Finance Department

Fraud Newsletter

December 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 December issue focuses on Fraud trends around Christmas online shopping and Black Friday deals.

The shopping period between Black Friday and the January sales is likely to prove a very busy time for fraudsters.
Please take some time to read through the newsletter to learn more about common scams that you may come across, feel free to share with friends and family to make them aware.

Always remember the golden rule - if it looks too good to be true, it probably is!

Online Christmas Shopping – Tips to stay safe

Keep your devices up to date

Make sure you install the latest software and app updates. These usually contain important security updates that can protect you against fraud and identity theft. If you are using a laptop or tablet to make purchases, make sure it is updated and secure before going ahead.

Take care with links in emails and texts

Some of the emails or texts you receive about amazing offers may contain links to fake websites, designed to steal your money and personal details. Not all links are bad, but it's good practice to check by typing the shop's website address manually into the address bar of your browser or find the website through your search engine.

Choosing where you shop

If you're making a purchase from a company or person you don't know and trust, carry out some research first.

If you decide to go ahead with the purchase, check your credit/debit card providers terms and conditions to see if you are insured for online purchases.

Secure your account and consider using multi-factor authentication

Use a strong, separate password and multi-factor authentication to secure your email account. Criminals can use your email to access other online accounts, such as those you use for online shopping.

Don't give away too much information

Only fill in the mandatory details of forms when making a purchase. These are usually marked with an asterisk*. If you can avoid it, don't create an account on a new site unless you're going to use that site a lot in the future. You can usually checkout as a guest to make your purchase.

If things go wrong

We all make mistakes, and these days the scams can be incredibly convincing.

If you think you may have been taken in by a bogus website, you should first, take a note of the website's address, then close your internet browser. If you have entered your financial details, you should contact your bank to seek advice. You can also report the matter to Action Fraud or by using the other reporting services which are available- suspect texts can be forwarded to 7726 and spam emails can be sent to report@phishing.gov.uk

Delivery Scams

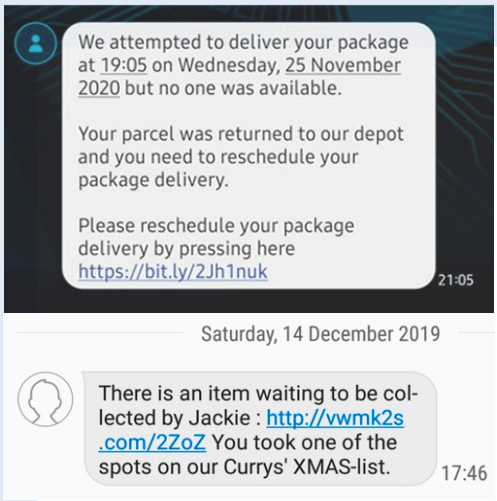
Parcel related scams have been extremely popular since the beginning of the pandemic. Now that we are heading into another busy shopping period, it is highly likely that fraudsters will try to use this strategy more often.

Fraudsters are sending fake delivery text messages to potential victims, the text message will look like it has come from a recognised postal service or delivery firm such as Royal Mail, DPD, UPS, or Hermes. The message will either claim that you have missed a parcel delivery attempt, or that insufficient postage has been paid on a parcel addressed to you.

The message will ask you to click on a link to rearrange delivery, and/or to pay a small fee to cover any missing or additional postage.

If you do click on the link, the fraudster will then start stealing your financial and personal information. In order to 'confirm your identity' they will ask for your full name, address, postcode and bank details.

Fraudsters using this tactic often use 'spoofing' so that when the text arrives on your phone, you cannot see which phone number was used to contact you. Instead, the details may be disguised behind a fake identity label such as "RLML" "DPD-PARCELS" or "HERMES-UK".



Avoiding this scam:

- If you receive a text and you're not sure if it is genuine, do not click on any links in the message.
- If you are expecting a parcel and you're not sure if you may have missed the delivery, contact the retailer or delivery company using their official customer service team.
- You can find examples of identified fraudulent text messages by visiting the Royal Mail website.
- Spam texts can be reported by forwarding them to 7726.

Fake Listings & Websites

During the Black Friday to January Sales period, bargain hunters look out for the hottest deals. This year, there have been concerns that the most desirable items will be harder to find due to global supply issues.

Fraudsters are very aware of which products are going to be the most sought after, so it is very likely that they will try and con shoppers into handing over money by creating fake listings and phishing websites.

Fake listings and phishing sites may encourage you to send payment for a product that does not exist, or which is never sent to you - this is known as Authorised Push Payment fraud.

These sites and listings may also be used to steal your financial and personal information which can then be used by fraudsters to take further money from your bank account.

Avoiding these scams:

- Be sceptical of listings and websites that are too good to be true.
- Research sellers before making purchases – search the retailer online and include key words such as 'scam' or 'fraud' to see if other people have reported problems.
- If you are in any doubt about whether you're looking at a scam, don't enter your personal or financial information.

Social Media Scams

Free 'Vouchers'

You might have spotted on Facebook users sharing 'vouchers' for supermarkets and big-name brands. These are shared alongside claims that brands are offering them out for free to celebrate a special event.

To access the voucher, you will be asked to share your personal and financial details. You are also likely to be asked to share the link for the voucher to be able to access the discount.

This is a tactic which is designed to make the voucher look more plausible to your friends and family. They may think that if you have shared it, then it must be legitimate.

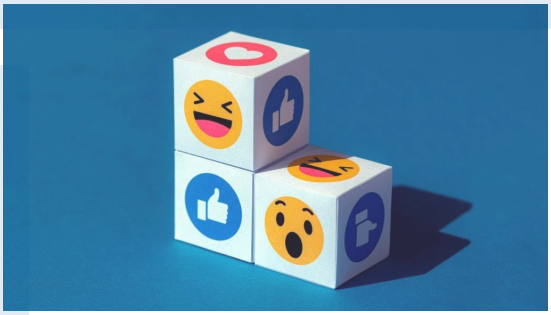
If you see offers like this on social media, do not engage with them. Do not click on any links offered and do not share the post with other people.

Social Media Competitions & Giveaways

Brands often run competitions online and via their social media platforms, that's why it is so easy for fraudsters to take advantage and copy these. Although some competitions you see online are genuine, it's a good idea to check a few things first before rushing in to entering personal information.

Here are some ways to spot fake competitions and giveaways:

- Most verified companies will have a blue tick next to their genuine social media accounts.
- Is there a link to a genuine website in the post? If not, it's probably a scam. A company is unlikely to promote a page which has nothing to sell.
- Check for spelling and grammatical errors. Professional sites will have had their articles checked for accuracy.
- All UK prize draws must have easily accessible terms and conditions. No T&C's imply it's a fake competition.
- Look on the company's official website to see if the competition has a link on there. If not, be suspicious.
- See how long the page has been up. Scams usually have a short shelf life.



'Odd One Out' Competitions

These posts usually show an image of lots of numbers, letters or words repeated over and over. Facebook users are asked to spot the 'odd one out' and to post their answers in the comments to win a cash prize.

Anyone who comments on the post with their answer is then contacted privately to 'arrange' the prize payment. This is highly likely to include handing over financial and personal information.

Please be very cautious and do not engage with any direct messages following from comments on posts like these.