Changes to spoofing controls on the NHSmail Service

Version 4
November 2018

Contents

Background – what is spoofing?

Email 'spoofing' is the forgery of an email address to give the appearance of being sent from someone or somewhere other than the actual sender. In other words, hiding one's identity or faking the identity of another user / organisation in an email.

Some senders of spoofed emails are from NHS organisations and they are spoofing for operational reasons. For example, they may have a contract with a mailing company for sending out newsletters to staff or reminders to patients.

Other spoofed emails are scams or malicious and are attempting to lure users into clicking on links or providing sensitive information.

Operational emails have been spoofed in the past because there has not been the ability to link internet-based mailing tools into the NHSmail Service using standard methods based on SMTP / POP / IMAP.

Spoofed emails are now being marked with the following message informing the recipient they are receiving a spoofed email:

> ---This email is being marked as junk as the message was sent from an email address external to NHSmail but gives the appearance of being from an NHSmail address. Verify the sender and content is legitimate before acting upon information contained within. You must also notify the sender to advise that they will need to take action to stop 'spoofing' @nhs.net. ---

Why is spoofing going to be stopped?

NHSmail is introducing an approach to prevent emails being sent from spoofed @nhs.net addresses from being delivered into NHSmail inboxes.

This is being introduced to protect the NHSmail Service and to ensure that senders are sending emails legitimately from @nhs.net addresses.

How are the changes being implemented?

The changes being introduced will prevent the practice of spoofing @nhs.net addresses and will be introduced in two stages, which have now started:

Phase one: Any emails spoofing the @nhs.net name are now being directed to a user's 'junk' mailbox instead of the inbox. This means the user will still receive the email, but they will have to search for it in their junk mail folder. This change reinforces the text warning that the email is spoofed and should be treated carefully. We explain below how to ensure operational emails can continue to be delivered to email inboxes.

Phase two: Any emails continuing to spoof at @nhs.net will be deleted from the NHSmail Service and will not be delivered to a user's account.

When will the changes come into force?

Phase	Activity	Date
One	Spoofed email delivered into NHSmail account junk mail folders	Implemented 31 October 2018
Two	Spoofed emails will not be delivered to NHSmail accounts	Early spring 2019

Specific dates for phase 2 will be communicated to NHSmail Local Administrators, Users and known suppliers as soon as they are confirmed.

Who will be impacted by the spoofing changes?

These changes are affecting:

- Users of the NHSmail Service who are currently receiving spoofed emails.
- Senders currently spoofing @nhs.net email addresses.

What actions need to be undertaken to ensure business processes are not impacted?

Recipients of spoofed email

- Users will need to pro-actively identify emails they receive that are being spoofed. All messages are tagged within the top of the email content with the following message:

  ---This email is being marked as junk as the message was sent from an email address external to NHSmail but gives the appearance of being from an NHSmail address. Verify the sender and content is legitimate before acting upon information contained within. You must also notify the sender to advise that they will need to take action to stop 'spoofing' @nhs.net. ---

- Users should contact the sender (in a separate email) to advise that an email has been received and it has been tagged as a spoofed email. Let the sender know that they need to stop spoofing, as measures are being taken to prevent this and eventually their emails will be blocked from the NHSmail Service if they continue to spoof @nhs.net.

Senders of spoofed email

If you send large volumes of email using an internet-based email service that is pretending to send from an @nhs.net email address, you are sending spoofed email. You should take immediate action to stop spoofing using one of the following options:

- **SMTP / POP / IMAP** – these protocols are now available over the internet. Health and social care organisations should apply for an NHSmail application email account and

send, legitimately, from an @nhs.net. The Applications Guide for NHSmail has more details on setting up access.

- **No NHSmail account** - senders without an NHSmail email account, who are currently spoofing, will need to send emails from their internet-based email domain using the proper name (for example, nhs.uk), rather than @nhs.net.
- Stop sending the spoofed emails.

Further guidance on the anti-spoofing controls is available on the Policy and Guidance page of the NHSmail Portal, under section ‘General Guidance’.