

# How to Identify and Protect Yourself from Online Scams

Office of Information Security (OIS)

Office of Technology Services (OTS)

October 16<sup>th</sup>, 2020



# NCSAM Background



**DO YOUR PART.**  
**#BECYBERSMART**



NATIONAL  
**CYBERSECURITY**  
ALLIANCE



# What is Phishing ?

## BEWARE OF PHISHING!

### Top Tips to Avoid being Phished

1. **Question the urgency:** Ignore demands to change account info. Call OTS at 410-704-5151 to confirm account status.
2. **Consider the source:** Do you know the sender? Did you request the info in the email?
3. **Keep passwords private:** NEVER reply with your NetID/password.
4. **Think before you click:** Be suspicious of sensitive info requests through links. Call the sender to confirm the request.
5. **Report phishing:** Forward suspicious emails to [phishing@towson.edu](mailto:phishing@towson.edu) – then delete. Remember: No one at TU will EVER ask for your NetID password.

Spread the word, not the phish!  
Learn more at [www.towson.edu/phishing](http://www.towson.edu/phishing)



Phishers send messages using a sense of urgency and claiming to be from a business or organization that you may be involved. Additionally, email addresses, logos and login pages can all be spoofed to appear legitimate. Phishing attempts will often impersonate various types of Towson University communications.

### Received a suspicious email?

- From a desktop/laptop, report it using the 'Report Phish Button' in Outlook or
- From a mobile device, forward it to [phishing@towson.edu](mailto:phishing@towson.edu) then DELETE it
- Submit a Tech Help Ticket (<https://techhelp.towson.edu>)

# How to Identify Phishing

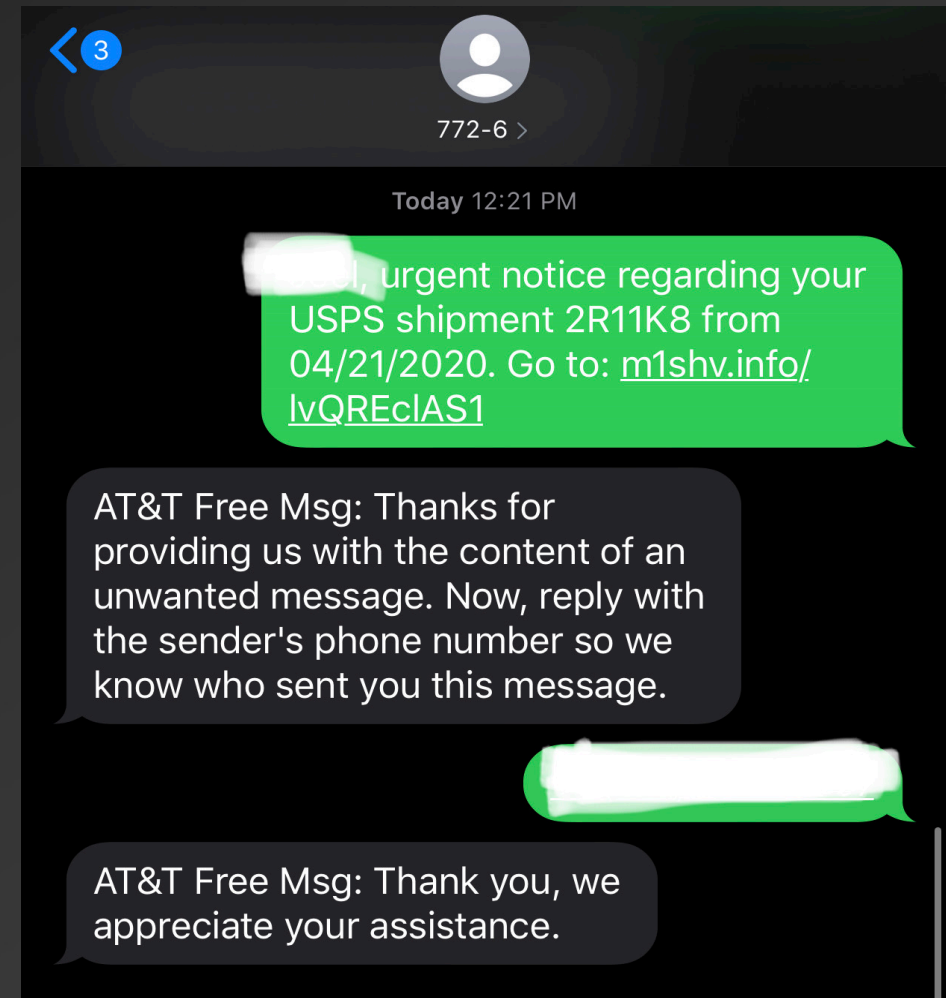
- Unknown sender, or an email from an unsolicited source.
- Unexpected attachments that are “.exe” or “.zip” files.
- Unfamiliar links in the body of the email.
- Unusual or strange purchase requests.
- Storage Space/account threats or urgent messages waiting.

