From: All University on behalf of Information Technology
To: All-University Mailing List
Subject: [ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [May]
Date: Wednesday, May 24, 2023 11:56:37 AM
Attachments: image001.png

Roger Williams University

Information Security [INFOSEC] Briefing

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

-

May - 2023 Cybersecurity Focus

Hip, hip, hooray, the official kick-off to Summer is just a few days away! Do you plan on taking some well-deserved time off this Summer? Whether it be a relaxing staycation or a hike across Alaska, most of us will soon break the usual routines in favor of spending time in the sunshine with family and friends. If you already started planning activities, you will likely notice the increasing number of online "self-service" systems. **Going to the city – ensure you install the mobile parking app. Attending a show or professional sporting event, keep a copy of your e-tickets. Need to make a dinner reservation – you guessed it, click the reservation button on the restaurant's website.** Like it or not, we are immersed in a digital world, and almost impossible to disconnect, even while on vacation.

You're on vacation, but scammers are working overtime. Unfortunately, the overseas prince still needs your help to invest in the US, and your favorite dean's baby grand piano is still available! We are no strangers to scams and can attest that some are obvious to spot while others take a more subtle approach to trick you. Below are a few scam tactics to keep an eye out for this Summer:

- **Be cautious with QR codes.** This array of blocked dots visually represents an alpha-numeric string, such as a hyperlink URL. When used properly, they provide a quick method to open a website using your phone's camera. This level of convenience makes QR codes an attractive marketing tool - to the extent that restaurants post them at dinner tables for online menus. Other merchants display them in storefront windows to download their mobile app or to register with an online rewards program. Although very convenient, hackers see them as an opportunity. **One popular scam is to overlay legit QR codes with ones that open malicious sites. This tactic is especially true in public locations that allow scammers full access to altering the original code image.** Because QR codes eliminate the hassle of typing URLs, you may only know the destination site once the page loads. Be reserved when scanning public QR codes. Take a moment to see if the code was altered or has a sticker overlaid, masking the legit code.
- **Public WIFI/Hotspots**. Staying at a hotel or visiting a park for the day and want WIFI access? Most venues realize the need to provide patrons with free WIFI. **One**

prevailing scam is to create temporary, open WIFI hotspots with names that reflect the event or location. Connecting to these counterfeit networks creates a "man in the middle" situation that allows the scammer to capture the sites you visit and the data you enter. This scam increases the risk of stealing your account credentials or credit card info. Be cautious when connecting to public hotspots, especially if you intend to visit sites that require entering personal or financial information. In addition, be sure to disable your mobile device from automatically connecting to open WIFI networks.

Nothing can ruin a vacation faster than realizing you got hacked. Do not let your plans get derailed by scammers. Keep your identity and restricted data safe by understanding the tactics they use. Unfortunately, cybercrime remains a lucrative business and has the potential to "bite" us when we lower our cyber shields. We need to play a good defensive game, so please remain aware while having fun this Summer!

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.