From:	All University on behalf of Information Technology
To:	All-University Mailing List
Subject:	[ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [April]
Date:	Friday, April 21, 2023 2:24:24 PM
Attachments:	image001.png image003.png image002.png

Roger Williams University

Information Security [INFOSEC] Briefing

Phone: 401-254-6363 E-
Mail: mediatech@rwu.edu

-

April - 2023 Cybersecurity Focus

It takes a village! We know firsthand higher-eds are frequent targets of malicious online attacks. The reason: universities have valuable data and technical resources threat actors seek to steal or exploit. To make matters worse, the number of threat actor groups is rising – especially in countries without extradition laws. **So let the games begin!** RWU's network and system engineers do a great job keeping the bad guys out while allowing legit traffic. However, threat actors turn to phishing when hacking a target's network perimeter is impossible. In this situation, you, the ground troops, are the most important line of defense. **As a collective community, we play a critical role in stopping the threat actors when technical controls cannot!**

Over the last several months, we noticed a significant increase in staff and faculty actively marking and reporting phishing emails. This data is great news! When the ***original recipient*** of phishing emails takes the time to **"mark it,"** it has a profound impact. Why? Phishing attacks arrive in waves. For example, the first wave of a phishing campaign typically targets a group of 50 recipients. This target size has the potential to get some "bites" yet is small enough to bypass SPAM filters. **When recipients in the first wave identify and classify the email as "phishing," subsequent waves are automatically blocked!**

For those unfamiliar, marking phishing emails is a simple process in both O365 and desktop versions of Outlook. On the O365 Outlook client, **marking a phish is done by right-clicking the phishing email and selecting "Reporting" followed by "Report Phishing."** The desktop version of Outlook is a little different and requires installing a "Report Phishing" add-in. Installing this add-in creates a ***Report Phishing*** ICON in the top ribbon bar of an open email. Pressing this ICON classified the email as phishing before automatically deleting it. Using either method only takes a few seconds to setup and use.

Thank you to all our cybersecurity ambassadors that continue to help mark and report phishing emails! Your actions are making a positive impact on reducing risks and increasing RWU's overall resilience! If you need guidance before "marking" an email as phishing, please do not hesitate to forward it to spam@rwu.edu.

We wish you a wonderful spring!

Sincerely,
IT Management

Don't take the bait! IT will never ask you for your username and password via email.
Phishing e-mails attempt to deceive you into giving up private information in a response
to a message or by leading you to a fraudulent web site.

For more tips about phishing, go to www.phishinginfo.org.

Follow Roger Williams University Information Technology
on Twitter and Facebook for alerts, technology notifications, tips, and news.

This has been an official communication for Roger Williams University's Office of Information Technology. You are receiving this message because of your current relationship with Roger Williams University.