# Secure your connection – Verify the Domain



# Tips to Protect Your Identity at Home

- Establish Text Alerts to help Fight Fraud
- Run an Antivirus scan periodically
  - Don't ignore updates
- Enable 2 factor authentication on personal accounts
  - Configure Privacy and Security and Login settings
- Report Phishing and Spam
  - Forward Text Scams to 7726 (SPAM)



# Report Phishing and Spam – Personal Outlook

The screenshot shows the Outlook interface with a phishing email open. The email is titled "Amazon Reward" and is from "Congratulations <fsdgrehygsdxg@j5YJo.baratheonboltons.com>". The main content of the email is a promotional message for a \$1000 Amazon gift card, which is a classic phishing tactic. The email includes a large image of a black Amazon gift card with "\$1000" and the Amazon logo. Below the image, it says "Take this 30 second survey about Amazon and we'll offer you a \$1000 exclusive reward." and provides a link "Click here to get started". At the bottom, there is a disclaimer: "\*PURCHASE REQUIRED. SEE OFFER FOR DETAILS. This advertisement was sent to you by a third party. If you are not interested in receiving future RewardZoneUsa advertisement, please Click Here. Alternatively, you can opt out by sending a letter to: RewardsFlow, LLC 128 Court Street, 3rd FL White Plains, NY 10601".

The Outlook interface shows the "Phishing Awareness E..." folder selected in the left sidebar. The right sidebar shows a list of actions for the email, including "Reply", "Reply all", "Forward", "Delete", "Mark as unread", "Flag", "Add to Safe senders", "Mark as junk", "Mark as phishing", "Block Congratulations", "Create rule", "Print", "Translate", "Show in immersive reader", "View message source", "Open in new window", "OneNote", "Evernote", and "Get Add-ins".

# Report Phishing and Spam – Personal Gmail

Updated FollowMyHealth Terms of Use and Privacy Policy Spam x

FollowMyHealth noreply@followmyhealth.com via sendgrid.net  
to me

Thu, Oct 17, 11:43 PM (4 days ago)

**Why is this message in spam?** It is similar to messages that were identified as spam in the past.

[Report not spam](#)

Reply  
Forward  
Filter messages like this  
Print  
Delete this message  
Block "FollowMyHealth"  
**Report phishing**  
Show original  
Translate message  
Download message  
Mark as unread

Hello,

The FollowMyHealth team has been working hard to add new features and services in order to improve your user experience. Today, we're emailing you to let you know about updates to our Terms of Use and Privacy Policy.

You may have noticed we updated our [Terms of Use](#) and [Privacy Policy](#) to provide more clarity about using FollowMyHealth, to address new features and functionality, and to include other updates and clarifications.

We encourage you to read our updated Terms of Use and Privacy Policy in full, but here are the high-level changes:

- How we collect, use, and disclose your information
- How we protect the security of your information
- How we may use and disclose your information for marketing or advertising purposes
- How we may display advertising or marketing to you while you use FollowMyHealth
- The manner in which FollowMyHealth may communicate with you

These terms went into effect for all users on August 14, 2019. Please be aware that by continuing to use FollowMyHealth, you acknowledge and agree to the updated Terms of Use and Privacy Policy. If you do not agree to the updated Terms of Use and Privacy Policy you can delete your FollowMyHealth account at any time. The Terms of Use are to be read in conjunction with the Privacy Policy, which is incorporated into the Terms of Use and forms part of our contract with you.

If you have any questions, please let us know.

[support@followmyhealth.com](mailto:support@followmyhealth.com)

Copyright © 2019 Allscripts, All rights reserved.

You're receiving this email because you have a FollowMyHealth® account or agreed to receive emails from your healthcare provider who uses FollowMyHealth®.

