Phishing

We have become all too familiar with phishing emails but if that's the case, why do we as a community still fall victim? In this newsletter our goal is to provide you with some basic information about what phishing is, a few techniques to help you identify phishing emails and then instructions on who to contact if you have any questions.

What do phishing emails do?

Phishing emails can be pretty nasty attacks yet some users just don't get it. Let's try and put this into perspective with a simple scenario.

> A user gets an email from another employee at Lynn University and it contains a hyperlink in the email that interests them. They don't really know the person but they decide to click on the link anyway and it takes them to a website that asks the user to login to view the content. The user enters in their Lynn username and password and viola, they can access the content. It ends up being nothing that they are interested in and they close the web page and forget about it.

What really happened? Well, it all depends on what that phishing campaign was trying to accomplish? Let me give you some examples of the potential risks that stem from clicking on the link in the email. This is only for illustration purposes and hopes to inform you on what COULD be done.

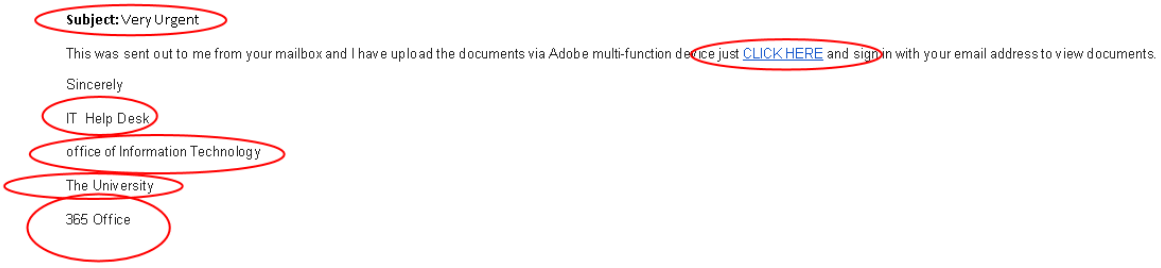
1. When the user clicked on the email, an embedded script ran silently in the background. The script did the following
    a. It pulled a log of all users who had previously logged into that computer along with their passwords that were still in memory
    b. It installed a keylogger that is now collecting all the keystrokes that the users types with their keyboard. Including any other usernames and passwords for any other sites they visit.
        i. What if you accessed your bank recently? Uh oh! Does this mean that they can log into your bank account? Yep!
        ii. Do you now have to worry about Identity Theft? Possibly?
    c. It copied all your documents on your desktop or H drive and zipped them in a hidden file on your computer to be used at a later time.
    d. It also installed a command and control backdoor agent that sends the information that it has collected to a server out on the internet. But wait, that server changes based on a sophisticated algorithm that generates a different server on the hour. All silently in the background.
2. When the user typed in their Lynn Username and password the attacker now has the users email address, domain name, username, and password.
    a. The attacker now has access to:
        i. all of your emails and it can send out emails to others in your contact list to spread the attack so that others can be affected.

ii. all of your documents that you have in:
    1. Office 365
    2. your local computer
    3. your Departmental Drives etc.

There we have it. A simple scenario to describe how a phishing attack could affect not only university data and information but also, your own personal information and data. We can't stress enough the importance of being more aware of what websites you are accessing and what hyperlinks you are clicking on. The repercussions can be pretty significant.

So what does a phishing email look like?

Here are some examples of the recent phishing emails that some members of the community have fallen victim to. You may have received a copy of them.



Subject: Very Urgent

This was sent out to me from your mailbox and I have upload the documents via Adobe multi-function device just CLICK HERE and sign in with your email address to view documents.

Sincerely

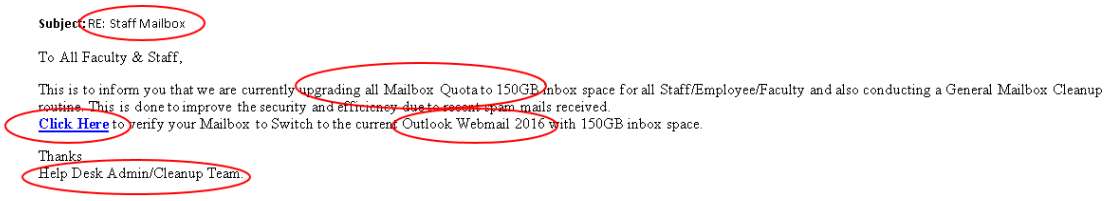
IT Help Desk

office of Information Technology

The University

365 Office

****



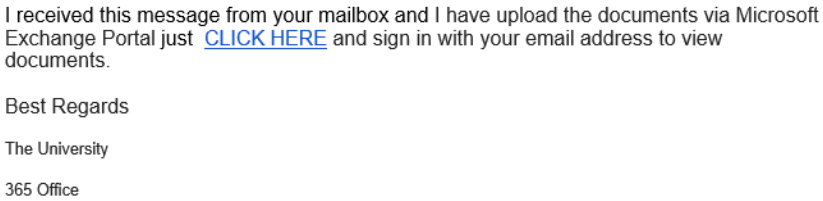
Subject: RE: Staff Mailbox

To All Faculty & Staff,

This is to inform you that we are currently upgrading all Mailbox Quota to 150GB inbox space for all Staff/Employee/Faculty and also conducting a General Mailbox Cleanup routine. This is done to improve the security and efficiency due to recent spam mails received.
Click Here to verify your Mailbox to Switch to the current Outlook Webmail 2016 with 150GB inbox space.

