From: All University on behalf of Information Technology
To: All-University Mailing List
Subject: [ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [June]
Date: Tuesday, June 28, 2022 12:08:08 PM
Attachments: image003.png

Roger Williams University

Information Security [INFOSEC] Briefing

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

June - 2022 Cybersecurity Focus

Happy summer to the RWU Community! Vacation, staycation, or anything in-between, it's a great time to digitally disconnect and relax. In this month's INFOSEC let's start by taking a trip down memory lane: everyone jumping into the car for a ride to the beach. If you go back far enough in time, seat belts were optional and cars did not have auto-locking doors. Safety and security were very relaxed and often an afterthought. Fast forward to the present day; it's now second nature to buckle up and listen for the doors to automatically lock. Although these advancements were much needed, they required new laws and willingness on our part.

A new IT security improvement was recently implemented here at RWU, forcing a second-level authentication, such as a one-time unique passcode, before allowing users access to their computer or email services. This multifactor method (a.k.a. MFA/2FA) is a necessary security control. Important enough that cyber insurance carriers are mandating their policyholders use it or risk getting dropped! Analogous to seat belt laws, MFA requires some action on our part. First, your mobile phone is now a critical prerequisite to the daily login process. Second, an "authenticator" app is required to install. And finally, a little extra patience is needed after finding a comfortable seat to do some work, but realize your phone is in the other room and you need it to login. **MFA may take some "getting used to", but moving forward, it will be worth it!**

MFA is an excellent security control but hackers are trying to find clever ways around it. One method is "smishing." This scam uses cleverly crafted SMS text messages to trick you into taking action. A common smishing scam based on MFA uses an unsolicited text message instructing you to reply with any MFA codes received via text message immediately. If the hacker already has your standard credentials, they must promptly trick you into supplying the one-time passcode. So it is no surprise you will receive this malicious text message just before an unauthorized login. Stay ahead of scams by spotting message attacks. Here are some questions to help identify a messaging attack:

- **Does the message create a tremendous sense of urgency, attempting to rush or pressure you into taking action?**
- **Does the message ask you to forward a multifactor authentication code? Note: RWU-IT and Media Tech agents do not use text messaging to correspond with users.**
- **Does the message come unsolicited and looks like the equivalent of a "wrong number?" If so, do not respond to it or attempt to contact the sender; delete it.**
- **Is the message taking you to websites that ask for personal information, credit card, passwords, or other sensitive information?**

Cybersecurity is everyone's responsibility, and we must all play an active part in protecting the integrity, availability, and confidentiality of RWU's systems and data. **For those with outstanding cyber training, you should receive email reminders from RWU's Litmos training system.** It only takes **10-15 minutes** to complete and is an excellent way to **build your cyber shield**!

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.