INKY®

INKY REPORT

Hijacked University Accounts

Corporate email servers often trust email coming from universities. This circumstance has enticed evil hackers to take over badly guarded university email accounts and use them against corporate targets. Most legacy email security gateways do nothing to stop this type of attack. INKY sees the discrepancy between where the email purports to come from (e.g., Microsoft) and where it actually comes from (e.g., the University of Oxford), flagging the assault for both IT and the user.

Introduction

As they attempt to pilfer corporate digital assets, bad actors are always looking for new ways in. They tap carefully and thoroughly around the edges of corporate networks like the professionals they are, and as soon as they find a little chink in the armor, they slip in and get to work. It's a cat-and-mouse game between the black hats and the white hats.

One productive way these crooks have figured out recently to get at the corporate digital gold mine is through perfectly legitimate university accounts. The legacy secure email gateways let them in because their credentials are impeccable: their emails really do originate from a known — perhaps even august — academic institution. But given the yearly comings and goings at universities, academics' email accounts are subject to takeover. A student may never change an originally assigned password, or may share it with a friend or friends. A professor may give a student the password to an account for a particular project and never change it when the project is done. Bad actors tapping around find these carelessly handled accounts, take them over, and change the passwords themselves, locking out the original owner.

From there, it's a short hop with booby trapped email into the unsuspecting commercial organization, where a recipient who clicks on the poisoned link or clever redirect has their login credentials harvested and used against the organization for further mayhem.

This report highlights a subspecies of the account-takeover genre: university account takeover. Students and professors often have legitimate reasons to access corporate networks. Perhaps the university and the business are working together on a joint project. Perhaps a professor or student has a consulting role. The vector of attack runs through the trusted outside contact and into the soft underbelly of the now-vulnerable company.

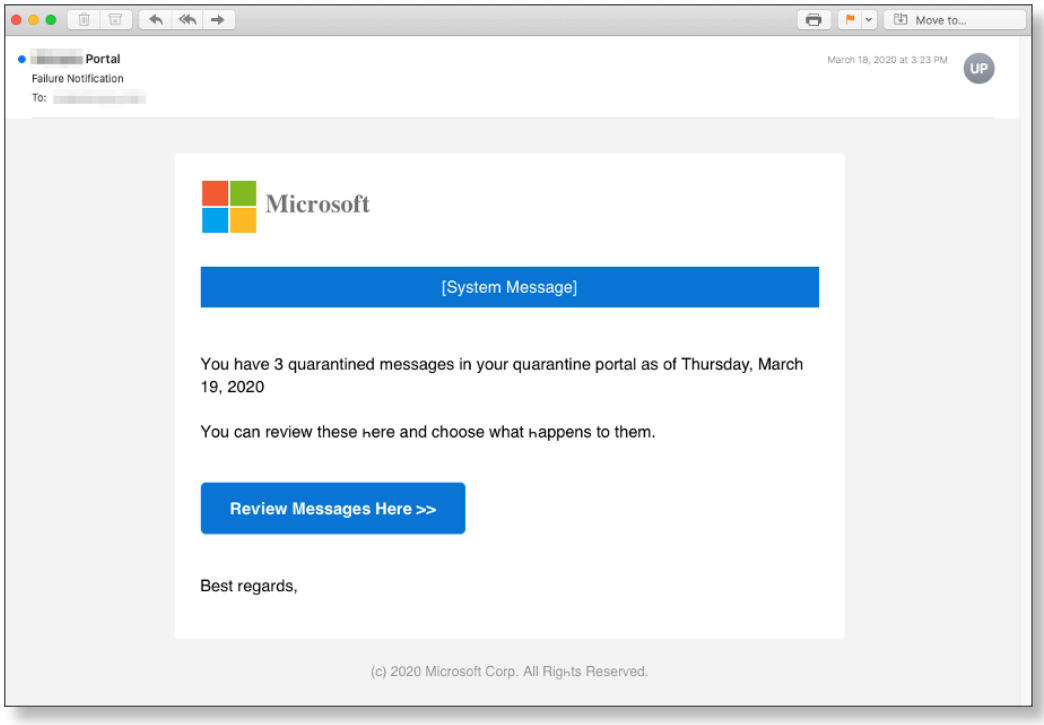
Hijacked University Accounts

This year INKY detected and stopped thousands of phishing emails that originated from multiple university accounts and servers. These attacks evaded detection by legacy secured email gateways because they came from real accounts and domains, which passed SPF and other reputation checks.

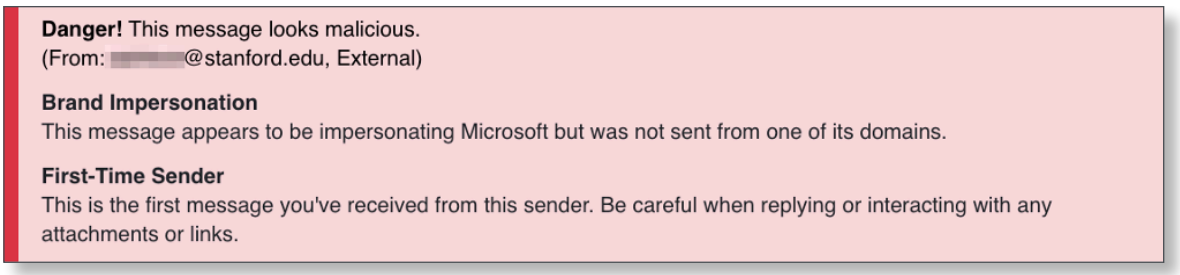
Here is a sample of the institutions, phishing campaign dates, and number of phishing emails detected:

