



THE UNIVERSITY OF  
**CHICAGO**

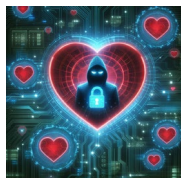
Biological Sciences Division  
**Information Security Office**

February 2024 ♡

## Cybersecurity Awareness

### Newsletter

Protecting yourself and information from cybersecurity threats.



This past month our institution experienced a more than normal amount of phishing e-mails from a threat actor outside of the US. Many individuals clicked on links and fell prey to the deceptive e-mails. Some folks purposely clicked on links knowing they were phishing e-mails just to see what would happen and, in the process, used up investigative resources. We won't get into that but it is concerning. It is important to ensure that everyone is Cyber Aware of the threats that can occur when clicking on links from unknown sources regardless of what tools are on our systems to protect us from harm. No tool is 100% effective at catching and protecting from cyber threats. So this month it is only fitting that we go over phishing detection and prevention especially since this is also the month where we see a rise in romance phishing scams.



### What is Phishing?

Phishing is a type of cyber-attack where an unsuspecting individual receives an e-mail and is tricked into providing information such as a username, a password, credit card information, social security number, or other sensitive information. In the case of basic phishing this is usually started with a convincing e-mail that can request information and commands such as click here, call here, or install an app. The e-mail message is usually urgent in manner, but the sky is the limit on the questions and vocabulary they can use to grasp our attention.

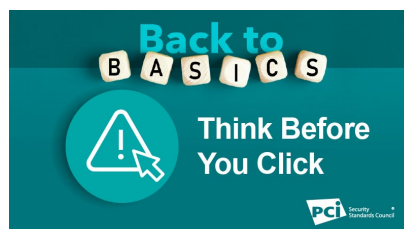


### Stay vigilant, avoid a phishing incident!

Phishing e-mail will usually look convincing or may be related to a web search or web site related content. Common themes and tag lines: “Sale going on now for a limited time.” “Lock in your rate now!” “Shipping was delayed for your Amazon package “ “An item you preordered will be cancelled unless you approve of the delay click here verify.” They can be real e-mails from the vendor and they can also be phishing attempts.



Cybercriminals always take advantage of distracted behavior such as the emotional state of urgency. Be aware that when purchasing popular products, such as item(s) that are the latest craze and in high demand that you will likely see messages targeted by scammers who are actively reviewing online vendor sales activity. Consider that popular sites like Amazon are often e-mail spoofed, cybercriminals are most likely to catch someone off guard by sending mass e-mails that look like they came from Amazon.



## Think before you click, avoid the trick!

Here are ten of the most common themes designed to prey on human emotions. These tricks are used to entice us to click a link or open an attachment.

**Urgency:** "Your account has been compromised! Act now to secure it."

**Fear:** "Immediate action required to avoid legal consequences."

**Curiosity:** "You won a prize! Click here to claim it."

**Authority:** "Verify your account to avoid suspension."

**Greed:** "Investment opportunity of a lifetime! Guaranteed returns!"

**Charity:** "Support this cause by donating now."

**Personal connection:** "A friend has tagged you in a photo. Click to view."

**Technical support:** "Your device is infected! Call this number for assistance."

**Financial incentives:** "You've earned a raise, click here to verify your new earnings."

**Job opportunities:** "Work from home and make thousands of dollars a month."

Here are ten most common romance phishing tactics:

**Fake romantic gestures:** "Send a virtual Valentine's Day card to your loved one! Click here to customize."

**Gift offers:** "Get exclusive Valentine's Day deals on jewelry, chocolates, and flowers! Claim your discount now."

**Date invitations:** "Meet your perfect match! Join our dating site and find love this Valentine's Day."

**Love letters:** "Receive a secret admirer's message! Open now to read."

**Relationship advice:** "Improve your love life with our expert tips and tricks. Subscribe today!"

**Romantic getaways:** "Win a dream vacation for two! Enter our Valentine's Day giveaway."

**E-card scams:** "Your friend sent you a Valentine's Day e-card. Click here to view."

**Romance scams:** "Find your soulmate online! Sign up for our dating service now."

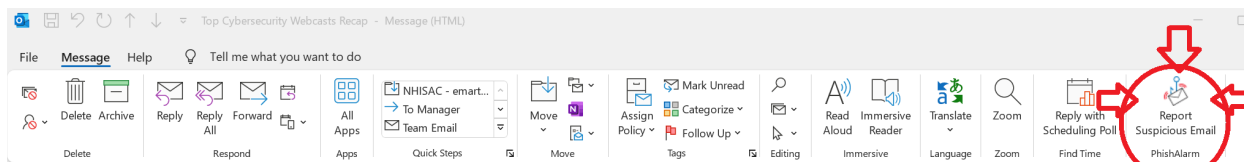
**Gift card scams:** "Get a free gift card for Valentine's Day. Claim yours today!"

