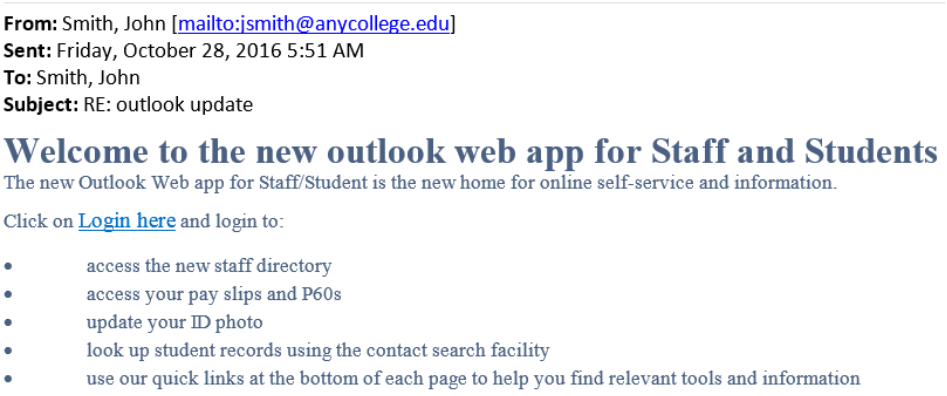
Malicious Phishing Emails

Unsolicited junk mail accounts for more than 85% of the world's e-mail traffic. Many of these emails are malicious phishing messages aimed at fooling recipients into clicking links or providing information such as email passwords. Here's an example:



From: Smith, John [mailto:jsmith@anycollege.edu]
Sent: Friday, October 28, 2016 5:51 AM
To: Smith, John
Subject: RE: outlook update

Welcome to the new outlook web app for Staff and Students

The new Outlook Web app for Staff/Student is the new home for online self-service and information.

Click on Login here and login to:

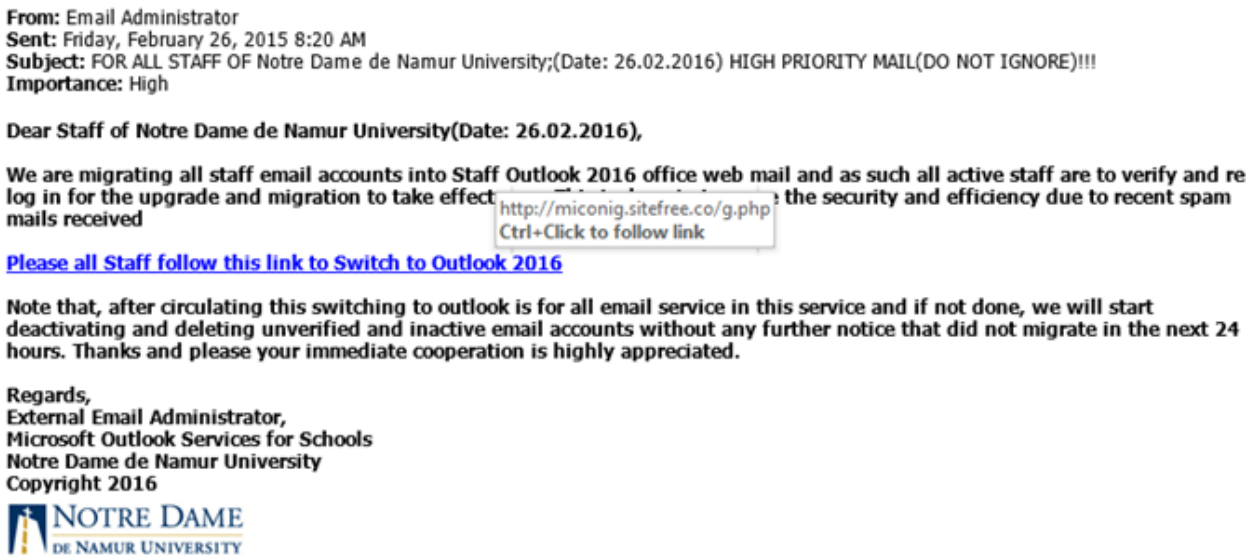
- access the new staff directory
- access your pay slips and P60s
- update your ID photo
- look up student records using the contact search facility
- use our quick links at the bottom of each page to help you find relevant tools and information

The first indicator that this is not sent by NDNU OIT is that the From address is not an NDNU email address.

What about the "Login here" link in the body of the message? You can hover your cursor over a link without actually clicking on the link to see what URL the link points to:

A callout box reveals that the URL is not an NDNU page.

In the above case, it was easy to determine that this was a fraudulent email. But not all are as obvious; sometimes the messages will have customized content that may even include branded logos:



From: Email Administrator
Sent: Friday, February 26, 2015 8:20 AM
Subject: FOR ALL STAFF OF Notre Dame de Namur University;(Date: 26.02.2016) HIGH PRIORITY MAIL(DO NOT IGNORE)!!!
Importance: High

Dear Staff of Notre Dame de Namur University(Date: 26.02.2016),

We are migrating all staff email accounts into Staff Outlook 2016 office web mail and as such all active staff are to verify and re log in for the upgrade and migration to take effect the security and efficiency due to recent spam mails received

http://miconig.sitefree.co/g.php
Ctrl+Click to follow link

Please all Staff follow this link to Switch to Outlook 2016

Note that, after circulating this switching to outlook is for all email service in this service and if not done, we will start deactivating and deleting unverified and inactive email accounts without any further notice that did not migrate in the next 24 hours. Thanks and please your immediate cooperation is highly appreciated.

