BLACK FRIDAY FRAUD ALERTS 2021

Welcome to our annual Black Friday Fraud newsletter. As ever, 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.

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

Missed Deliveries and Postage Paid Scams

Parcel related scams have been extremely popular since the beginning of the pandemic. Which magazine report that three in five people have received at least one scam delivery text in the past year. Now that we are heading into another busy shopping period, it is highly likely that fraudsters will try to use this strategy more often.

To carry out this scam, fraudsters send fake text messages to thousands of 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 had been paid on a parcel addressed to you.

The message will ask you to click on a link in order to rearrange delivery, and/or to pay a small fee to cover any missing or additional postage. Often the message will mention a small payment of around £1.99 to £3.50 being needed. This figure has been chosen as it is a small amount of money and people will therefore think that making the payment is a low risk transaction.

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.

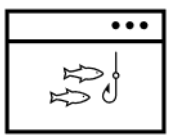
Fraudsters using this tactic often use "spoofing" so that when the text arrives on your phone, you cannot see which phone number was used to contact you. Instead, the senders details may be disguised behind a fake identity label such as "RLML" "DPD-PARCELS" or "HERMES-UK".

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.

Last year, a prolific text fraudster was convicted after sending thousands of fake messages which impersonated various organisations including Royal Mail. You can read more here.

Fake Listings and Websites



During the Black Friday to January Sales period, bargain hunters look out for the hottest deals, with particular items being particularly popular. 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. It is very likely that they will try and con shoppers into handing over their hard earned 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 - use Google to look up the retailer and include key words such as "scam" or "fraud" to see if other people have reported problems. Remember, an absence of reports does not mean the link is safe!
- If you are in any doubt about whether you're looking at a scam, don't enter your personal or financial information.

Shopping Safely Online

Shopping online is convenient and offers a myriad of choice at the click of a button. However, there are also pitfalls that fraudsters may choose to exploit. Here are some handy tips to keep you and your family safe from online fraud.

1. 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. Remember - 'If in doubt; don't check out!'.

If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. You will need to check your card's Terms and Conditions for exact details.

2. 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.

Information can easily be found about how to install these updates from Apple, Microsoft and Google. Even better, just turn on automatic updates so your device will update itself in future.

3. 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 (e.g. Google).

4. Secure your account and consider using multi-factor authentication

Use a strong, separate password and multi-factor authentication (which could come in the form of a one-off text code, a fingerprint scan, or use of an authentication app etc.) to secure your email account. Criminals can use your email to access other online accounts, such as those you use for online shopping.

Multi factor authentication is a way for the service you're using to double check that you really are the person you claim to be, when logging in.

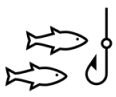
5. Don't give away too much information

You shouldn't need to give out your mother's maiden name, or the name of your primary school, in order to buy something. There's some obvious details that an online store will need, such as your address and your bank details, but be cautious if they ask for details that are not required for your purchase.

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.

6. 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 down 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).

Whether you've been a victim of fraud will depend on how much information you've provided to the website. So keep an eye on bank transactions, if you can. Contact your bank immediately about anything that you don't recognise, even small amounts as often fraudsters will try a few low value transactions first to see if anyone is watching the account.

Social Media Scams

There are always new scams popping up on social media. Below you'll find a list of common tactics being used to target the general public.

Free Big Name "Vouchers"

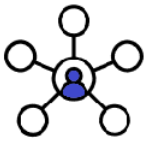
At this time of year you may see more posts from other users sharing "vouchers" for supermarkets and big name brands. These "vouchers" are shared on Facebook and alongside claims that brands are offering them out for free to celebrate a special event. The vouchers offered are often for supermarkets or major shopping chains and the amounts offered can vary from £30 to over £250. 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 in order 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. As a a result, they will be more likely to click on the link themselves.

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

Name Brand Competitions

Last year, fraudsters set up a fake competition using a Currys PC World logo. It enticed people to like the page, tag three friends and share it. The post claimed that a prize draw would take place for the chance to win a television. It may not be easy to spot the scam in this.

Fake competition promoters have been known to message entrants with a link which then requests personal details. Other 'winners' have been duped into giving their bank card details to pay for the delivery cost of the 'prize'. Hopefully you will have read enough of our newsletters to know what the fraudsters can do with this information. Facebook terms and conditions say promotions and giveaways must not require entrants to 'like' the page (known as 'like farming').



For fraudsters, a page on social media with a big following = big bucks. One of the Currys PC World scams amassed over 56,000 likes. This page can then be sold on to others who will then change its name and image and use it to target the unsuspecting followers in other scams.

How to spot fake competitions:

- Verified companies will have a blue tick next to their genuine social media accounts. Some companies will not so this is not a one stop way of checking if it is a scam.
- Is there a link to a genuine website in the post? It's probably a scam if not. 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 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.

We don't want to deter from the genuine prize giveaways, but please make sure that you undertake the above checks before entering competitions.