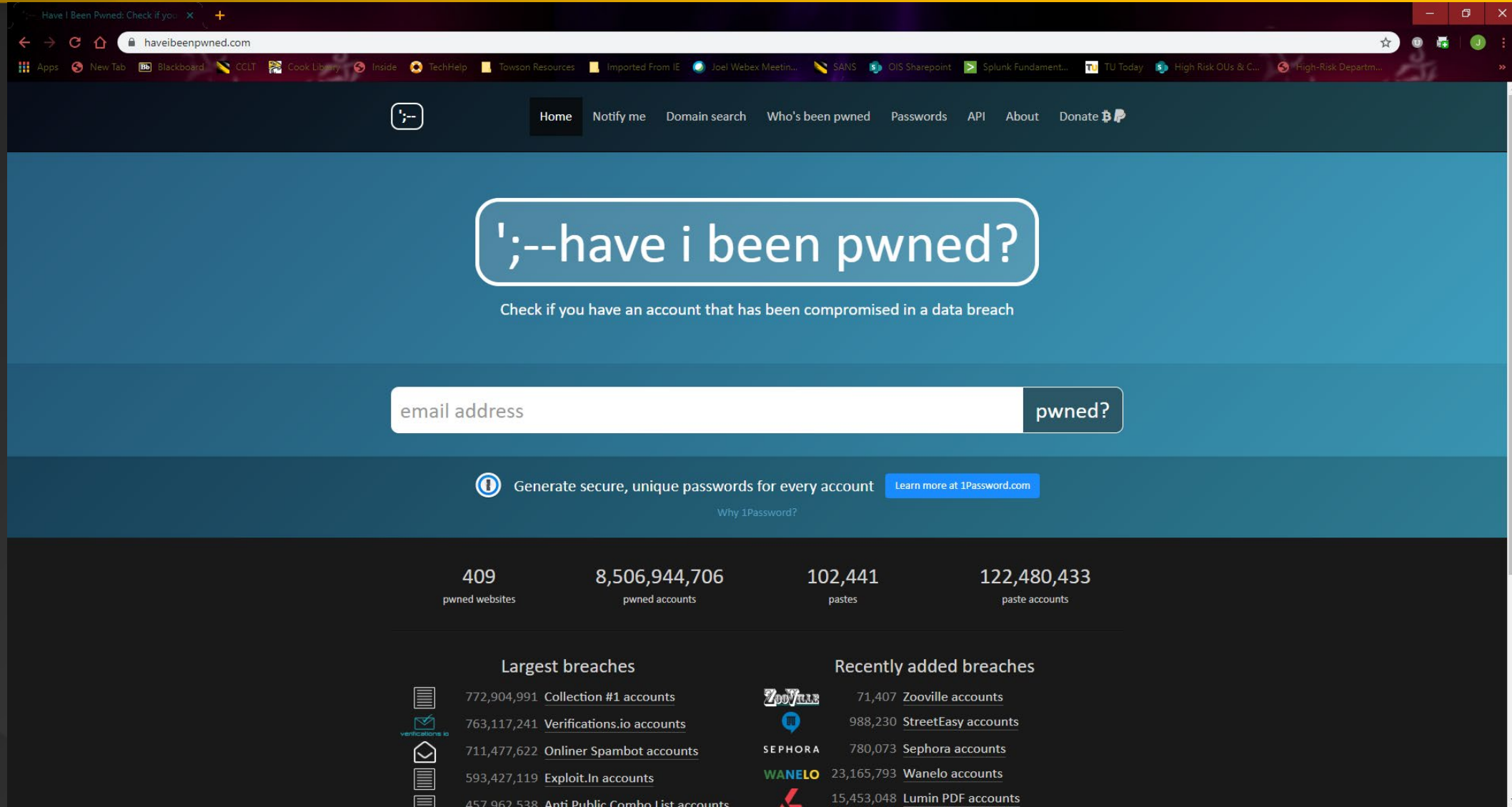
Our mailing address is:  
222 Merchandise Mart  
Chicago, IL 60654



