Fresh Phish: Britain’s National Health Service Infected by Massive Phishing Campaign

Posted by Roger Kay

- Tweet
-

Over a period beginning last fall and continuing into April, the National Health Service (NHS) of the United Kingdom fell prey to a large phishing operation. What had been sporadic use of legitimate NHS accounts to send phishing emails to unsuspecting third parties became a massive campaign in March.

The true scope of the attack could have been much larger, as INKY detected only those attempts made on our customers. But given how many we found, it’s safe to say that the total iceberg was much bigger than the tip we saw.

INKY shared its findings with the NHS, which sent the following response:

“We have processes in place to continuously monitor and identify these risks. We address them in collaboration with our partners who support and deliver the national NHSmail service.

"NHS organisations running their own email systems will have similar processes and protections in place to identify and coordinate their responses, and call upon NHS Digital assistance if required."

Between background statements by the NHS and our investigations, we were able to determine that the breach was not a compromised mail server but rather individually hijacked accounts.

As of April 19, INKY mostly stopped receiving phishing reports from the NHS domain, likely due to the messaging team’s efforts to mitigate the incursion. One exception was the author, who received a simple request to reply to a Gmail account, sent from the NHS domain. Our data analysts found a few others scattered about our user base.

Quick Take: Attack Flow Overview

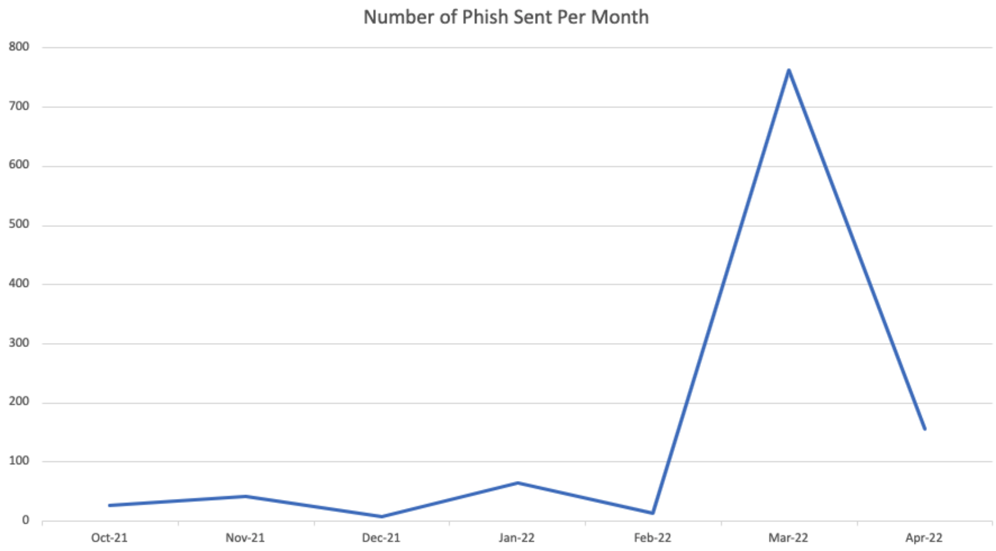
- Type: phishing
- Vector: emails sent from NHS servers
- Payload: credential harvesting links
- Techniques: brand impersonation, credential harvesting, hijacked accounts
- Platform: Microsoft 365

- Target: Microsoft 365 users

The Attack

Starting in October 2021 and escalating dramatically in March 2022, INKY detected 1,157 phishing emails originating from NHSMail, the NHS email system for employees based in England and Scotland. Last year, this service was migrated from an on-premise installation to Microsoft Exchange Online. This migration, with its changed security environment, could have been a factor in the attack.

We reported our initial findings to the NHS on April 13, and as of April 14, the volume of attacks decreased dramatically, as the NHS took measures to stop them. However, INKY users were still receiving a few phishing emails from the NHS mail domain (nhs[.]net) after that time.

