Fraud Information Alert 2

MIAA Anti-Fraud Service

June 2022

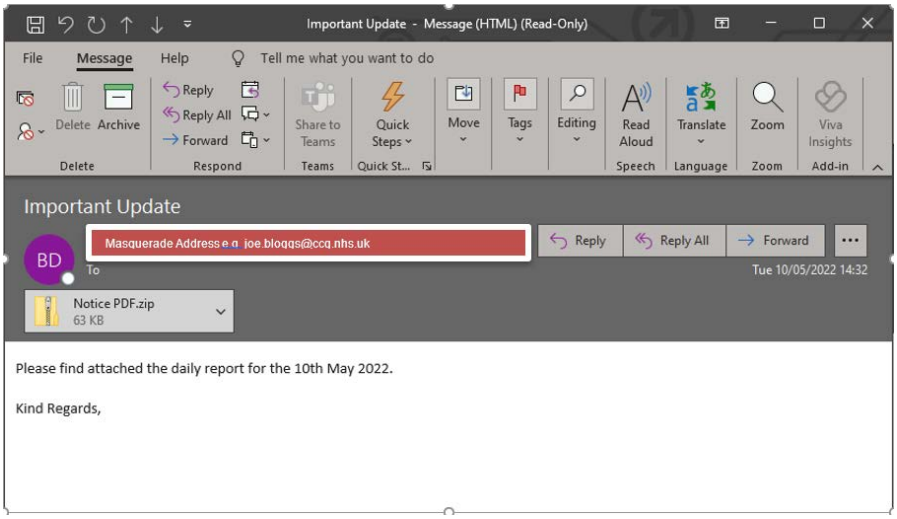
Targeted Phishing Campaign by Fraudsters

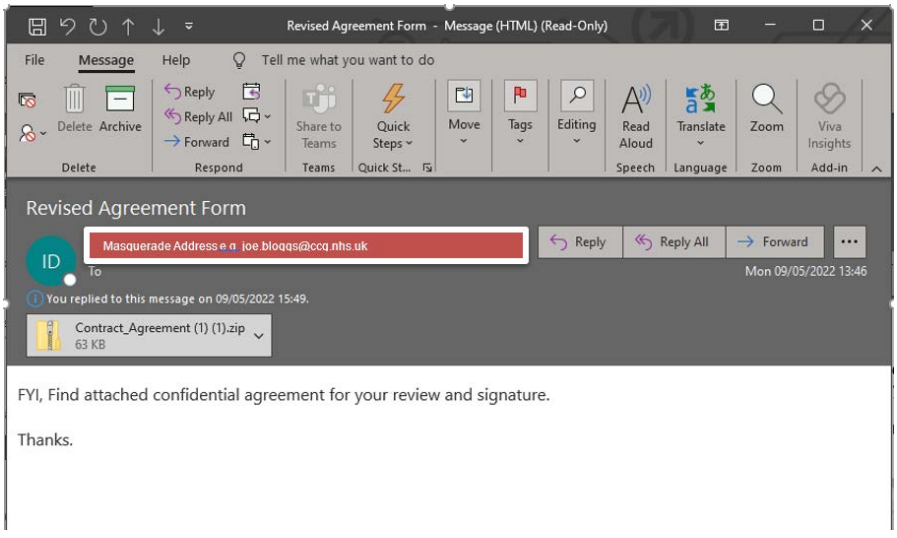
We are aware of a phishing campaign that is currently targeting NHS staff.

Phishing emails, containing malicious attachments, are being sent directly to colleagues from email addresses which have been masqueraded and look legitimate (in some cases referencing a familiar name within your organisation or NHS in the email address) but are actually being sent from someone else.

Please be extra vigilant and do not respond to the message or open any links or attachments if you cannot be sure the email is genuine.

Examples of these emails.