University Name	Campaign Dates	# of phishing emails detected
Purdue University	1/3/20 - 9/17/20	2068
University of Oxford	1/8/20 - 6/26/20	714
Stanford University	1/9/20 - 4/21/20	287
Hunter College	2/5/20 - 10/12/20	709
University at Buffalo	2/24/20 - 8/26/20	207
University of New Mexico	3/2/20 - 7/17/20	357
University of Chicago	3/31/20 - 9/17/20	112
University of Texas	4/6/20 - 4/7/20	60
Worcester Polytechnic Institute	4/17/20 - 4/21/20	393
Louisiana State University	5/29/20 - 9/28/20	183
University of California, Davis	6/9/20 - 7/17/20	57
University of Utah	7/17/20 - 7/17/20	54
University of California, Los Angeles	7/29/20 - 9/16/20	211

A Closer Look at an Email Sent From a Compromised Account



In this example, a message actually sent from Stanford University purports to be a system message telling the user about the status of some quarantined messages. It offers several links to view these potentially important notes. Those links likely lead to a harvesting site or initiate a malicious code injection. Why would someone (or an auto-generate function) from Stanford be sending someone at a company a message about quarantine? It seems unlikely, but the attacker is relying on the recipient's not adding things up. They may see only the request to review and pay no attention to the strange sender. And the legacy gateway security software sees only that the domain of origination is trusted.



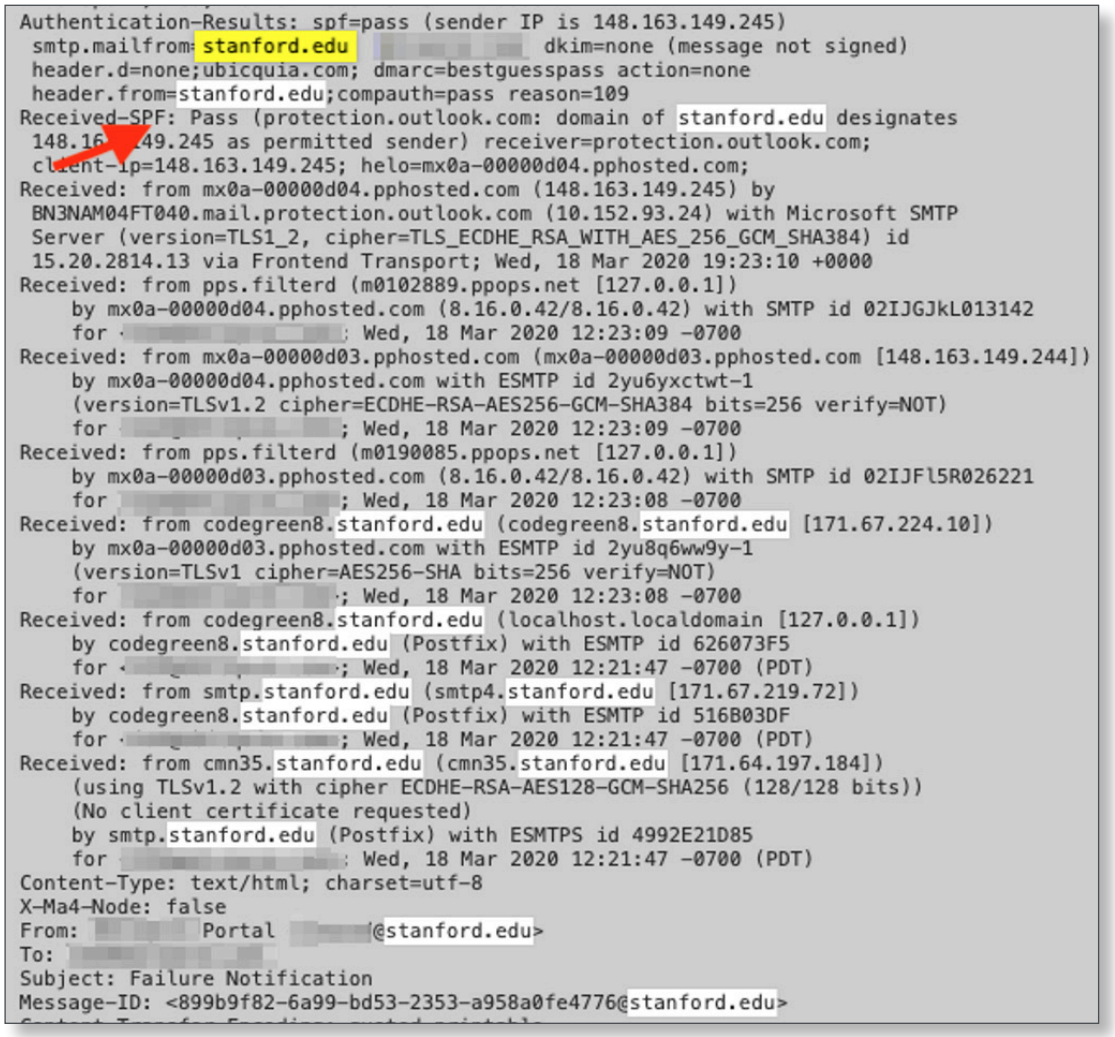
INKY throws a red flag because it sees something trying to be a Microsoft system message coming from Stanford.