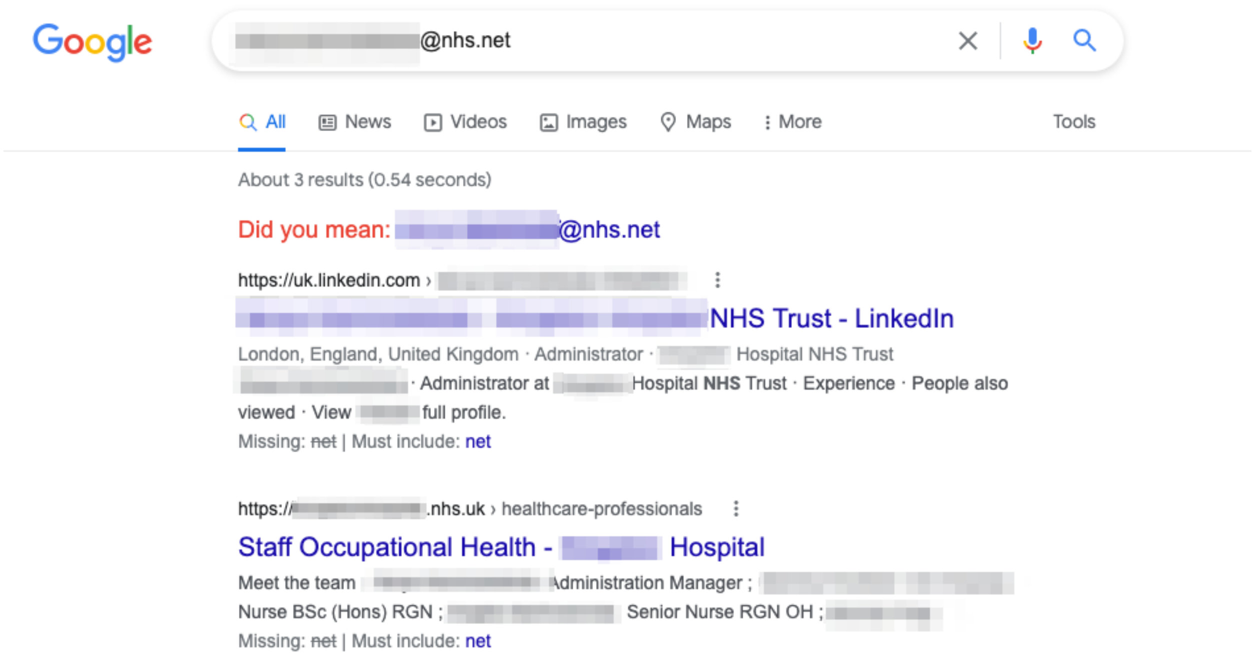


Graph of NHS phish sent per month

During the study period, the phishing emails originated from email accounts that belonged to 139 NHS employees.

INKY data analysts validated the email accounts via two methods:

> LinkedIn profiles and NHS staff directory links confirmed that these accounts belonged to real NHS employees.



[redacted]@nhs.net

About 3 results (0.54 seconds)

Did you mean: [redacted]@nhs.net

https://uk.linkedin.com › [redacted]

[redacted] NHS Trust - LinkedIn

London, England, United Kingdom · Administrator · [redacted] Hospital NHS Trust [redacted] · Administrator at [redacted] Hospital **NHS** Trust · Experience · People also viewed · View [redacted] full profile.

Missing: ~~net~~ | Must include: net

https://[redacted].nhs.uk › healthcare-professionals

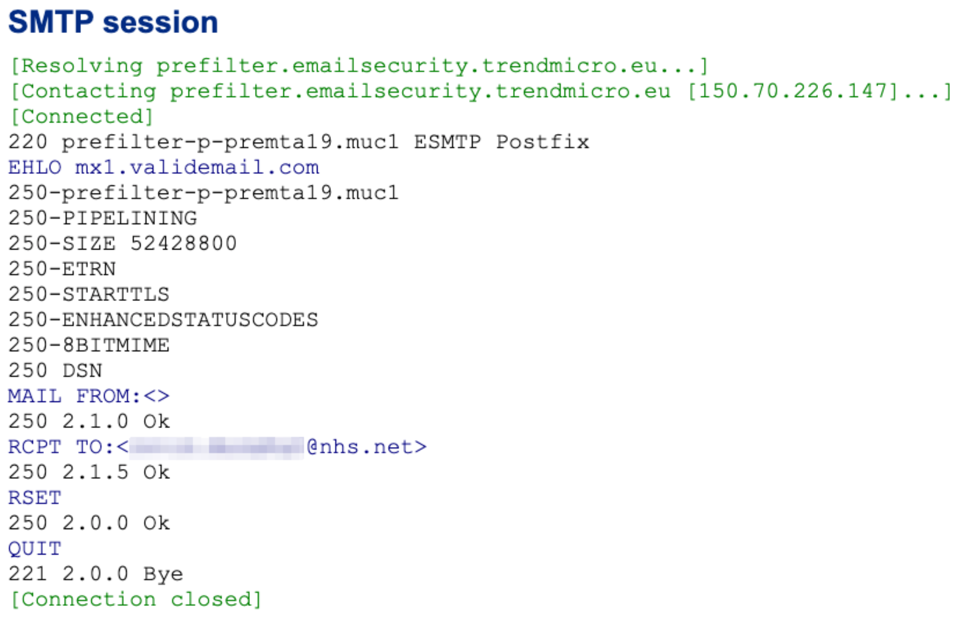
Staff Occupational Health - [redacted] Hospital