ACTION REQUIRED

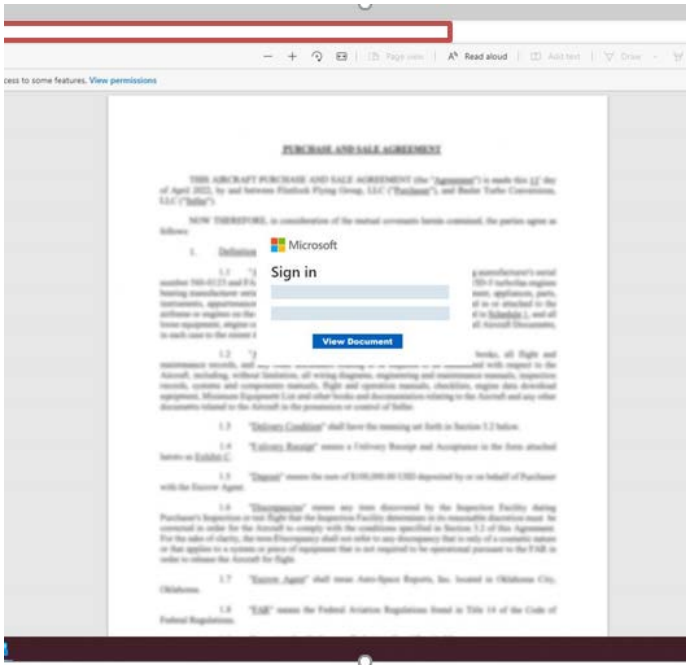
MIAA Anti-Fraud Service recommend this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

MIAA IA 22/23 2

For further information on MIAA's Anti-Fraud Service visit miaa.nhs.uk

If an attachment is opened, in some cases, you may be asked to sign-in to your Microsoft account as shown in the example below. Please do not sign-in.



139 NHS Email Accounts compromised by Phishing Campaign
An NHS-targeted phishing campaign has been uncovered, with 139 NHS email accounts known to have been compromised. These accounts have been used to distribute at least 1,157 phishing emails. The campaign appears to have started in October 2021 and reached a peak in March 2022. It is believed that there are likely to be more compromised email accounts which have not been identified yet.

NHS Net Email Account Password Reset Scam
The email below was sent to an NHS employee and is likely 1 of 139 email accounts compromised in NHS Email Accounts following the Phishing Hacks. This hacked email is now being used by scammers to try to capture your NHS net password details.

If you receive it do not click on the link but report the email to spamreports@nhs.net

Self-service NHS Net Password– The correct Reset
If you have forgotten your password you will need to use the self-service password reset feature within the NHSmail Portal, over the internet or the Health and Social Care Network / Transition Network. For further details go to Reset your password – NHSmail Support . On this web page the correct link to the reset is present as shown below:

What do you need to do if you receive a phishing email?
If you receive a phishing email, similar to the above, do not respond to the message and do not open any links or attachments within the email. Please immediately forward anything suspicious to spamreports@nhs.net and delete the message.

Guidance on phishing emails from NHS Digital: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-phishing-emails

Fraudulent SMS Messages
Please be aware that fraudsters are still using Fake NHS SMS messages to harvest data and scam money for fake Covid tests. SMS messages similar to the one below are still circulating. In the example below, the link containing .com is obviously not an NHS site. In addition, the NHS does not ask for money or personal details via SMS messages.

Further information and support
Whilst the digital devices and IT systems you use are monitored around the clock to identify and respond to potential threats, using the latest innovative technologies, all colleagues are asked to remain vigilant and follow IT security best practice to help keep you, your colleagues and your patients secure.

For further information on the risks to look out for as well as handy hints and tips on how to be cyber savvy, please visit https://www.be-cybersavvy.co.uk/

Information for individuals and families
Cyber security information from the National Cyber Security Centre https://www.ncsc.gov.uk/section/information-for/individuals-families

TAKE FIVE TO STOP FRAUD™

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040