INKY™

Under the Hood

Email headers (the blocks of text at the top of all emails, which are usually not shown to recipients) give INKY the information it needs to confirm that this email is the result of an account takeover.

The illustration shows a header confirming that this phishing email originated from Stanford university servers. This sender passes SPF filtering for university domains. The commercial organization's policy is to accept email from Stanford servers.



INKY™

A Simple Mail Transfer Protocol (SMTP) Conversation Doesn't Catch the Phish.

A compromised email address can be validated as legitimate via an SMTP conversation. A connection from the corporate email server to the university's SMTP server is made, requesting whether the email address in question exists. If the server replies with "250 OK," then the email address is deemed valid by the corporate server. A negative response (550-5.1.1 User Unknown) confirms that the email address does not exist.

In the SMTP session below, we see Stanford's servers telling the corporate server that everything is fine:

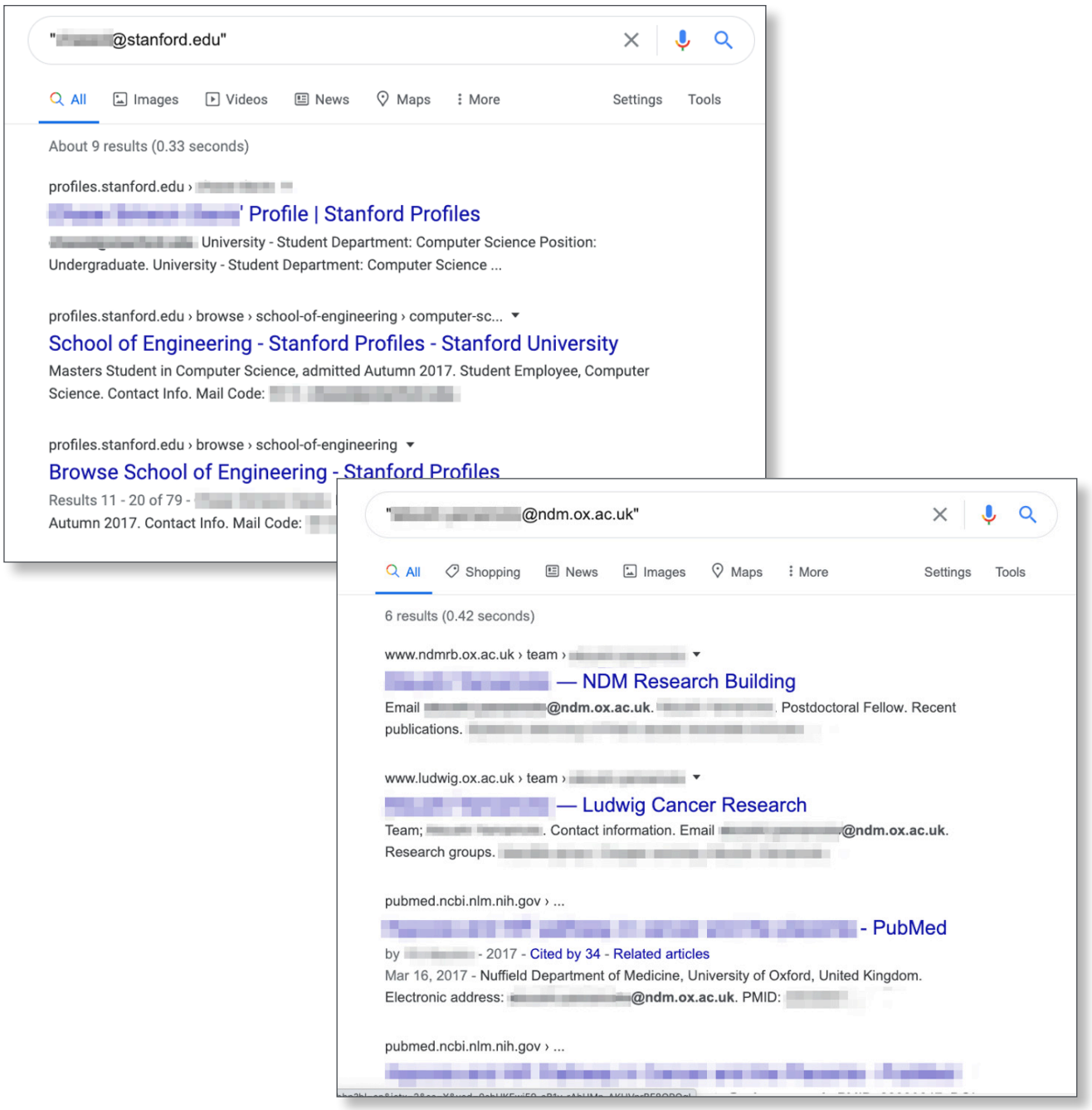
SMTP session

```
[Resolving mxb-00000d03.gslb.pphosted.com...]
[Contacting mxb-00000d03.gslb.pphosted.com [148.163.149.244]...]
[Connected]
220 mx0a-00000d03.pphosted.com ESMTP mfa-m0102880
EHLO mx1.validemail.com
250-mx0a-00000d03.pphosted.com Hello mx1.validemail.com [75.126.251.247], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250 STARTTLS
MAIL FROM:<>
250 2.1.0 Sender ok
RCPT TO:<[redacted]@stanford.edu>
250 2.1.5 Recipient ok
RSET
250 2.0.0 Reset state
QUIT
221 2.0.0 mx0a-00000d03.pphosted.com Closing connection
[Connection closed]
```