Meet the team [redacted] Administration Manager ; [redacted] Nurse BSc (Hons) RGN ; [redacted] Senior Nurse RGN OH ; [redacted]

Missing: ~~net~~ | Must include: net

Search results confirmed the identity of NHS employees with compromised accounts

> Pinging the SMTP server drew replies of “250 OK,” establishing that the email addresses existed. Although our spot checks were statistical rather than exhaustive, we got a “250 OK” response for every email that we checked.

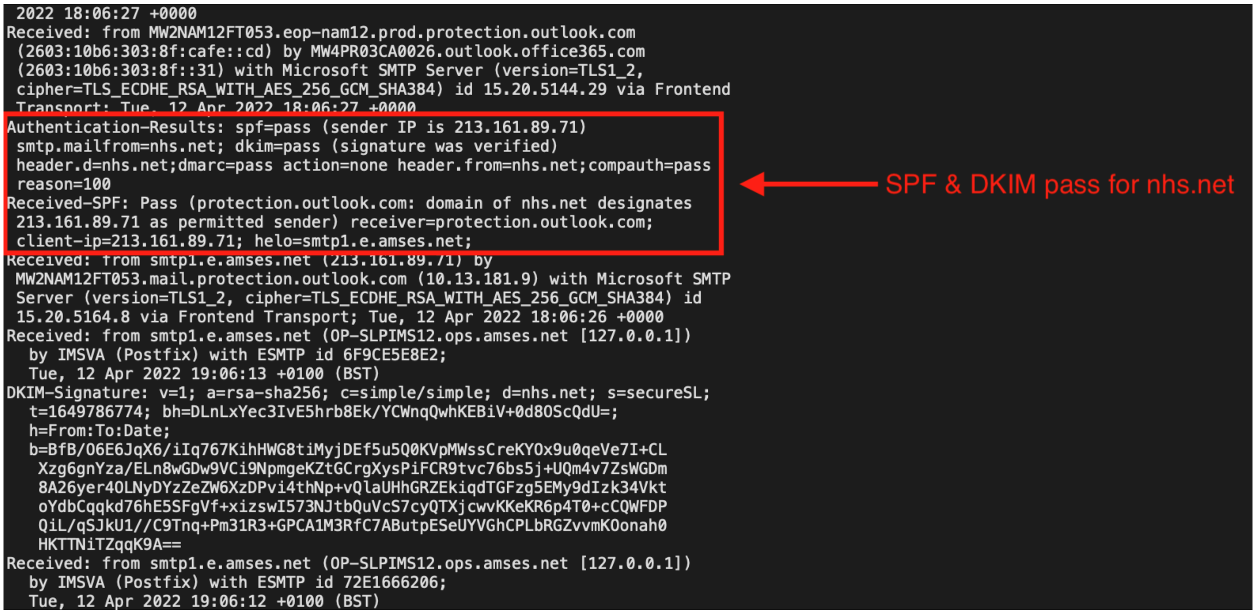


SMTP session

```
[Resolving prefilter.emailsecurity.trendmicro.eu...]
[Contacting prefilter.emailsecurity.trendmicro.eu [150.70.226.147]...]
[Connected]
220 prefilter-p-premta19.muc1 ESMTP Postfix
EHLO mx1.validemail.com
250-prefilter-p-premta19.muc1
250-PIPELINING
250-SIZE 52428800
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<>
250 2.1.0 Ok
RCPT TO:<[redacted]@nhs.net>
250 2.1.5 Ok
RSET
250 2.0.0 Ok
QUIT
221 2.0.0 Bye
[Connection closed]
```

Example of SMTP ping results

All phishing emails were sent from two IP addresses (213.161.89.71 and 213.161.89.103) used by the NHS. They also passed email authentication for nhs.net. The NHS confirmed that the two addresses were relays within the mail system used for a large number of accounts.

