Finance Department

Fraud Newsletter

June 2021

As more of us are working, shopping and communicating online there has been a rise in online fraudulent activity.

This newsletter is to raise awareness and share recent fraud trends so you know what to look out for.

The June 2021 issue focuses on fraud around the Covid-19 vaccine roll out.
Also highlighting holiday and ticket scams, to keep you fraud aware as restriction ease.

Covid-19 Vaccine Fraud

As the Covid-19 vaccine roll out continues, so do the vaccine related scams.

The most common way that fraudsters are trying to scam people is through text messages, stating that the recipient is eligible for a vaccine and need to click a link to book.

But there is an even more worrying scam which informs the receiver that their vaccine dose was from a "suspect batch" and that they must ring a number urgently.

Remember, the NHS will **never** ask for the following information:

- your bank account or card details
- your pin or banking password
- copies of personal documents to prove your identity such as your passport, driving licence, bills or pay slips

The NHS are using text messages to ask people book their vaccines, but they will never ask for the above information.

If you get a genuine text message from the NHS the sender will be *'NHSvaccine'* if you are worried that a text message might be a scam you can wait until your letter arrives in the post a few days later or contact your GP surgery directly.

Stay fraud aware as Covid restrictions ease

As restrictions start to lift and people are planning holidays and booking live events there has been an increase in fraudsters selling fake tickets, travel insurance and holiday deals that are too good to be true.

Ticketing scams

As events, concerts, festivals, and theatre shows start to reopen ticket scams are increasing.

Beware of fake websites and social media profiles selling tickets, websites may look genuine subtle changes in the URL can indicate that it's fraudulent.

Make sure you book tickets directly through official sellers who are members of the self-regulatory body STAR, as anything else could be a scam.

Global Health Insurance Card (GHIC) scams

When travelling in the EU, people can access emergency and medical care with a Global Health Insurance Card (GHIC). This card has replaced the European Health Insurance Card (EHIC) - criminals are capitalising on this new card to commit fraud, asking victims for payment details when the GHIC is free.

The GHIC, which replaces the European Health Insurance Card, is FREE to use and can only be obtained directly via the NHS website

You don't need to apply for a GHIC until your current EHIC expires.

Travel deal scams

Criminals set up fake websites offering 'travel deals', these websites may look similar to the genuine organisations but subtle changes in the URL can indicate that it's fraudulent.

These websites may seem professional and convincing, using images of luxury villas and apartments that don't exist to convince victims they're trusted and genuine.

Quite often a deposit is made to book the accommodation but when it is found out to be a scam, the deposit is not returned.

Always remember:

- Be suspicious of any "too good to be true" offers or prices.
- Where possible, book directly with an established hotel or through a reputable travel company/agent that is a member of a trade body such as ABTA or ATOL.
- If you do decide to book independently, establish if you're dealing with the property owner or a letting agent or via the local tourist information desk, and verify that the address exists through web searches and online maps.
- Always access the website you're purchasing from by typing it in to the web browser and avoid clicking on links in unsolicited emails or social media posts. The website should use the padlock symbol to indicate that the site is secure.
- Always use the secure payment options recommended by reputable online travel providers and don't accept requests to pay separately via a bank transfer.
- Where possible, use a credit card when booking holidays over £100 and up to £30,000 as you receive protection under Section 75 of the Credit Consumer Act.

Other scams on the rise

Here is a summary of some of the other scams circulating. Fraudsters are constantly changing their tactics and updating their schemes, so if it doesn't feel right, it probably isn't.

Compromised National Insurance number scam
People have been receiving automated phone calls with a recorded message stating that their National Insurance number has been "compromised". The person is instructed to "press 1" to address the problem. If you do press 1, you may be connected to a premium rate number and further targeted in an attempt to steal your financial information.

TV Licencing phishing emails
There are a number of phishing emails going around which claim to be from TV Licencing. The emails ask the recipient to update their account information and threaten that failure to comply will lead to their account being suspended.

HMRC
There has been a rise in people being contacted saying they owe tax and face arrest or are due a tax refund.

If you are unsure if a communication appearing to be from HMRC is genuine, use the checklist on the gov.uk website - **here**

Useful websites:

Action Fraud

Take 5 to stop fraud