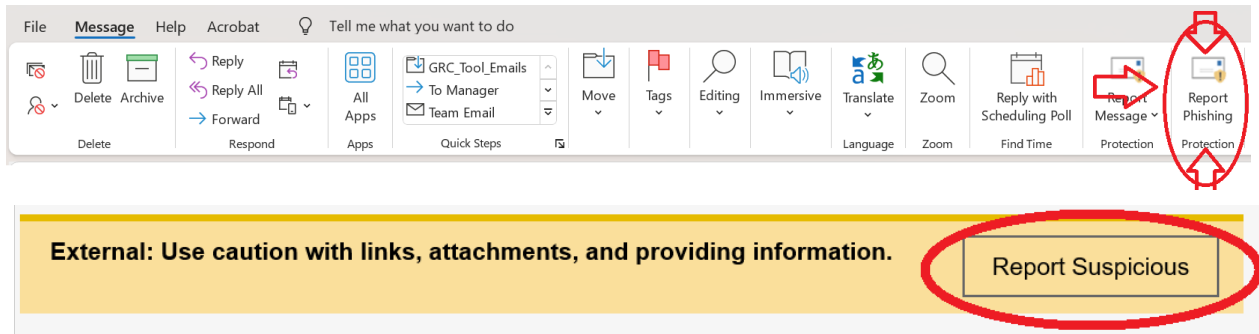
**Love-themed phishing emails:** "Spread the love this Valentine's Day. Click here to donate to a charity supporting love and romance."

## Don't click the link, Report it!

What should you do when you find a phishing e-mail?

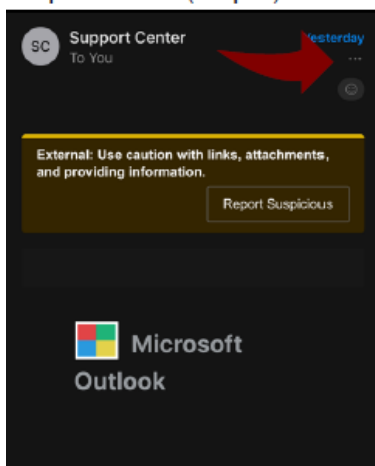
1. Report the phishing attempt within your mail client by clicking on the phish reporting button. Here are some options available depending on your e-mail configuration:



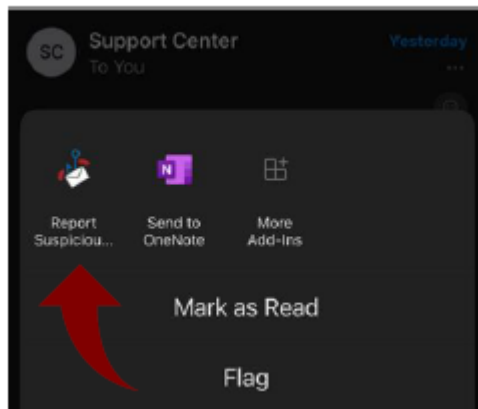


When using a mobile device:

Ellipsis menu (step 1)



• Ellipsis menu (step 2)