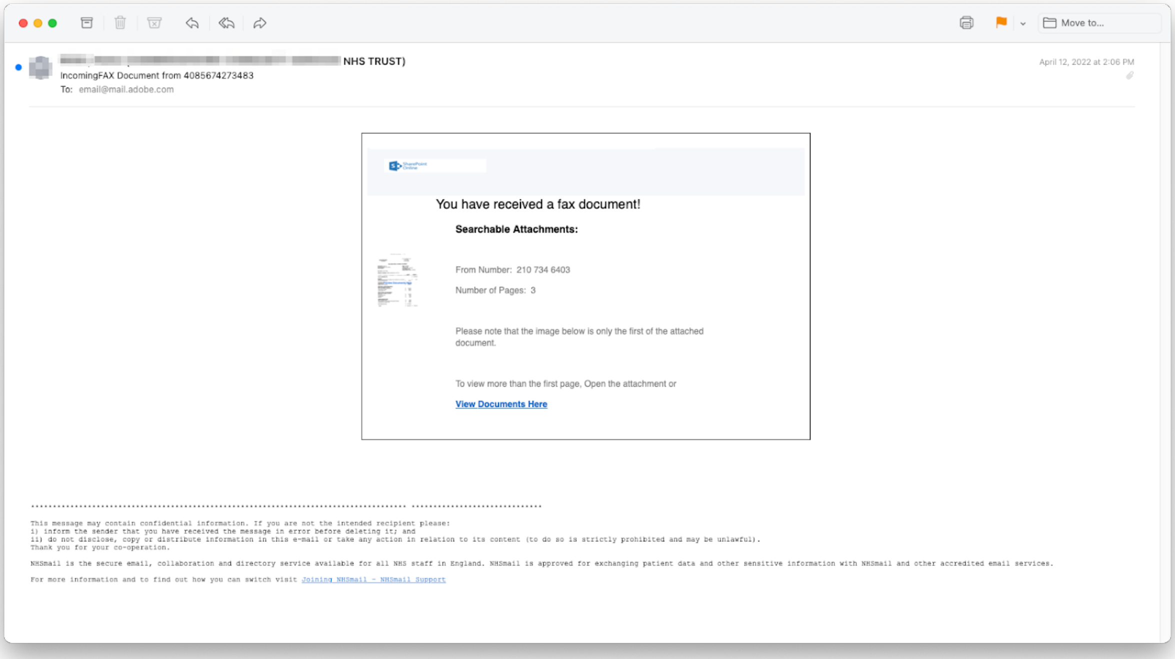


```
 2022 18:06:27 +0000
Received: from MW2NAM12FT053.eop-nam12.prod.protection.outlook.com
 (2603:10b6:303:8f:cafe::cd) by MW4PR03CA0026.outlook.office365.com
 (2603:10b6:303:8f::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5144.29 via Frontend
 Transport; Tue, 12 Apr 2022 18:06:27 +0000
Authentication-Results: spf=pass (sender IP is 213.161.89.71)
 smtp.mailfrom=nhs.net; dkim=pass (signature was verified)
 header.d=nhs.net;dmarc=pass action=none header.from=nhs.net;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of nhs.net designates
 213.161.89.71 as permitted sender) receiver=protection.outlook.com;
 client-ip=213.161.89.71; helo=smtp1.e.amses.net;
Received: from smtp1.e.amses.net (213.161.89.71) by
 MW2NAM12FT053.mail.protection.outlook.com (10.13.181.9) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5164.8 via Frontend Transport; Tue, 12 Apr 2022 18:06:26 +0000
Received: from smtp1.e.amses.net (OP-SLPIMS12.ops.amses.net [127.0.0.1])
   by IMSVA (Postfix) with ESMTP id 6F9CE5E8E2;
   Tue, 12 Apr 2022 19:06:13 +0100 (BST)
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=nhs.net; s=secureSL;
   t=1649786774; bh=DLnLxYec3IvE5hrb8Ek/YCWnqQwhKEBiV+0d8OScQdU=;
   h=From:To:Date;
   b=BfB/O6E6JqX6/iIq767KihHWG8tiMyjDEf5u5Q0KVpMWssCreKYOx9u0qeVe7I+CL
    Xzg6gnYza/ELn8wGDw9VCi9NpmgeKZtGCrgXysPiFCR9tvc76bs5j+UQm4v7ZsWGDm
    8A26yer4OLNyDYzZeZW6XzDPvi4thNp+vQlaUHhGRZEkiqdTGFzg5EMy9dIzk34Vkt
    oYdbCqqkd76hE5SFgVf+xizswI573NJtbQuVcS7cyQTXjcwvKKeKR6p4T0+cCQWFDP
    QiL/qSJkU1//C9Tnq+Pm31R3+GPCA1M3RfC7ABUtpESeUYVGhCPLbRGZvvmKOonah0
    HKTTNiTZqqK9A==
Received: from smtp1.e.amses.net (OP-SLPIMS12.ops.amses.net [127.0.0.1])
   by IMSVA (Postfix) with ESMTP id 72E1666206;
   Tue, 12 Apr 2022 19:06:12 +0100 (BST)
```