# Free Resources



# Have I been Pwned: https://haveibeenpwned.com



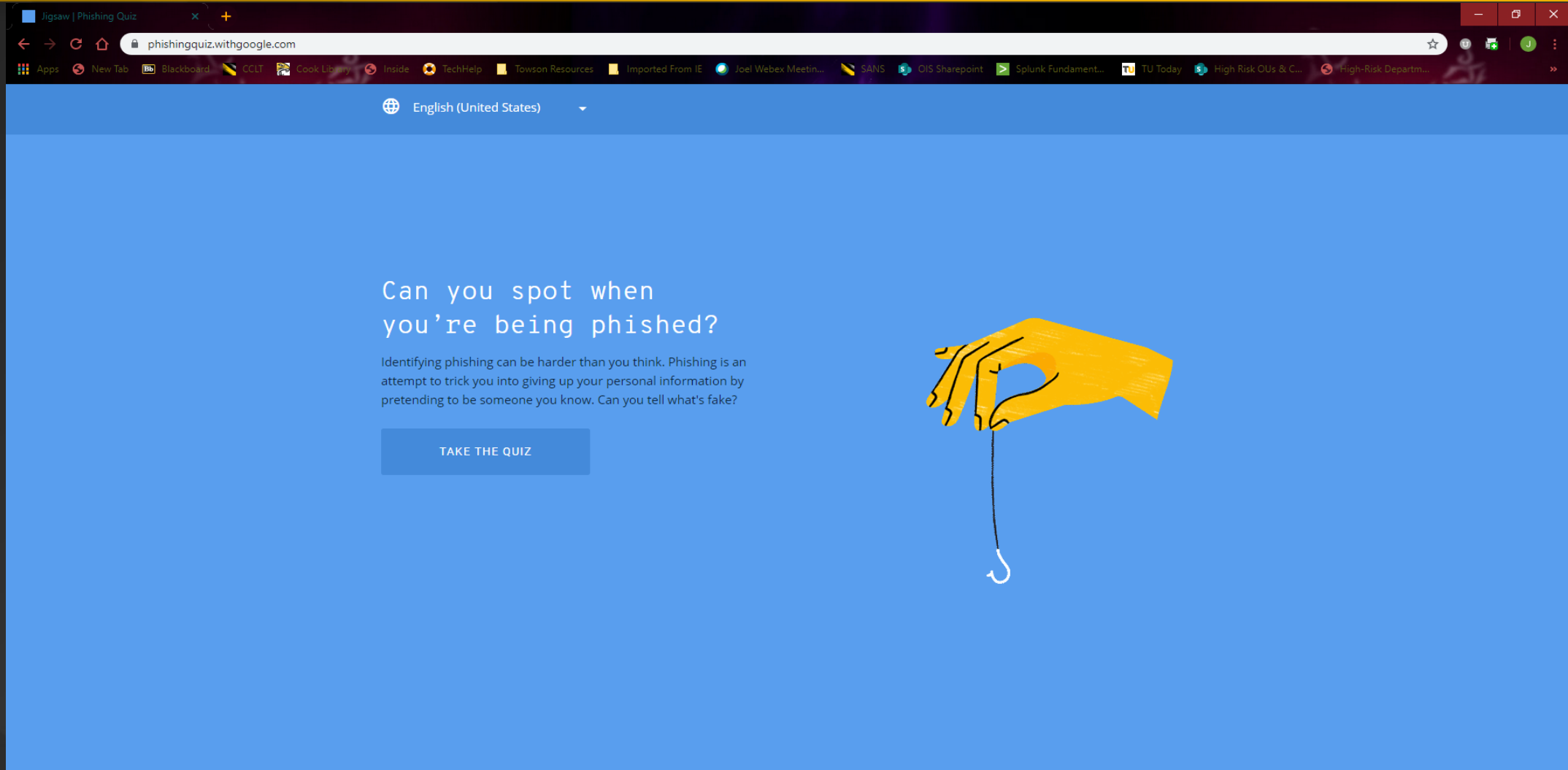
The screenshot shows the homepage of the 'Have I Been Pwned' website. The browser's address bar displays 'haveibeenpwned.com'. The navigation menu includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading asks ';---have i been pwned?' and prompts users to check if their accounts have been compromised in a data breach. A search input field labeled 'email address' is followed by a 'pwned?' button. Below this, there is a promotional banner for 1Password, stating 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. The footer section features four statistics: 409 pwned websites, 8,506,944,706 pwned accounts, 102,441 pastes, and 122,480,433 paste accounts. It also lists 'Largest breaches' and 'Recently added breaches' with their respective account counts and breach names.

Category	Count
pwned websites	409
pwned accounts	8,506,944,706
pastes	102,441
paste accounts	122,480,433

Category	Count	Breach Name
Largest breaches	772,904,991	Collection #1 accounts
Largest breaches	763,117,241	Verifications.io accounts
Largest breaches	711,477,622	Onliner Spambot accounts
Largest breaches	593,427,119	Exploit.In accounts
Largest breaches	457,962,538	Anti Public Combo List accounts
Recently added breaches	71,407	Zooville accounts
Recently added breaches	988,230	StreetEasy accounts
Recently added breaches	780,073	Sephora accounts
Recently added breaches	23,165,793	Wanelo accounts
Recently added breaches	15,453,048	Lumin PDF accounts

# Jigsaw | Google Phishing Quiz : <https://phishingquiz.withgoogle.com>




English (United States)

## Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

[TAKE THE QUIZ](#)





# Question & Answers



- Email questions to **[securityawareness@towson.edu](mailto:securityawareness@towson.edu)**
- If you would like an OIS team member to give an interactive virtual phishing or security awareness presentation to your group or department, please visit put in a **TechHelp** service request.

# Thank You for Attending Today's NCSAM Event