INKY™

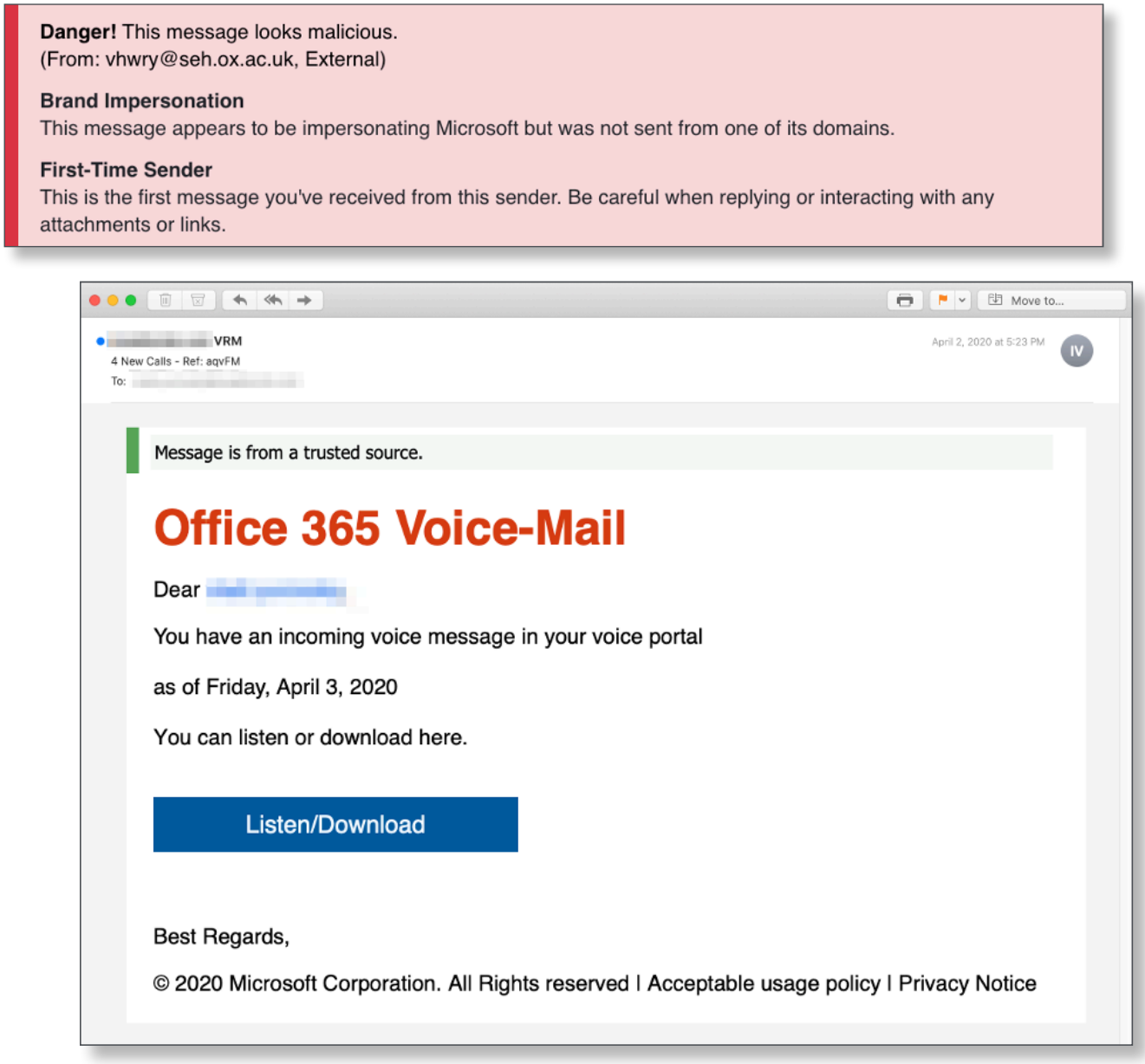
Search Engine Results

Search engine results also confirm that the address sending this phishing email corresponds to a real university profile (e.g., of a student, faulty member, staffer, or research publication).