Regards,
External Email Administrator,
Microsoft Outlook Services for Schools
Notre Dame de Namur University
Copyright 2016

NOTRE DAME
DE NAMUR UNIVERSITY

This one where it's helpful to hover the cursor over the link as shown; it's not an NDNU web page.

Spoofed Email Addresses

Not all malicious emails are to spot, because in many cases, the From email address is *spoofed* to appear to have been sent from someone else. Spoofing is quite common; Google "How Spammers Spoof Your Email Address" to read up on it. Here's what can happen:

- You receive a message that has your email address in the From field, but you never sent the email.
- A colleague forwards you a suspicious email he/she received that has you as the sender, but you never sent it.
- You receive Undeliverable messages for spam emails that you never sent.

If you receive "undeliverable" messages for emails you didn't send, log-in to your email account on the mymail.ndnu site, then:

1) Look in your Sent Items folder, and see if there are sent messages you didn't send. If there are none,
2) Check to see if there are any Rules you didn't set-up in Outlook. You can check that in your Outlook Web App: click Options, then Inbox Rule. There are cases where the entity that hijacks the account creates a rule to delete incoming or outgoing messages so that the account owner isn't aware of anything wrong.

If there are no Sent Items messages, and no Rule that you didn't set up, it's unlikely that your account has been compromised. Check with OIT Help Desk if you're not sure.

What Can Happen If You're Fooled

We've all received fraudulent messages that have official-sounding Subject lines, such as "Web-Admin," "System Administrator," or "Help Desk." They typically make claims such as, "Mailbox Quota has been exceeded," "Mailbox is over its size limit," "Confirm your email address," etc.

If you fall for this ruse, and click the link, a site will open where you'll be asked to type in your username and password. If you do that, major problems will ensue, for you, and NDNU. Knowing your password, the phisher will be able to hijack your account, then use it to send large volumes of spam messages. Internet monitoring entities and ISP's will see this volume of spam messages coming from the ndnu domain, and may systematically begin blocking any and all emails from our domain. One person unwittingly providing his/her password in response to a phishing email can lead to entire domains (gmail, hotmail, yahoo, etc.) rejecting any emails coming from any NDNU email address. When OIT detects that an NDNU account has been compromised, we immediately disable the account, and purge any emails that are queued to be sent. We keep the account disabled for at least one week.

Please be wary of these threats, and carefully examine emails that ask you to submit personal info such as passwords, credit card numbers, etc.. Note who is the sender; even if looks like it's from someone you know, it may be that the From address is "spoofed." Look at the URL in the body of the message; even if it looks official, hover your cursor above it so that you can see the real URL. It won't be from NDNU.

Note that even just clicking a link and opening a web page without ever providing your username/ password info can result in an attack on your computer known as a drive-by install, an exploit that downloads and runs malware silently, without the warnings or dialogs one would expect.

The best defense against these threats is to have an informed community fully aware of the prevalence of these social-engineering (designed to motivate you through risk or reward to take action) malicious emails, so that we all learn to recognize, then delete them.

NDNU Mailfilter

NDNU's Sophos email intrusion prevention mailfilter receives anti-spam/anti-malware/anti-virus updates regularly, and blocks more messages than it passes. Most messages sent to our mail system are discarded before they are delivered because they're recognized as spam or malicious.

But when an email is coming from a legitimate email address that's just been hijacked, it passes. Usually the sender's email provider shuts down the account quickly (after recognizing the high volume of messages being sent out of their system, or having received an Internet Abuse notification from their ISP). But by then, the message has gone out to potentially thousands of recipients, and if just one person is fooled into submitting personal account info, the cycle of hijacked accounts and spam attacks continues.

When OIT becomes aware of a malicious email that is sent to many NDNU accounts, we are able to run a process that extracts all instances of the message from our mailboxes. However, sometimes such message are only sent to a few users, so we are not able to remove all malicious messages from legitimate senders.

Our email protection system (mailfilter) quarantines messages recognized as potential spam. Each Wednesday, you'll receive an email like the one below :

From: Administrator
Sent: Wednesday, November 30, 2016 6:01 AM
To: John Doe
Subject: Quarantined spam and bulk messages since Nov 23 06:01

Notre Dame de Namur University's email protection service has quarantined messages as potential spam. To view these messages, please login to your NDNU Message Center:

1. Browse to NDNU Mail Filter

Note: This is a safe link. Please accept the certificate to continue to the mail filter's web page.

Internet Explorer - Click the Continue to this website...
2. In the Login field, type your **Email Username** (e.g., jsmith) without adding @ndnu.edu
3. In the Password field, type your **Email Password**
4. Click Login, or press Enter

Do not reply to this message; if you do so all your suspected spam messages will be forwarded to you account. (No virus-infected messages will be sent; they have been discarded.)

The most efficient way to review your messages is to log-in to mailfilter.ndnu.edu as detailed above.

However, if you're on-campus using Outlook, you do have the option of clicking a link in the ID field in the blue table below. When you do that, a message window will open that once you send will tell the system to go ahead and send you that quarantined message. The only case in which you might want to do this would be if you recognize the email address in the table as someone from who you want to receive a message.

Otherwise, use the NDNU Mail Filter site to manage your suspected spam emails, and again, do not reply to this message unless you want all your potential spam messages sent to your Inbox.

ID	Type	Time	From	Subject
[=0]	Spam Medium	07:02:41	ejohnson@lumpyhead.com	
[=1]	Spam Medium	08:03:25	wirelesssecuritycameras@everydayshared.stream	Search For Wireless Surveillance Cameras

This is a legitimate email, and the only one you'll receive from NDNU OIT that has clickable links.