**Phishing**

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

It is critical for all users to be able to recognise phishing/scam emails. Recognise the signs someone is trying to scam you and learn how to check if a message you have received is genuine.

If a message or call makes you suspicious, stop and consider the language it uses. Scams often feature one or more of these tell-tale signs.

* **Authority** - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
* **Urgency** - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
* **Emotion** - Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
* **Scarcity** - Is the message offering something in short supply, like concert tickets, money, or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.
* **Current Events** - Are you expecting to see a message like this? Criminals often exploit current news stories, big events, or specific times of year (like Covid, tax returns etc.,) to make their scam seem more relevant to you.

**How to check if a message is genuine**

* If you have any doubts about a message, contact the organisation or individual directly. Don’t use the numbers or address in the message – use the details from their official website.
* Remember, your bank (or any other official source) will never ask you to supply personal information via email.

**Reporting an email, you think is a Phishing/Spam/Scam**

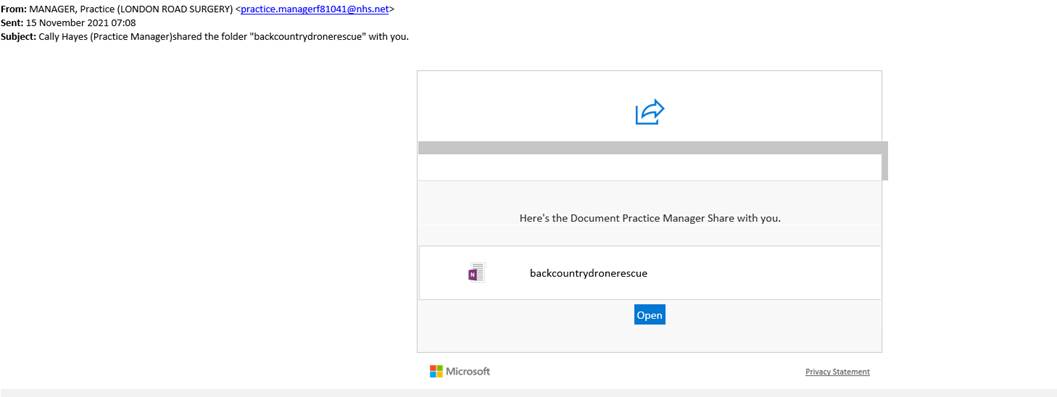
If you have received an email which you suspect is phishing/spam/scam, forward it to the following email ids

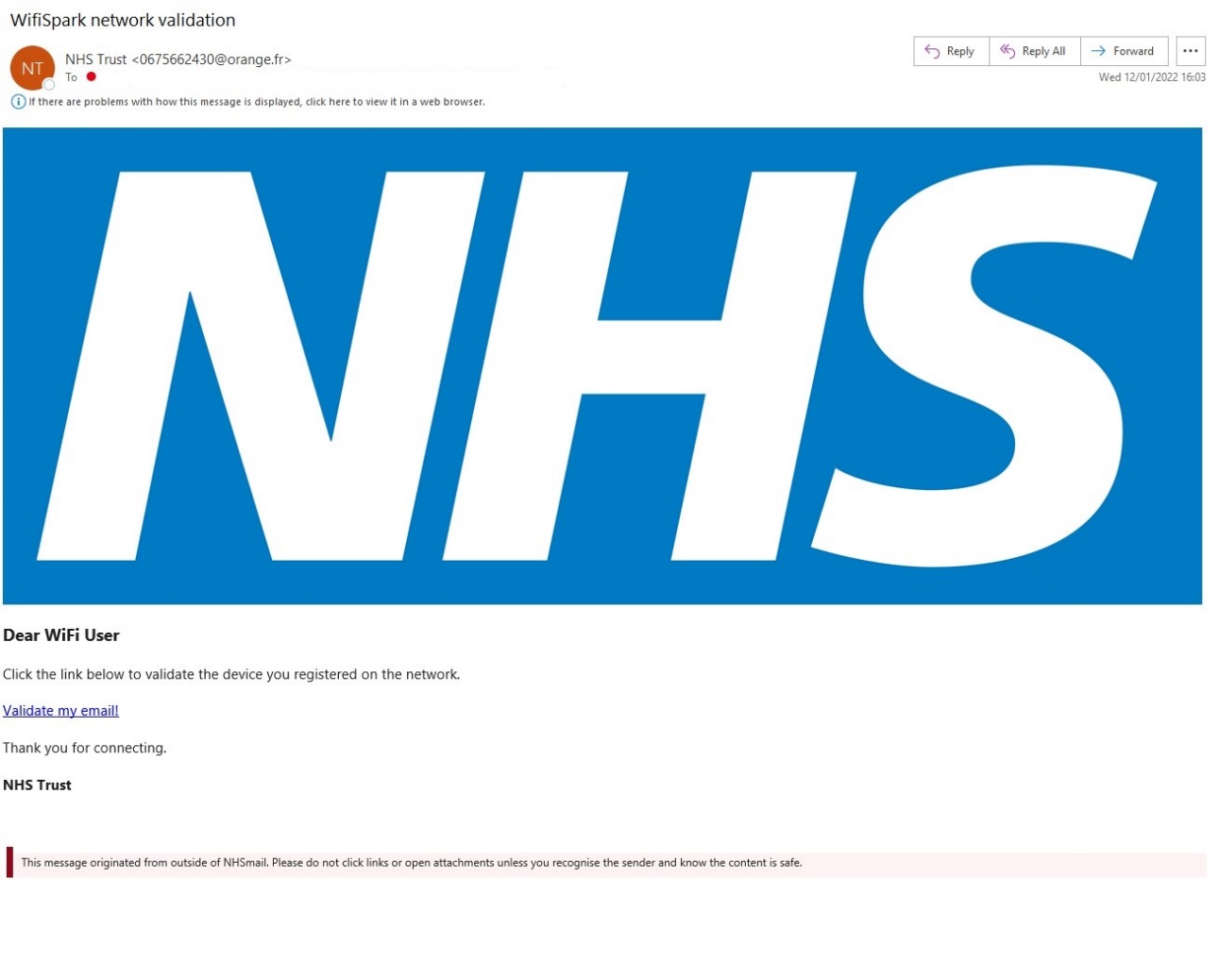
* [spamreports@nhs.net](mailto:spamreports@nhs.net)
* [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

**DO NOT CLICK ON ANY OF THE LINKS IN THE SUSPICIOUS EMAIL OR FORWARD IT TO ANYONE OTHER THAN THE ABOVE EMAIL IDs.**

**DELETE THE EMAIL IMMEDIATELY AFTER FORWARDING TO ABOVE EMAIL IDs.**

**Examples of Phishing/Scam Emails**





**What to do if you have shared sensitive information:**

What to do if you’ve been the victim of a scam, or you’ve been tricked into sharing info such as passwords or bank details.

Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust.

**If you have clicked on a link and/or entered personal details, contact Arden & GEM CSU IT Service Desk on 0300 123 1020 immediately.**

**How to reset your Nhs.net credentials:**

1. Login to Nhs.net from a browser by going to [www.nhs.net](http://www.nhs.net)
2. Click on **Profile** tab and then **My Profile**
3. Click on **Change Password**

