151 285 4520

07785 286381

darrell.davies@miaa.nhs.uk