SPF & DKIM pass for nhs.net

All phishing emails authenticated to nhs.net

The majority were fake new document notifications with malicious links to credential harvesting sites that targeted Microsoft credentials. All emails also had the NHS email footer at the bottom.



[redacted] NHS TRUST)

IncomingFAX Document from 4085674273483

To: email@mail.adobe.com

April 12, 2022 at 2:06 PM

You have received a fax document!

Searchable Attachments:

From Number: 210 734 6403

Number of Pages: 3

Please note that the image below is only the first of the attached document.

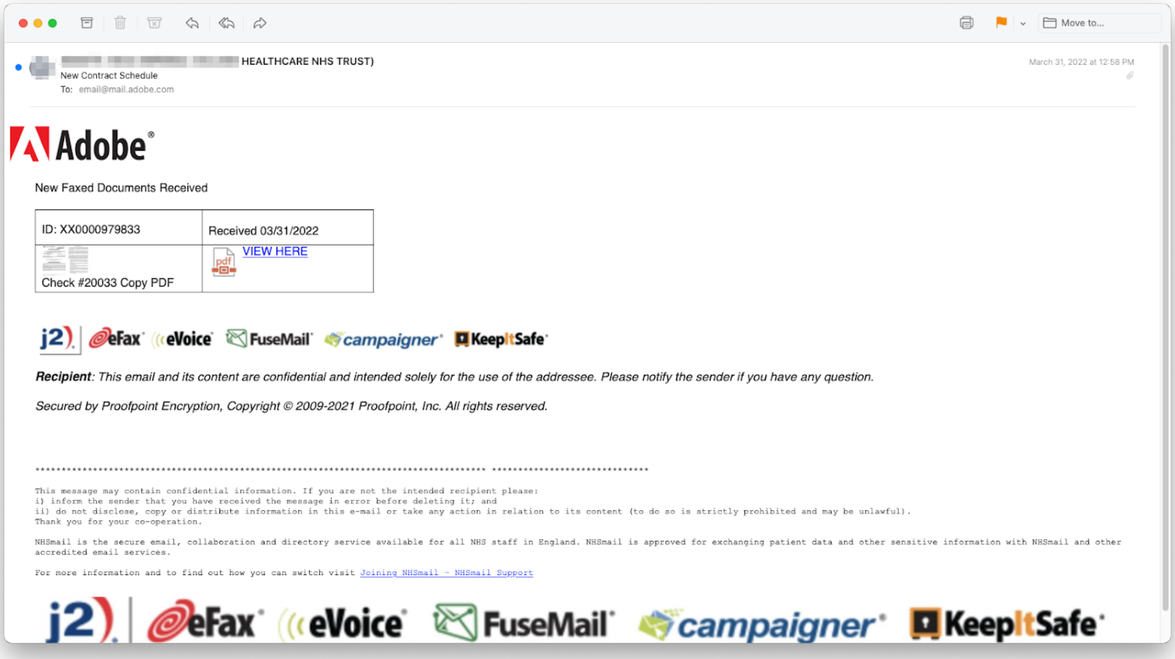
To view more than the first page, Open the attachment or

View Documents Here

```
***************************************************************************** ***************************

This message may contain confidential information. If you are not the intended recipient please:
i) inform the sender that you have received the message in error before deleting it; and
ii) do not disclose, copy or distribute information in this e-mail or take any action in relation to its content (to do so is strictly prohibited and may be unlawful).
Thank you for your co-operation.

NHSmail is the secure email, collaboration and directory service available for all NHS staff in England. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other accredited email services.

For more information and to find out how you can switch visit Joining NHSmail – NHSmail Support
```

Sample phishing email with NHS footer

Some emails impersonated Adobe and Microsoft by using their logos in phishing emails.