2. Report the email to your IT security support department so they are aware of the senders address.

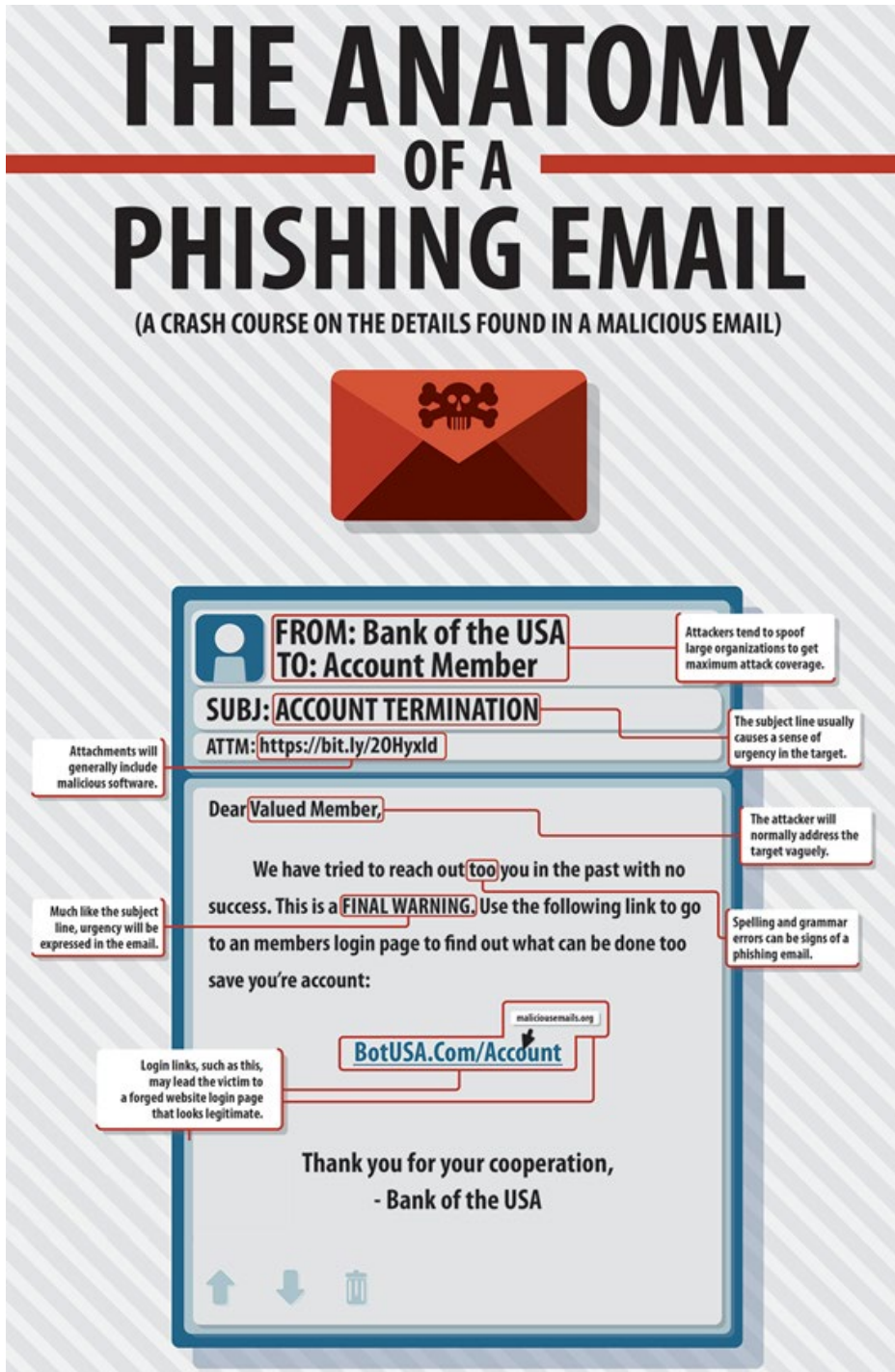

UCMC & Ingalls Information Security Office	IT.Security@uchicagomedicine.org
BSD Information Security Office	security@bsd.uchicago.edu
University IT Security	security@uchicago.edu

3. Do not forward the email to anyone other than your security team.

Further help in spotting a phishing e-mail:

# THE ANATOMY OF A PHISHING EMAIL

(A CRASH COURSE ON THE DETAILS FOUND IN A MALICIOUS EMAIL)



**FROM:** Bank of the USA  
**TO:** Account Member

**SUBJ:** ACCOUNT TERMINATION

**ATTM:** <https://bit.ly/20Hyxld>

Dear Valued Member,

We have tried to reach out too you in the past with no success. This is a **FINAL WARNING**. Use the following link to go to an members login page to find out what can be done too save you're account:

[BotUSA.Com/Account](https://BotUSA.Com/Account)

Thank you for your cooperation,  
- Bank of the USA

↑ ↓ 🗑

**Callout boxes:**

- Attachments will generally include malicious software.
- Much like the subject line, urgency will be expressed in the email.
- Attackers tend to spoof large organizations to get maximum attack coverage.
- The subject line usually causes a sense of urgency in the target.
- The attacker will normally address the target vaguely.
- Spelling and grammar errors can be signs of a phishing email.
- Login links, such as this, may lead the victim to a forged website login page that looks legitimate.

As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at [security@bsd.uchicago.edu](mailto:security@bsd.uchicago.edu).