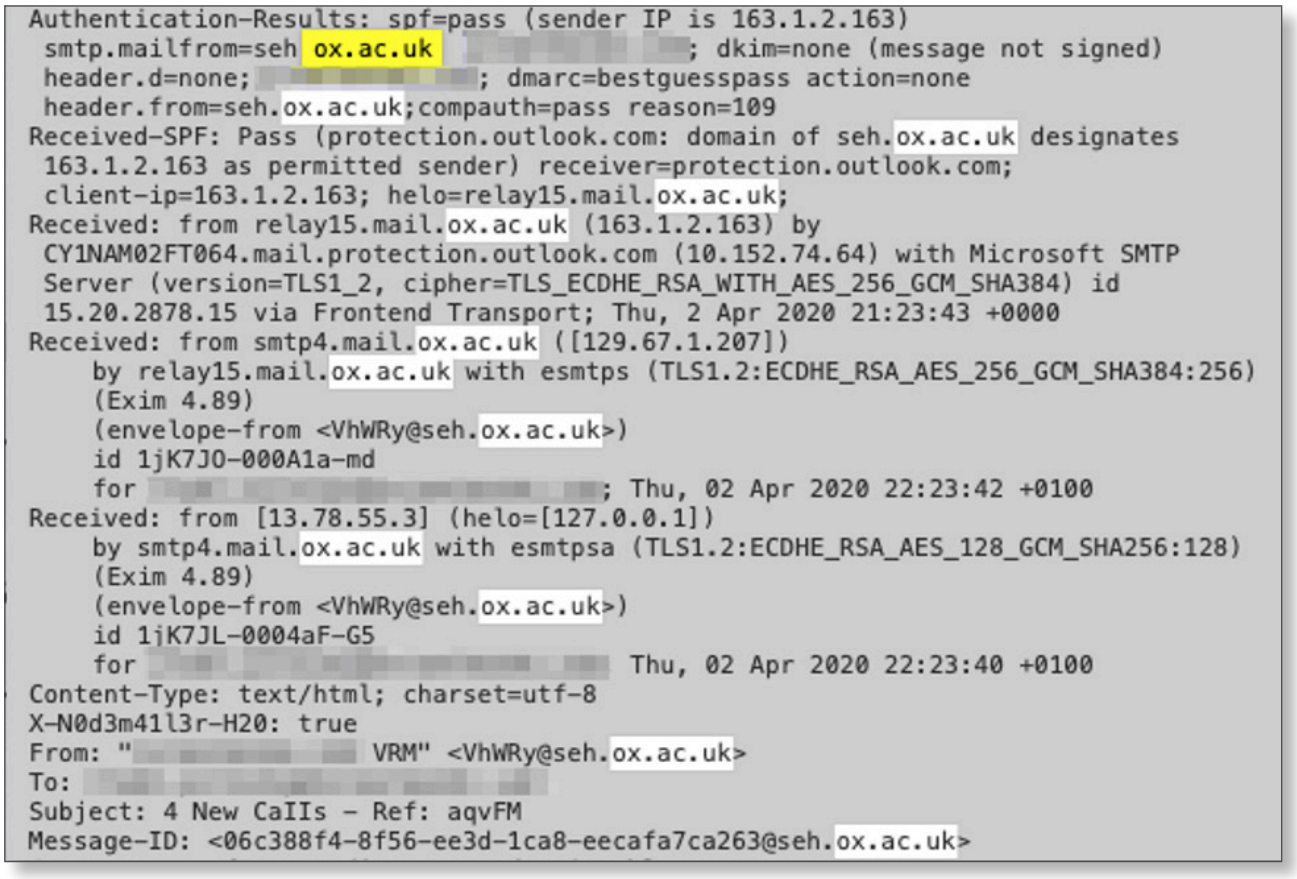
SMTP Server Abuse

In this case, a bad actor was able to abuse the University of Oxford's improperly configured SMTP server, causing it to automatically generate email addresses, from which phishing emails were then sent.



INKY caught the discrepancy.

The email headers revealed that this Microsoft impersonation originated from an IP address (13.78.55.3) in Japan and was accepted by Oxford's SMTP servers.



