# Fraud Alert

MIAA Anti-Fraud Service

November 2022

## ‘Black Friday’ & ‘Cyber Monday’ Fraud Alert

Beware of Black Friday and Cyber Monday Scams. Fraudsters step up their activity around Black Friday every year. You’ll find details of common Black Friday Scams below – remember, if something looks too good to be true, it probably is. With the price of everything on the increase, don’t fall into the temptation trap.

### Fake Black Friday and Cyber Monday Deals - Emails and Texts

These messages will tempt you by offering “exclusive” discounts and deals – all you need to do to access the offer is to click on a link. However, the link will take you onto a phishing site which may be a convincing copy of the retailer’s real website. You will not receive the item you have paid for, leaving you out of pocket and with your personal/financial information in the hands of fraudsters. These scams can be hard to tell apart from genuine marketing materials sent out by retailers.

Fraudsters use the usual ‘social engineering’ techniques to try and persuade, pressure and deceive you into responding.

### Some give away signs include:

- The offer is designed to be “unmissable” – they are offering an amazing discount, or access to a product which is sold out everywhere else (such as the latest smart phones, games consoles, or luxury items).
- The message claims that to access the offer you must click on a link.
- If you open a browser and visit the retailer’s official website the offer will not be shown.
- The text or email may also claim that this is a time-limited offer, or that only the first 50 people to order will get the discounted price. This is a tactic to pressure you into acting quickly without thinking it through.
- The message may appear to be from a company you know, but the sender’s details are slightly different from their usual contact methods. It may look legitimate at first glance – but doesn’t quite match what you’d normally see.
- When you hover over the links in the email, you don’t recognise the web address which pops up.
- The message may be from a company you’ve never previously interacted with or heard of.

Be very cautious of offers that seem “too good to be true”. Do not click on links in texts or emails. Instead, go the long way round by opening a browser and navigating to the retailers website, or use their official app if they have one. If you are being pressured to make a quick decision, stop and consider whether you could be being scammed.

**ACTION REQUIRED**

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

**GP Staff for ACTION & AWARENESS**

MIAA IA 22/23 1

For further information on MIAA’s Anti-Fraud Service visit https://www.miaa.nhs.uk/services/anti-fraud/

## Social Media Scams Posting dodgy deals.

Throwaway or hijacked SM accounts may also be used to post links to what appear to be amazing deals and discounts. These posts are similar to phishing emails and work by stealing your personal and financial information once you've clicked on the link. Use the principles above to help you spot fake posts.

## Competition scams.

Social media scammers also post fake competitions where you're promised the chance to win a voucher, a prize, or cash. Some brands will run genuine promotions on social media, which makes it trickier to spot the scams.

• Large and well-established brands should have a blue verification tick next to their profile name.

• If it's a smaller brand, have a look at their page and see how long it has been active, what their official website is, whether comments on posts are allowed, and whether there are any reviews on sites such as Trust Pilot or on wider social media in general.

• If a competition requires you to provide your personal or financial information, please think twice about entering.

**And remember, DO NOT use any login, password or information details that relate to your NHS email account or any NHS access details. Your personal and NHS passwords should be completely separate.**

# Take Five test– phishing emails

You can report phishing scams and unsolicited emails to Action Fraud online at https://www.actionfraud.police.uk/ and report@phishing.gov.uk. You can also forward an email regarding your personal bank account that's suspicious or contains links etc. to your bank. All banks have an email to report phishing emails to which you can find on your bankers website.

Also, you can send any phishing emails you receive to your NHS.net account to spamreports@nhs.net (and then delete the message).

**For further information visit:**

- https://www.actionfraud.police.uk/
- https://takefive-stopfraud.org.uk/
- https://report.ncsc.gov.uk/
- https://www.miaa.nhs.uk/services/anti-fraud/

TAKE FIVE TO STOP FRAUD™

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040