HOW TO RECOGNIZE & DISPOSE OF PHISHING EMAILS

It is estimated that cyber criminals will net 80,000 individual logins & passwords every 24 hours.

It only takes 1 stolen password for a breach to occur!

WHAT IS PHISHING? WHY ATTACK SIU?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Medical records can be more valuable than credit cards on the dark web

SIU is required by law to protect information regarding our employees, students, and patients.

End users are SIU's first line of defense against security threats.

TIPS FOR RECOGNIZING A PHISHING EMAIL

- Look for email addresses that are close but not exact. Example, email address may end in ".co" rather than the expected ".com".
- Verify all links included in the body of the email. Users are able to hover over a link to see what URL it will actually take them to if they were to click on it.
- Look for logos that feel a bit off, misspellings, or grammatical errors in emails that appear to be from reputable institutions such as banks or government offices.
- Be suspicious of emails that request passwords, personal information, or money.
- Don't download attachments unless you're positive you know the sender.

You can always call the sender to verify the email is legitimate

Attackers will try to create a sense of false urgency or make an emotional plea using fear, obedience, greed or even helpfulness

WHAT IS MALWARE?

SIU blocks potential malware as much as possible

Do not download attachments from unknown sources

Malware is software that is designed to damage and destroy computers and computer systems.

Viruses-Attached to a document or file.

Worms-Infects a device via a download or connection.

Adware-Collects data on your computer usage and provides advertisements. Not always dangerous, but can cause issues on your system or cause slowness.

Macros-Hide in Microsoft Office files and are delivered as email attachments or inside ZIP files

Spyware-Runs secretly on a computer and reports back to the remote user.

Trojan Viruses-disguised as helpful software programs.

Ransomware-gains access to sensitive information within a system, encrypts that information so the user cannot access it, and then demands financial payout for the data to be released.

It is very important to Verify legitimacy before enabling macros or even downloading unrequested items via attachment or links

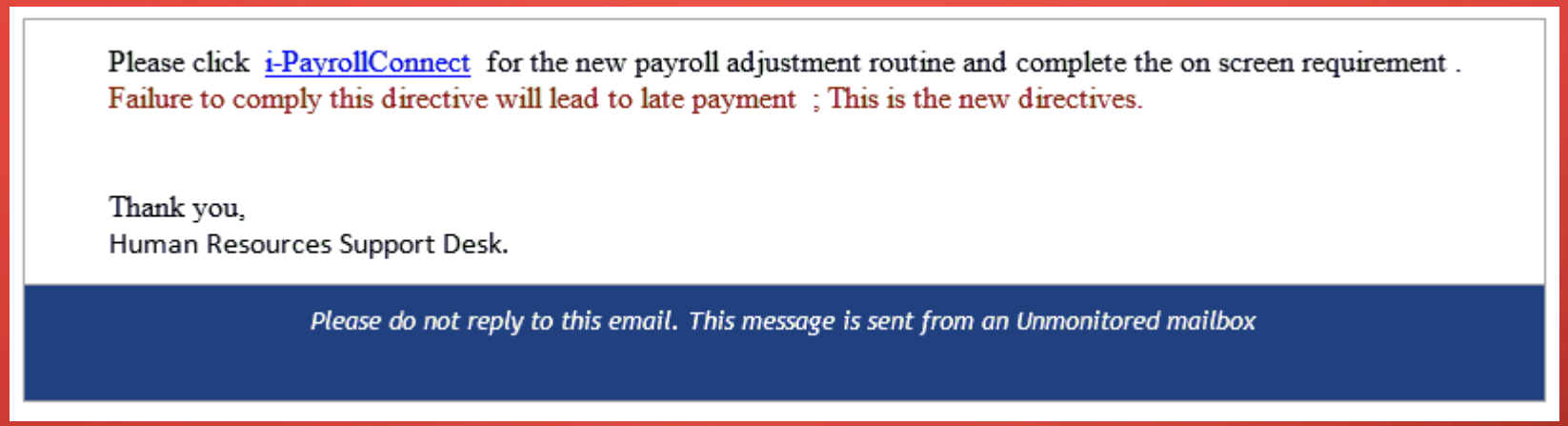
HOW TO DISPOSE OF PHISHING SCAMS

1. Forward email to abuse@siumed.edu
2. Delete email from your sent mailbox
3. Delete email from your trash mailbox

Defending against these attacks requires a coordinated and layered approach to security by both SIU IT and the End User.

When in doubt, forward the email!

ACTUAL PHISHING EMAIL ATTEMPTS AGAINST SIU *FALSE URGENCY*

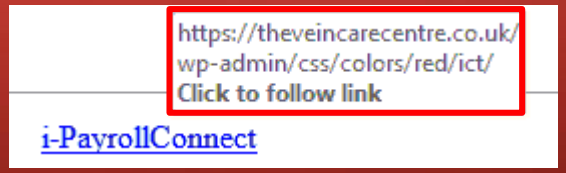

Please click i-PayrollConnect for the new payroll adjustment routine and complete the on screen requirement .
Failure to comply this directive will lead to late payment ; This is the new directives.