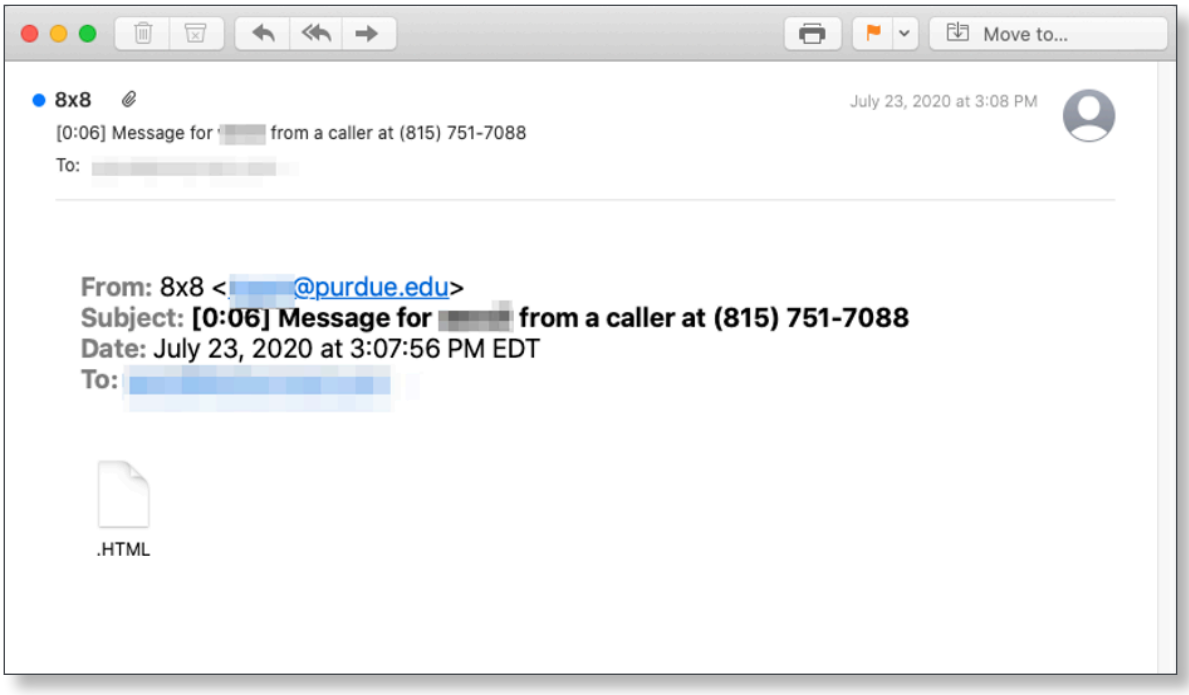
```
Authentication-Results: spf=pass (sender IP is 163.1.2.163)
 smtp.mailfrom=seh ox.ac.uk [redacted]; dkim=none (message not signed)
 header.d=none; [redacted]; dmarc=bestguesspass action=none
 header.from=seh.ox.ac.uk;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of seh.ox.ac.uk designates
 163.1.2.163 as permitted sender) receiver=protection.outlook.com;
 client-ip=163.1.2.163; helo=relay15.mail.ox.ac.uk;
Received: from relay15.mail.ox.ac.uk (163.1.2.163) by
 CY1NAM02FT064.mail.protection.outlook.com (10.152.74.64) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.2878.15 via Frontend Transport; Thu, 2 Apr 2020 21:23:43 +0000
Received: from smtp4.mail.ox.ac.uk ([129.67.1.207])
    by relay15.mail.ox.ac.uk with esmtps (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
    (Exim 4.89)
    (envelope-from <VhWRy@seh.ox.ac.uk>)
    id 1jK7JO-000A1a-md
    for [redacted]; Thu, 02 Apr 2020 22:23:42 +0100
Received: from [13.78.55.3] (helo=[127.0.0.1])
    by smtp4.mail.ox.ac.uk with esmtpsa (TLS1.2:ECDHE_RSA_AES_128_GCM_SHA256:128)
    (Exim 4.89)
    (envelope-from <VhWRy@seh.ox.ac.uk>)
    id 1jK7JL-0004aF-G5
    for [redacted] Thu, 02 Apr 2020 22:23:40 +0100
Content-Type: text/html; charset=utf-8
X-N0d3m41l3r-H20: true
From: "[redacted] VRM" <VhWRy@seh.ox.ac.uk>
To: [redacted]
Subject: 4 New CaIIs - Ref: aqvFM
Message-ID: <06c388f4-8f56-ee3d-1ca8-eecafa7ca263@seh.ox.ac.uk>
```

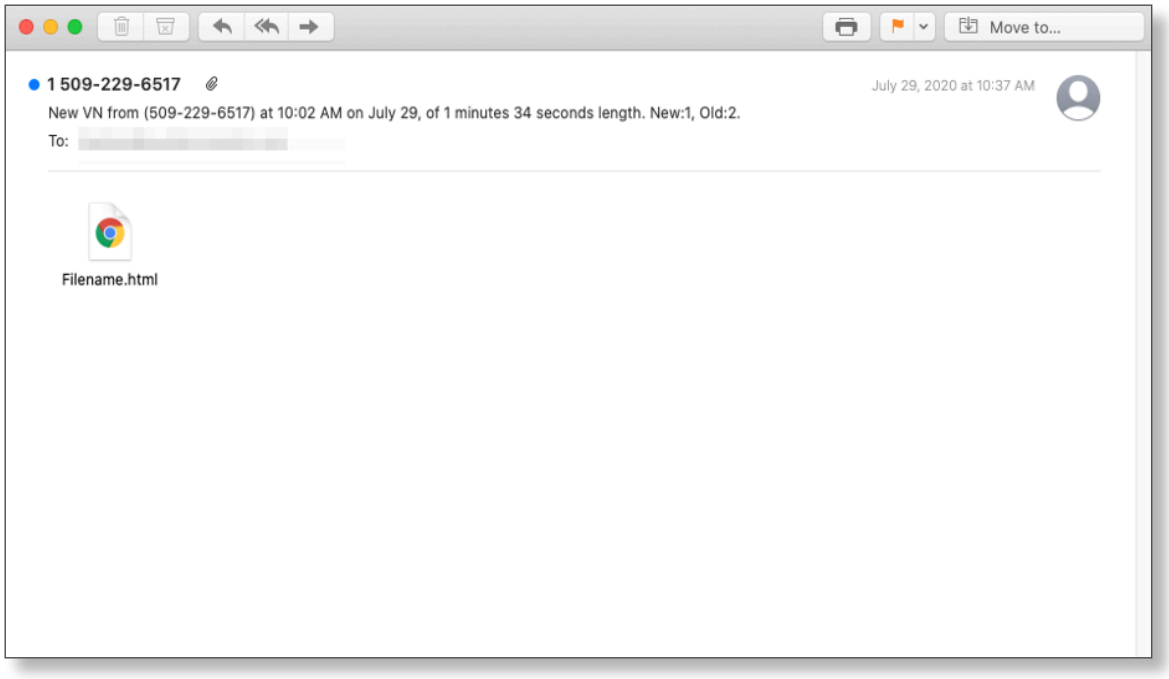
By using Oxford's servers as an open mail relay, a bad actor was able to send phishing emails that passed both SPF and DMARC for the University of Oxford!