[redacted] HEALTHCARE NHS TRUST)
New Contract Schedule
To: email@mail.adobe.com

March 31, 2022 at 12:58 PM

New Faxed Documents Received

ID: XX0000979833	Received 03/31/2022
Check #20033 Copy PDF	VIEW HERE

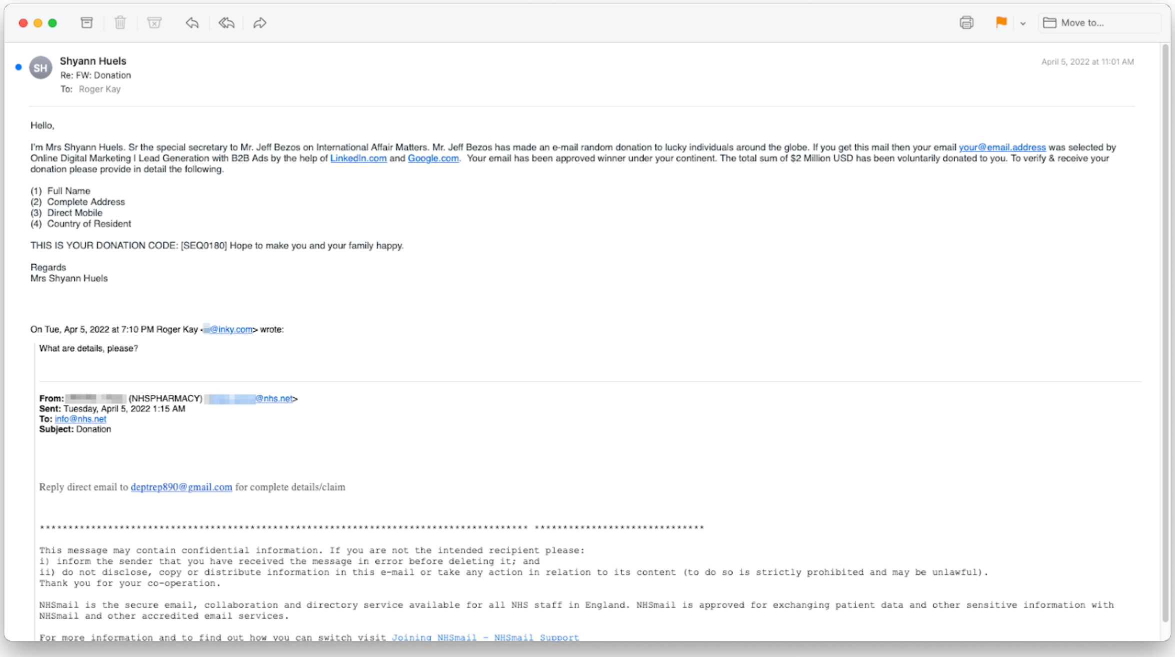
***Recipient**: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have any question.*

Secured by Proofpoint Encryption, Copyright © 2009-2021 Proofpoint, Inc. All rights reserved.

```
**************************************************************************** ****************************

This message may contain confidential information. If you are not the intended recipient please:
i) inform the sender that you have received the message in error before deleting it; and
ii) do not disclose, copy or distribute information in this e-mail or take any action in relation to its content (to do so is strictly prohibited and may be unlawful).
Thank you for your co-operation.

NHSmail is the secure email, collaboration and directory service available for all NHS staff in England. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other
accredited email services.

For more information and to find out how you can switch visit Joining NHSmail – NHSmail Support
```

Example of an Adobe impersonation

A few were advance-fee scams.