Thanks
Help Desk Admin/Cleanup Team.

****



I received this message from your mailbox and I have upload the documents via Microsoft Exchange Portal just CLICK HERE and sign in with your email address to view documents.

Best Regards

The University

365 Office

****

Subject: RE: Your password
Importance: High

Dear User,
Your password will expire in 24 hours Click on: **Staff and Faculty** to validate your e-mail

****

All Staffs and Students are expected to migrate to the New 2017 Microsoft Outlook Web portal to access the below, click here to migrate:

- **Access the new staff directory**
- **Access your pay slips and P60s**
- **Update your ID photo**
- **E-mail and Calendar Flexibility**
- **Connect mobile number to e-mail for voicemail**

Important notice: All staffs and students are expected to migrate within 24 hours to avoid delay on mail delivery.

On behalf of IT Support. This is a group email account and its been monitored 24/7, therefore, please do not ignore this notification, because its very compulsory.

Sincerely.
Admin Team.

****

LYNN UNIVERSITY

You have received an important document 'Outstanding Payment'. Click here to view the secured document.

Lynn University
3601 N. Military Trail
Boca Raton, FL 33431

Key things to look out for:

- **Spelling and bad grammar.** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam. For more information, see Email and web scams: How to help protect yourself.
- **Beware of links in email.** If you see a link in a suspicious email message, do not click on it. Rest your mouse (but do not click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.

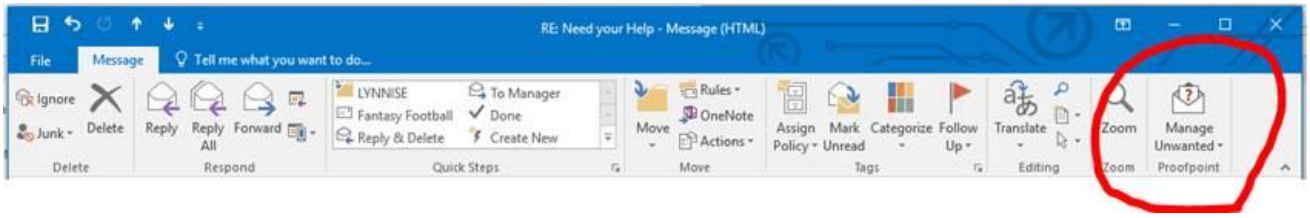
Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- **Do you even know the person sending you the email?** Does it make sense that the person sending you an email to a finance document but they work in a department that has no affiliation with finance?
- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised. For more information, see Watch out for fake alerts.
- **Spoofing popular websites or companies.** Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. For more information, see Avoid scams that use the Microsoft name fraudulently.

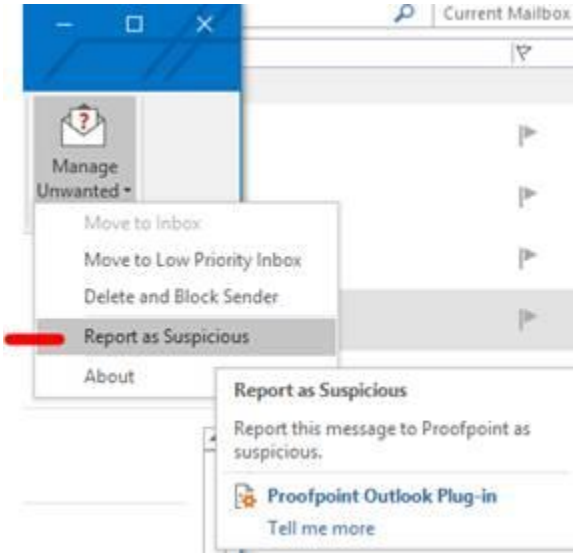
  Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered. For more information, see Protect yourself from cybersquatting and fake web addresses.

How to Report Phishing emails using the Proofpoint Unwanted Email Plugin in Outlook:

1. Identify email in question.
2. Select and Highlight the email and go to the Message Tab. On the far right you will see a Proofpoint Group on the ribbon.



3. Click on Manage Unwanted and Select Report as Suspicious.



If the Proofpoint Unwanted Email Plug is not installed on your computer, please contact Support Services at 561-237-7979.