From: All University on behalf of Information Technology
To: All-University Mailing_List
Subject: [ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [AUGUST]
Date: Monday, August 1, 2022 8:58:38 AM
Attachments: image001.png
image003.png

Roger Williams University

Information Security [INFOSEC] Briefing

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

August - 2022 Cybersecurity Focus

Did you catch a Phish this summer? During the week of June 27th, you may [or may not] notice an email that came from a staged phishing exercise. By design, this training exercise mimics actual phishing emails we encounter. It appeared to originate from RWU's IT department asking employees to update their account security settings - via a hyperlinked form to enter their *password* and *mobile phone number*. This live training aims to safely prepare us for cyber threats we previously encountered and expect will continue. Unlike a real phish, the hyperlink in the email goes to a safe page. Any data entered by a user "evaporates" after clicking the submit button, and the user gets redirected to a training page detailing the signs to spot this phish.

Overall, the RWU Community continues to make significant progress in identifying and reporting phishing threats. In this latest test, we are happy to report a 98% overall success rate. Most important is how quickly users report suspicious emails to RWU MediaTech. This "time-to-report" metric is critical because it enables IT to block, contain, and mitigate the phishing threat before other users inadvertently fall victim. **A big shout-out to Joann Silva in the Cumming School of Architecture for reporting the staged phishing email approximately 1 minute after it was delivered!**

Last month, RWU IT implemented multi-factor authentication (MFA) to better protect our university email and data stored in the O365 cloud environment. **Despite new anti-spam and multi-factor authentication investments, scammers continuously try to hack employee accounts.** Be aware that some new scam tactics include sending a text message to your cell phone, after sending an initial email, to trick you into sending them your one-time MFA code. This is **just another clever trick to circumvent RWU's security controls and the reason why last month's live training asked users to enter their mobile phone number used for MFA access codes.**

Don't get hooked on future phishing emails [training or actual]. You are the RWU's first and last line of defense against phishing attacks**. If you encounter an email with [EXT] in the subject line that includes hyperlinks or attachments, proceed with caution.** If unsure, do not hesitate to ask MediaTech for assistance or forward the email to *spam@rwu.edu*. Security **awareness is one of our best defenses against phishing threats.** If you have not completed RWU's cyber training or visited any knowledge-based articles, we encourage you to do so as soon as possible.

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.