Shyann Huels
Re: FW: Donation
To: Roger Kay

April 5, 2022 at 11:01 AM

Hello,

I'm Mrs Shyann Huels. Sr the special secretary to Mr. Jeff Bezos on International Affair Matters. Mr. Jeff Bezos has made an e-mail random donation to lucky individuals around the globe. If you get this mail then your email your@email.address was selected by Online Digital Marketing I Lead Generation with B2B Ads by the help of LinkedIn.com and Google.com. Your email has been approved winner under your continent. The total sum of $2 Million USD has been voluntarily donated to you. To verify & receive your donation please provide in detail the following.

(1) Full Name
(2) Complete Address
(3) Direct Mobile
(4) Country of Resident

THIS IS YOUR DONATION CODE: [SEQ0180] Hope to make you and your family happy.

Regards
Mrs Shyann Huels

On Tue, Apr 5, 2022 at 7:10 PM Roger Kay <[redacted]@inky.com> wrote:

> What are details, please?
>
> **From:** [redacted] (NHSPHARMACY) [redacted]@nhs.net>
> **Sent:** Tuesday, April 5, 2022 1:15 AM
> **To:** info@nhs.net
> **Subject:** Donation
>
> Reply direct email to deptrep890@gmail.com for complete details/claim

```
**************************************************************************** ****************************

This message may contain confidential information. If you are not the intended recipient please:
i) inform the sender that you have received the message in error before deleting it; and
ii) do not disclose, copy or distribute information in this e-mail or take any action in relation to its content (to do so is strictly prohibited and may be unlawful).
Thank you for your co-operation.

NHSmail is the secure email, collaboration and directory service available for all NHS staff in England. NHSmail is approved for exchanging patient data and other sensitive information with
NHSmail and other accredited email services.

For more information and to find out how you can switch visit Joining NHSmail – NHSmail Support
```

Advance-fee scam example

When the author replied to a phish he received from this broad campaign, he got a reply from “Shyann Huels,” who purported to be Jeff Bezos’s secretary. Apparently, he was the lucky recipient of $2 million (for a small handling fee).

Broader Implications

As to the question of why there might still be a few phishes slipping through the net, even after the NHS took steps to mitigate this campaign, the answer might be found in the numbers. The NHS is a national organization in Great Britain, and as such, it has tremendous scope. Not only does nhs[.]net serves tens of millions of individual email users, it also provides an infrastructure for 27,000 organizations, each with its own technology staff. These organizations include hospitals, clinics, doctor's offices, public bodies, suppliers, services, social-care organizations, and many other related entities.

We found 139 compromised accounts, which may sound like a lot, but that number represents only a few ten-thousandths of one percent of the total. Given the huge number of NHS accounts, this tiny percentage could still be expected to produce a few newly compromised accounts every day.

Perhaps this is a moment to introduce the idea that phish can be like a leak in the boat. It doesn't matter that the hole is small. It will still sink the boat eventually. Even if only a few bad emails get through, with a malicious enough payload, a single successful attack can be life-altering. The NHS has been lucky so far. Credential harvesting by itself is small potatoes. But, of course, those credentials can be recycled in subsequent attacks with more dangerous results.

Recap of Techniques

- Brand impersonation — uses brand logos and trademarks to impersonate well-known brands.
- Credential harvesting — occurs when a victim thinks they are logging in to one of their resource sites but are in fact entering credentials into a dialogue box owned by the attackers.
- Hijacked accounts — are used by phishers to make their emails appear to come from legitimate senders

Best Practices: Guidance and Recommendations

Email users should always check a sender's email address carefully and scrutinize any links in an email by hovering over them. Most emails in this campaign claimed to be from Adobe or Microsoft, but nhs[.]net is not an Adobe or Microsoft domain. The links in them did not belong to these organizations, either.

Recipients should also be cautious with unfamiliar new document notifications and decline to respond to or click any links in an email from a sender who has never been in touch before.

Ready to see INKY in action? Request a free trial or a demo today.

INKY is an award-winning, cloud-based email security solution developed to proactively eliminate phishing emails and malware while simultaneously providing real-time assistance to employees handling suspicious emails so they can make safer decisions. INKY's patented technology incorporates sophisticated computer vision, machine learning models, social profiling, and stylometry algorithms to effectively sanitize emails, rewrite malicious links, detect and block security threats, mitigate sender impersonation, and more. Cost-effective and powerful, the INKY platform was developed for mobile-first IT organizations and works seamlessly on any device, operating system, and mail client. Learn more about INKY™ or request an online demonstration today.