How to Identify and Protect Yourself from Online Scams

Office of Information Security (OIS)
Office of Technology Services (OTS)
October 16th, 2020
NCSAM Background

DO YOUR PART.
#BECYBERSMART

TOWSON UNIVERSITY

NATIONAL CYBERSECURITY ALLIANCE
What is 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.

Incoming Email

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?
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 - 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

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 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)
Congratulations <fodgrhypodig@J5Ylo.barathonboltons.com>
Mon 9/30/2019 5:29 AM

You've been selected to participate in our monthly $1000 Amazon Promotion!

Click here to get started

*PURCHASE REQUIRED. SEE OFFER FOR DETAILS.

This advertisement was sent to pay for a delinquent bill. If you are not interested in receiving future RewardZoneUSA advertisements, please unsubscribe. Alternatively, you can opt out by sending a letter to: RewardZoneUSA, LLC, 159 Gulf Street, Suite A1, West Palm Beach, FL 33401.

This is an Advertisement. If you prefer not to receive further emails of this type, please click here to unsubscribe.

You may also write to us at: PO Box 3341 PMB 1541 Hollywood, FL 33041.
Report Phishing and Spam – Personal Gmail

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 Policies.

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, 2015. 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

Copyright © 2015. 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
Have I been Pwned:
https://haveibeenpwned.com
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

• 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