Thank you,
Human Resources Support Desk.

Please do not reply to this email. This message is sent from an Unmonitored mailbox

In the above example a sense of urgency is used!

Below example is what a user would have seen if they hovered over the link in the email.



ACTUAL PHISHING EMAIL ATTEMPTS AGAINST SIU
EMOTIONAL PLEA USING FEAR

Techsupport <admin@forumthroughorbit.com>
WARNING: Mailbox Quota Exceeded

Pay attention to the sender's email address

Hi

Your mailbox quota usage has exceeded 85%. You may not be able to receive all new emails

490MB **498**MB

Increase mailbox size here.

Please be advised that messages will be automatically deleted from server if not retrieved after 2 "Days".

Thanks
Mail Server Team

Sender is using a sense of fear of not receiving new emails.

Hovering over the link would have shown where the user would be taken by clicking it

http://forumthroughorbit.com?rid=nqwknrj
Click to follow link

Increase mailbox size here.

ACTUAL PHISHING EMAIL ATTEMPTS AGAINST SIU
EMOTIONAL PLEA OF OBEDIENCE

Dear customer,

For easy contact from our representatives and in other to keep up with notifications concerning your ADP account activities, we want you to review the contact information we have for you.

This mini survey serves as a means of enhancing and updating contact information for security reliability and excellent customer service.

Your Email tracking number: **7HDN49JSLABUL63N4**

Review your contact information below:

https://workforcenow.adp.com/security_profile20%Emailtracking_ID=7HDN49JSLABUL63N4

Due to email tracking, you will keep receiving this notification until you have taken the steps required.

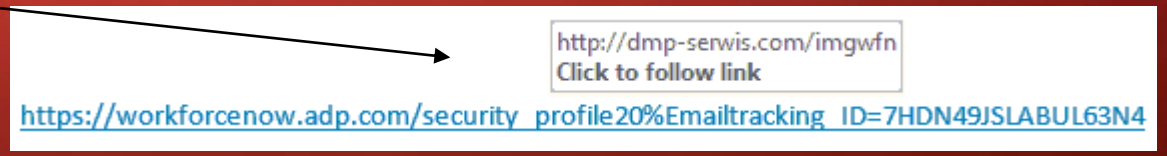
We apologize for any inconveniences this may have caused.

Thank you,

ADP Service

Sense of Obedience

Hovering over the link would have shown where the user would be taken by clicking it



ACTUAL PHISHING EMAIL ATTEMPTS AGAINST SIU
EMOTIONAL PLEA OF HELPFULNESS

From: J. Kevin Dorsey
Sent: Tuesday, October 02, 2018 10:29 AM
To: [redacted]@siumed.edu>
Subject: Re: Follow up

1. Original email to user:

Subject: Follow up

Are you available?

2. User Response:

Subject: RE: Follow up

Yes. Pretty flexible today.

3. Response back to user using the sense of helpfulness

Subject: Re: Follow up

I want you to help me get an iTunes gifts card from the store, i should have call you, but i can't call with the phone so that is why I'm contacting you through here.

i need you to help me get an iTunes gifts card from the store,i will reimburse you the money when you come back.

I need to send it to someone and it is very important okay.

It's one of my best friend daughter birthday today so i want to give her the iTunes Gift Card as a birthday present.

The amount i want is $100 each in three (3) pieces so that will make it a total of $300 I'll be reimbursing back to you. i need physical cards which you are going to get from the store. When you get them,just scratch it and take a picture of them and send it to me here okay
Get the iTunes Gift Card for me now

Notice the from user. However, the end user can hover on the senders name and see the full email address.

From: J. Kevin Dorsey [mailto:J.kevindorsey@outlook.com]

NOT ALL EMAILS ARE BAD
LEGITIMATE SIU EMAIL NOTIFICATION

You have received this email notification because your Information Technology/SIUMED password is about to expire.

User ID:
Password Expiration Date: Thursday, November 14th 2019

To avoid disruption of services, please change your password as soon as possible. You can change your password at:

https://weblogin.siumed.edu/changepw/Password/Change

This password is used to access the following resources:

- SIUMED Computer Logon
- Citrix - apps.siumed.edu
- Email
- Springfield Wireless Access
- Password Protected web pages on
  - https://www.siumed.edu/
  - https://intranet.siumed.edu/

If you need further assistance, please contact techsupport@siumed.edu or call 217-545-4357.

Copies of SIU School of Medicine Computing Policies can be found at:
http://www.siumed.edu/ir/policy/

If an account password remains expired for greater than 120 days the account will be deleted automatically. Alumni and retired faculty accounts will NOT be reactivated after they are deleted.

Additional information is available on the IR intranet site:
http://intranet.siumed.edu/ir/

Thank You
Information Technology

END USER RESPONSIBILITIES

Users are responsible for their accounts & passwords

DO NOT:

Share your password with others including IT staff

Write down or publicly post passwords

Login to computers/applications on behalf of other users

Allow users to use your account to act on your behalf