To prevent this type of abuse, SMTP servers must be configured to not accept and forward emails from non-local IP addresses to non-local mailboxes by unauthenticated and unauthorized users.

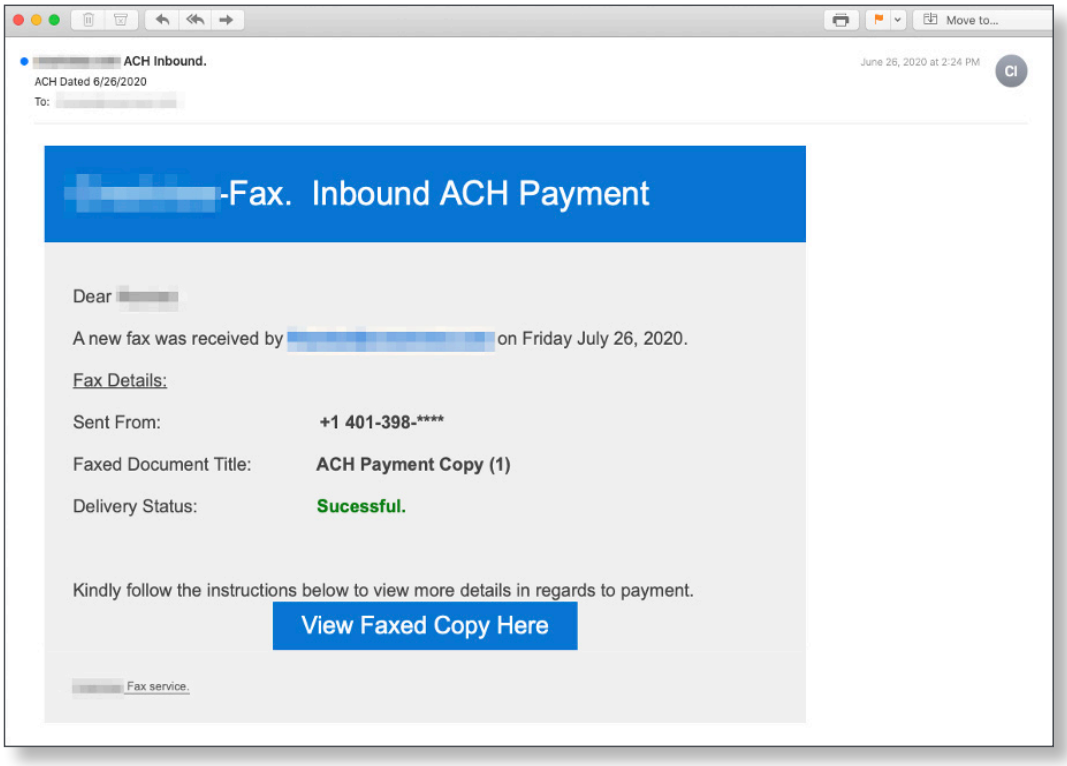
More Examples of Academic Account Takeover

