NHSmail

Cyber Security Guide for NHSmail

Version 3.0
February 2017

Contents

Introduction

Purpose of Document

Target audience: all NHSmail users

This guide gives information on how to keep your account and the NHSmail service safe and secure from common cyber threats such as spam, junk, spoofing and phishing. A brief definition of each term is given below.

Junk – *Junk email (also known as spam) involves the sending of nearly identical messages to numerous recipients.*
Malware – *A term used to refer to various forms of intrusive or hostile computer software, such as viruses, worms and trojan horses.*
Phishing – *The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.*
Spam – *Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.*
Spoofing – *The creation of email messages with a forged sender address. A forged sender address uses a respected or reputable origin email address to conceal the fact that the email has come from elsewhere.*

This guide provides some information on how to spot common cyber threats and how to report these threats to the NHSmail service if you receive them.

How to identify common cyber threats

If you receive an email that you suspect to be spam, or suspect may be an attempt to spoof or phish your account, it is extremely important that you report this to the NHSmail helpdesk using the instructions in the Reporting Cyber Threats section of this document. Below are some tips on how to identify common cyber threats such as spam, junk, spoofing and phishing.

- **Check for legitimate URLs** – hover your mouse over any URLs that the email is trying to get you to visit to make sure that it is legitimate. You should never open any links from unknown senders.
- **Request for personal information** – a common tactic of spam emails is to alert you that you must provide or update personal information, including bank account details or an account password. You will **NEVER** legitimately be asked to provide your NHSmail credentials to anyone.
- **Urgent emails** – if an email seems too good to be true, it most likely is. Be cautious of any email offering to place money into your bank account etc. If the email uses any kind of urgency, asking you to “log in *now*” for example, this may also be evidence of spam.
- **Incorrect grammar/spelling** – many hackers use misspelled words and bad grammar on purpose. This is a tactic used to identify an easy target that may not

identify the errors and may do as the email instructs them, such as providing bank/personal details.

- **Plain text/Absence of logos** – the majority of legitimate emails will be written with HTML (HyperText Markup Language) and will be a mix of text and images. If an email is all plain text and does not include images such as a company's logo, this may be evidence of spam.
- **Suspicious attachments** – if a source that does not normally send you attachments, such as your bank, sends an email with an attachment, this may be evidence of spam. You should never open attachments from unknown sources.
- **Legitimate sender** – if you receive an email purporting to be from an official agency or bank, the sender address should reflect this. For example, an email that claims to be from a government agency but is sent from "abc.smith@yahoo.com" is clearly not legitimate. If you are in any way suspicious of the request, you should contact the sender by phone or other established channels (not those in the email) to confirm the legitimacy of the sender and the request.
- **'From'/'To' Address** – If you notice that your email address is being used as the 'From' address, this is a sign of a fake email message. Furthermore, you should also be cautious if the 'To' field shows a large number of recipients.

Reporting Cyber Threats

If you receive an email that you suspect to be spam, or suspect may be an attempt to spoof or phish your account, it is extremely important that you report this to the NHSmail helpdesk.

You will **NEVER** legitimately be asked to provide your NHSmail credentials to anyone. Do not respond to or follow any links within an email that asks you for your login details. If you receive an email asking you for your NHSmail account credentials please report it following the instructions below. If you have responded in any way to any such email please contact your Local IT service desk immediately and report it to them in the first instance. They will be able to provide initial support and advice on further actions, such as password changes.

In order for the service to efficiently process your spam report please ensure that you have attached a copy of the offending email in .eml or .msg format. This must be attached directly from your mailbox (not from a forward or copy). The guidelines below explain how to do this and report it to: spamreports@nhs.net.

If you choose to simply mark an email as junk in Outlook, the sender's emails will no longer arrive in your inbox but the threat will not have been reported to the NHSmail service and may still affect other users.

If you have already attached a copy of the spam mail in the correct format, and it has been taken directly from the recipient's mailbox, then it will be uploaded to the spam filters for blocking. Please allow up to 48 hours for this blocking process to take effect. No further correspondence will be required.

Reporting threats with Microsoft Outlook 2010

Forward the email to spamreports@nhs.net as an attachment for virus analysis and central trend monitoring:

1. Select the suspect email from your email list
2. In the Outlook ribbon in the respond area, select 'More' and then select 'Forward as Attachment'.
3. In the email window that opens add spamreports@nhs.net as the recipient in the 'To field'.
4. Click **Send**.

Reporting threats with Outlook Web App (OWA)

Follow the instructions below to save a copy of the email you suspect is spam in Outlook Web App (OWA – www.nhs.net

1. Click on the Spam Email in the reading pane to select it
2. Click on the **New mail icon** in the top left of the screen
3. Drag and drop the spam email from the email list into the body of the new blank email
4. Type spamreports@nhs.net into the To: field
5. Enter the appropriate subject text
    a. Note: It is recommended that you use spam, phishing or malicious depending on the type of email you are reporting
6. Click **Send**

Permanently deleting suspicious email (by-passing the deleted items folder).

If using OWA (www.nhs.net) or Outlook

- Select the suspect email from your email list
- Hold down the 'shift' key and press the 'Delete' key
- Click 'Yes' to confirm if a warning dialogue appears.

