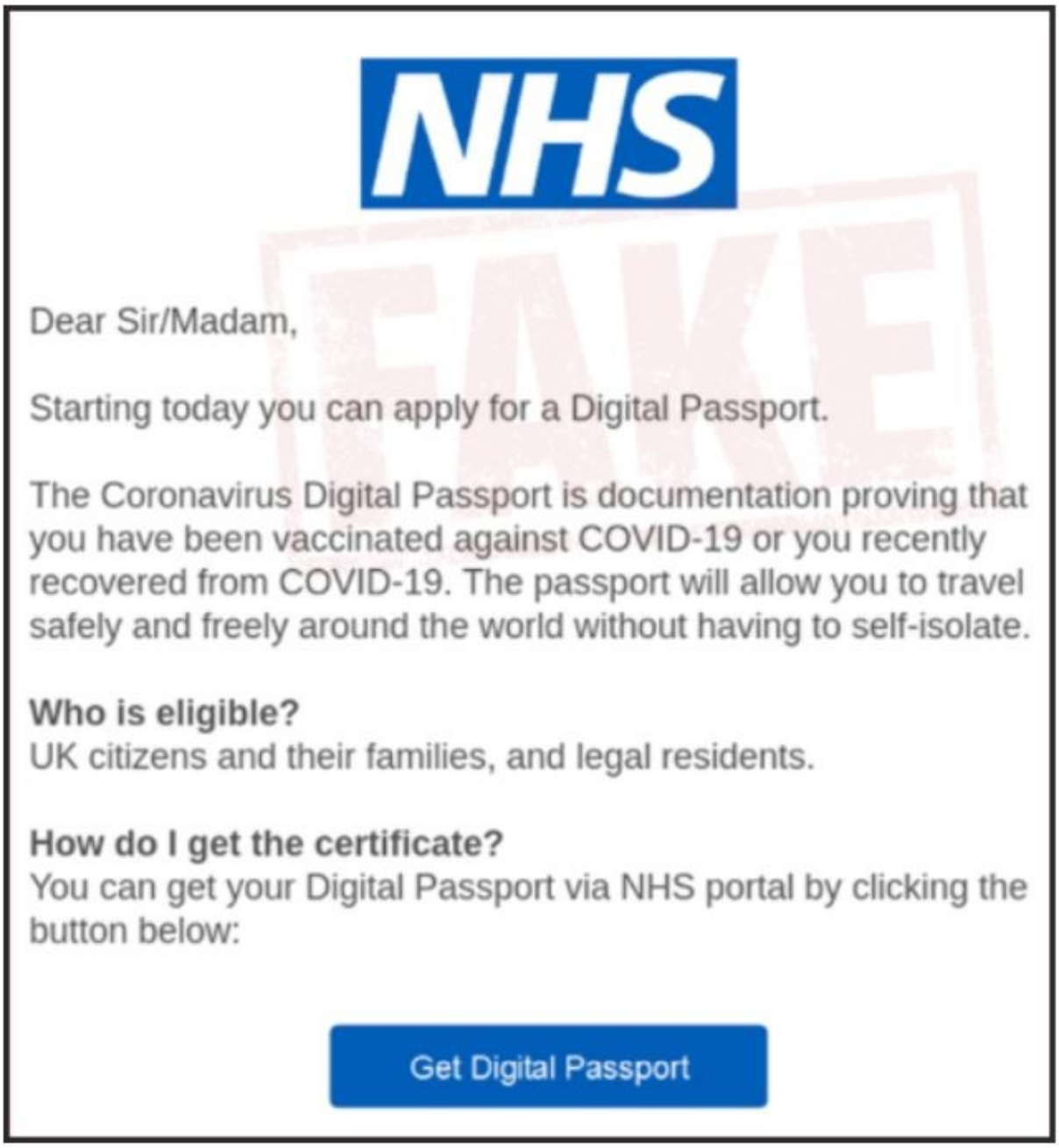
Information Security:

Phishing Alert

Action Fraud have recently issued an alert after receiving high number of reports of a circulating scam email regarding ‘digital coronavirus passports’.



Phishing is a major threat to both business and individuals, with attackers using social engineering to defraud individuals or trick them into providing their credentials for email, social media, online shopping or other web based accounts.

Do not respond to suspicious emails. If you believe that you may have been a victim of a phishing attack then report the incident immediately.

Protect both yourself and the business from phishing attacks:

Be suspicious of unknown senders - Always be wary of unsolicited emails and new contacts reaching out, as well as any unexpected links and attachments in emails. In fact you should sense check the validity of any email you receive, whoever has sent it. Stop and think, does the email look and feel right both in content and what is being requested? If you have any doubts, validate the enquiry through alternative means - not via interacting with the requester by email.

Don’t click on links - Any link in any email is inherently dangerous. If a customer, vendor, supplier—or anyone, for that matter—sends you a link do not click on it unless you were explicitly expecting it and it’s from a known source. Open up your browser and manually navigate to a website by typing its name into the URL bar rather than using a link embedded in an email.

Don’t give away your credentials -The only time you should enter your email address, password, account information or credit card number online is if you navigate directly to a website and/or a login.

Never email or message your credentials to someone.

Beware the Urgent Action - Look out for e-mails that convey a sense of urgency, fraudsters often rely on victims clicking before having thoroughly thought about the situation. Attackers will often try to drive an emotional reaction, using fear tactics, urgent language, and offers that seem too good to be true.

Minimise available data - In the event that your email account is ever compromised limit the potential damage an attacker can inflict by regularly reviewing and deleting emails from your inbox and sent items. Remember to regularly empty the Deleted Items folder.