"Odd One Out" Competitions

We have recently spotted a number of suspicious posts on Facebook. These posts usually show an image of lots of numbers, letters or words repeated over and over. Other users are asked to spot the "odd one out" and to post their answers in the comments in order to win a cash prize.

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

Please be very cautious of these posts. Ask yourself what the person posting the picture has to gain? Are they really likely to be a good Samaritan looking to hand out money to total strangers? Could they be fishing for your personal and financial information?

Brushing and Fake Order Notifications

Brushing

You may not have heard of “brushing” in a fraud context before, but you might have experienced it. An article on the Which? website estimates that over 1 million UK households may have already been affected by brushing.

This tactic is being used by unscrupulous online retailers, usually those that are selling on well established platforms such as eBay and Amazon. These retailers want to make sure that their goods appear in the first couple of pages of results when a customer is searching for a product. This is because most shoppers only check the first two or three pages of results when looking to make a purchase. To get onto these pages, the retailer needs to have a strong volume of sales. If they are not able to achieve this legitimately, they may turn to brushing.

Brushing involves sending out unsolicited parcels of random goods to unsuspecting members of the public. The retailer will log it as a sale, even though no order was placed. Although the recipient isn’t charged for the items, continuing to receive parcels that were never ordered can be distressing and confusing. Amazon have asked anyone who receives an unsolicited parcel to report it to them immediately. You can read the full Which? article on their website here.

Fake Amazon Customer Service Emails

A new scam technique has been identified in which fraudsters send out fake Amazon order notification emails. The emails which are sent out are designed to get you to ring a fake customer service number which is given within the message.

If you do call the customer service number, it is likely that you will not get through to anyone. Later, you will get a call back and the caller will claim they need your financial information to cancel the order. They will try and persuade you to hand over your credit card number and the three digit CVV code from the back of your card.

These emails are particularly sneaky as they include several genuine links to the real Amazon website. By including these links, the recipient might feel reassured that they are dealing with an email from the genuine Amazon customer service team.

If you receive an email that might fit with this particular scam, you should visit the Amazon website by typing their web address into a fresh page on your browser. Alternatively, you can use their official app in order to find the customer services phone number. You should also be able to check the order history on your genuine Amazon account so you should be able to check that the items listed in the scam email have not actually been charged to your account. As ever, please do not click on links or attachments on emails if you are not certain that it is from a legitimate sender.

Protecting Yourself Online

It can be overwhelming trying to keep up with the variety of scams and tactics which are being used online. There are some simple things you can do to improve your online security. Here are some top tips:

1. Use separate, strong passwords for your various online accounts. You don’t want one compromised password to unlock all of your other accounts.

2. Where it is available, turn on multi-factor authentication. If you’re only going to activate this on one of your online accounts, turn it on for your email account. If someone manages to get into your email account, they can reset passwords to all your other online accounts.

3. If you find it difficult to remember lots of different passwords, use a password manager to help you. You can install these as mobile phone apps or as add-ins to your web browser. If you would like to read more about these programmes and how they work (and keep your passwords safe), you can find further information on the National Cyber Security Centre website.

4. Don’t rush any purchases. Fraudsters often use pressure and urgency to try and trick us into making mistakes. When shopping online, this could look like adverts for time-limited discounts and sales. This is also a legitimate sales tactic that is used by some retailers (for example, Amazon lightning-deals), but often it is a method for getting people to quickly complete purchases without taking the time to check all of the details are right.

5. You can check whether your email address has ever been involved in a data breach by visiting Have I Been Pwned? If your address has been affected, the website will give you advice on how to improve your account security.

6. Consider joining one of our Fraud Prevention Masterclasses if you’d like to learn more about protecting yourself from cyber-enabled fraud risks at home and at work. You can find details of the dates and times, as well as information on how to book a place on the next page.

Cyber Enabled Fraud Prevention Masterclasses

The counter fraud team are running a number of cyber enabled fraud prevention masterclasses for NHS staff during December. These sessions are ideal for anyone who wants to refresh their knowledge of common cyber enabled fraud tactics that might be seen at home and at work.

The sessions are being delivered via Microsoft Teams. Content which will be covered includes:

- How to spot fraudulent emails and how to report them to the appropriate authorities.
- What makes a good password and how to increase your account security measures.
- How telephone and SMS fraudsters operate and actions you can take if you're unsure about a call or text you receive.
- How to report cyber enabled fraud attempts made against you at work or at home.

The sessions are running on the following dates:

- 2nd December 10-11
- 8th December 2-3
- 14th December 1-2
- 20th December 11-12

To book a place on one of these sessions, or for details of our other Fraud Prevention Masterclasses, please contact rosie.dickinson1@nhs.net

How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:

Steve Moss, Head of Anti-Crime Services	Steven.moss@nhs.net 07717 356 707
Marie Hall, Assistant Anti-Crime Manager	Marie.Hall15@nhs.net 07970 265 017
Rosie Dickinson, Local Counter Fraud Specialist	Rosie.dickinson1@nhs.net 07825 228 175
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Local Counter Fraud Specialist	R.maw@nhs.net 07771 390544