Warning Messages

If you receive any spam emails which contain the warning *"NHSmail detected and removed a file named (name of file sent to you)"* please proceed to delete the email without reporting it to us. The NHSmail spam filters have added that message and removed the file for your protection as they have already identified a potential threat in the original content. No further action is necessary. However, if you believe a legitimate email has been incorrectly filtered, contact your Local IT service desk who will be able to provide assistance in the first instance.

You may also receive an email which contains the following warning: *"This message was sent from an email address external to NHSmail but gives the appearance of being from an NHSmail(@nhs.net) address. The recipient should verify the sender and content before acting upon information contained within."* The NHSmail spam filters have added this

message as a warning for your protection to advise you that although it looks like the mail is sent from an nhs.net account, it is not. Caution should be used before acting upon the email. If you do believe this message to be unsolicited then please report it following the instructions in section 3.

Nuisance emails and blocking senders

If you receive nuisance emails such as newsletters, marketing or social media updates which you do not wish to continue receiving but do not think pose a threat, you can block the sender or sender's domain.

Blocking senders in Microsoft Outlook 2010

The easiest way to block a sender in Microsoft Outlook 2010 is to **right click** on the email in your inbox and choose **Junk** from the dropdown list. However, you may also want to block multiple senders at once, or block a sender that you have not yet received an email from. Follow the instructions below to do this with Microsoft Outlook 2010.

1. Click **Home** at the top of the screen and click on **Junk** in the menu bar.
2. Click on **Junk Email Options** from the drop down list
3. Select the **Blocked Senders** tab from the top ribbon of the window that appears on screen
4. Click **Add** on the right side of the window
5. Type the email address you wish to block and click **OK**
6. Repeat steps 4. & 5. to add more addresses you wish to block
7. When you have finished, click **OK** at the bottom of the window

You can also use the same **Blocked Senders** tab to remove a sender from your blocked senders list if you have added them in error.

1. In the **Blocked Senders** tab, highlight the email address you wish to remove and click **Remove**. You can highlight and remove more than one email address at once
2. Repeat step 1. to remove more addresses
3. When you have finished, click **OK** at the bottom of the window

Blocking senders with Outlook Web App (OWA)

The easiest way to block a sender in Outlook Web App (OWA) is to **right click** on the email in your inbox, select **Move** from the dropdown list and then select **Junk Email**. However, you may also want to block multiple senders at once, or block a sender that you have not yet received an email from. Follow the instructions below to do this with Outlook Web App.

1. Click on the settings icon at the top right of the screen and select **Options**
2. Click **Block or Allow** on the left side of the screen
3. Scroll down to the **Blocked Senders** section
4. Click the **plus** icon on the right side of the window
5. Type the email address you wish to block and press **Enter** on your keyboard

6. Repeat steps 4. & 5. to add more addresses to block
7. When you have finished, click **Save** at the bottom of the page

You can also use the same **Blocked Senders** section to remove a sender from your blocked senders list if you have added them in error.

1. In the **Block Senders** section, highlight the email address you wish to remove and click the **minus** icon. You can highlight and remove more than one email address at a time
2. Repeat step 1. to remove more addresses
3. When you have finished, click **Save** at the bottom of the page

Frequently asked questions

Can emails be encrypted?
Yes. For full details on how to encrypt NHSmail emails, please see the Encryption Guide available on the Portal Training and Guidance pages.

What security features are part of the NHSmail service?
The NHSmail email gateway has advanced threat detection for malware, as well as phishing and spam detection.

What can I do to protect myself against cyber security threats?
Always be aware of messages coming into your mailbox, especially from new unsolicited senders. Also, ensure appropriate antivirus software is installed and up to date on your PC.

How do I know if I have anti-virus software on my computer?
A program from vendors such as McAfee, Symantec, Sophos and Trend Micro would prompt you to update your virus definitions from time-to-time. Also, you should see the running application in the computers ‘system tray’ (close to the date and time of the computer).

If there is no obvious anti-virus running on your computer, you should contact your local IT service to confirm.

As NHSmail scans attachment types, does it mean all attachments received are safe?
No. Caution should always be exercised when opening email attachments. Extra care should be taken when messages come from unsolicited sources. If in doubt about the sender, never open an attachment until the sender has been verified.

Why is email malware filtering necessary?
Malware/viruses are not only annoying, they can corrupt essential data and information stored on a computer accessing the affected message. Once a single system is compromised, depending on the type of infection, security of the entire local network can be at risk. Therefore, it is very important to scan messages.

What should I do if I believe my system is affected by a virus or malware?
Contact your local IT department immediately.

How does virus filtering work, and do I have to do anything?
As an email user you don't have to do anything to benefit from the advanced filtering service in place for NHSmail. Depending on the route of the email (i.e. incoming, outgoing, being sent to nhs.uk, nhs.net or hscic.gov.uk addresses) messages pass through various 'checkpoints' with each check having separate rules for malware as well as spam scanning engines. Therefore, when messages reach your inbox, messages should be determined to be ok to read and reply. But, as outlined in this document caution should always be taken especially from unsolicited senders. To aid in the identification of spam, you are encouraged to send spam messages to spamreports@nhs.net through the process identified in this document. We also recommend that users occasionally check their Junk Email folder to ensure that legitimate emails are not placed there incorrectly.