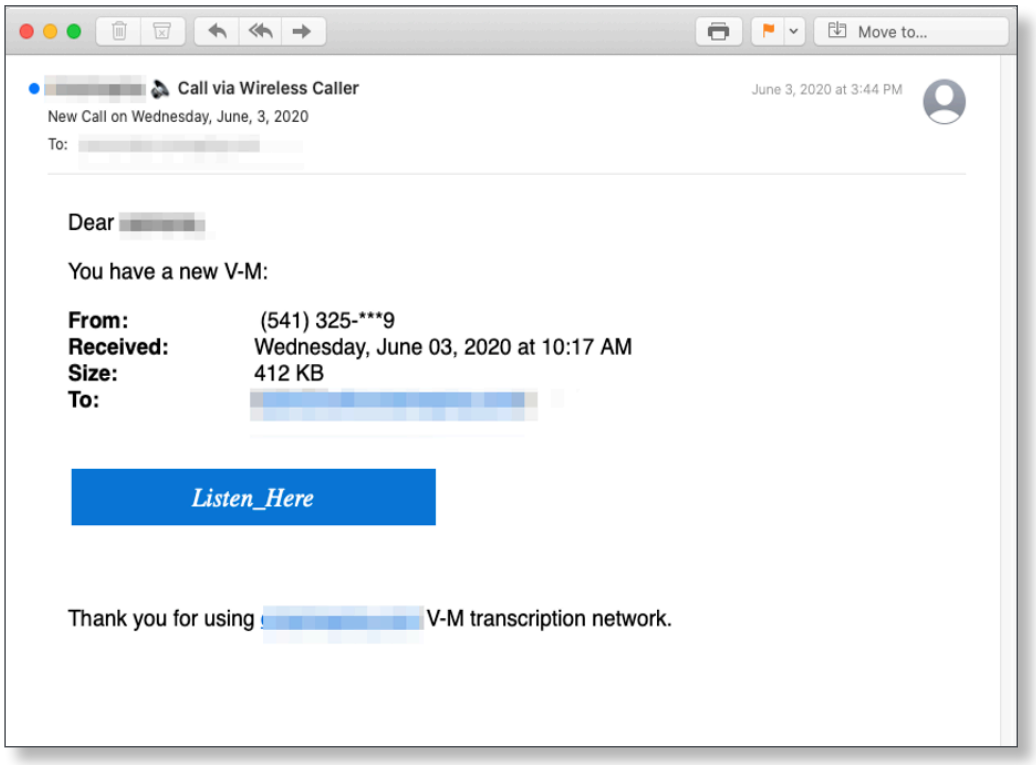
Purdue University



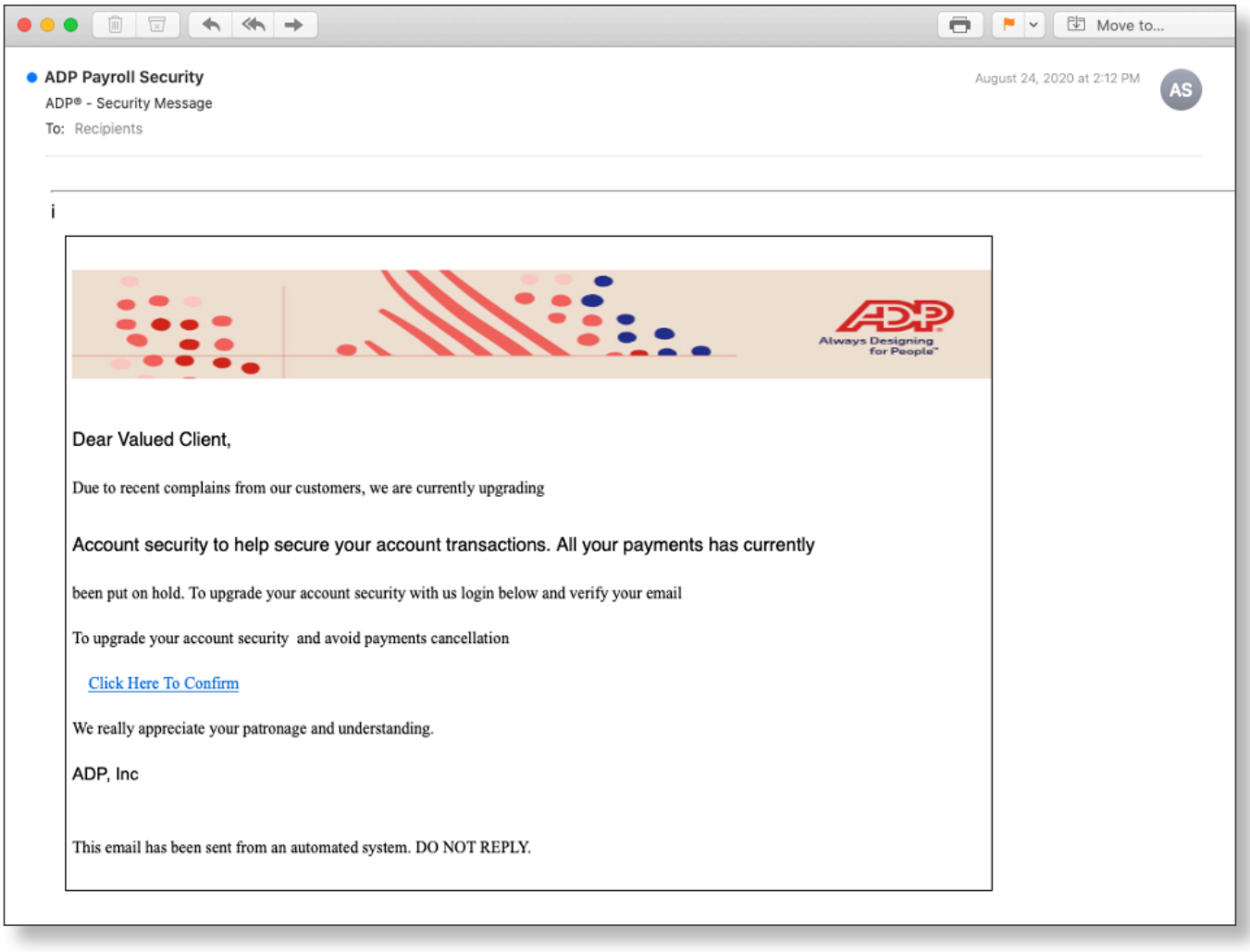


University of Oxford





Louisiana State University



Move to...

ADP Payroll Security
ADP® - Security Message
To: Recipients

August 24, 2020 at 2:12 PM

AS

i

Always Designing for People™

Dear Valued Client,

Due to recent complains from our customers, we are currently upgrading

Account security to help secure your account transactions. All your payments has currently

been put on hold. To upgrade your account security with us login below and verify your email

To upgrade your account security and avoid payments cancellation

Click Here To Confirm

We really appreciate your patronage and understanding.

ADP, Inc

This email has been sent from an automated system. DO NOT REPLY.

INKY™

Conclusion

The black hats are clever and always shape shifting to regain access to corporate email servers when they are discovered and locked out. For now, the university account takeover is working much of the time. Inky, among all white hats, is the most advanced in detecting and defeating this attack vector.

To see INKY in action request a live demo, or sign up for a free trial today.

We're passionate about email.

Want to talk about an issue you're facing in email security at your organization?

Request a demo today

www.inky.com