From: All University on behalf of Information Technology
To: All-University Mailing_List
Subject: [ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [February]
Date: Friday, February 24, 2023 1:54:48 PM
Attachments: image001.png
image003.png
image004.png

Roger Williams University

Information Security [INFOSEC] Briefing

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

February - 2023 Cybersecurity Focus

Don't take the bait! The RWU IT Department wants to remind faculty and staff that cybercriminals continue to target University employees. Even with multifactor authentication (MFA) in place, we see an uptick in the number of sophisticated phishing emails seeking to steal account credentials, sensitive university data, and personal information. **Knowing is half the battle, so let's take a look at how a typical attack plays out:**

1. Send phishing email: trick a user into clicking a hyperlink. Some phishes are very easy to identify, while others are not! Most often, a cloned exact replica login page that uses multiple redirects is behind the hyperlink.
2. Threat actor intercepts any user credentials entered on the landing page of the hyperlink and then forwarded them to the real login page (such as Google or Microsoft login). This action prompts the real service provider to send the one-time Multifactor passcode to the user's mobile phone.
3. The user then enters the one-time MFA passcode into a subsequent fake web page before passing it over to the real Microsoft site that issues a valid session token. **To the user, everything seems legit.**
4. The hacker then steals this session token to access the user's SharePoint or email account to stage malware or steal sensitive documents. They also use this opportunity to switch the multifactor setting and add forwarding rules to further their malicious intentions.

How can I protect my accounts? Quite often, the initial phishing email provides the most evidence. First, does the email's subject line include the external flag [EXT]? This step is important because almost all official University emails will originate from an internal or trusted 3rd party. The next area to look at is the sender. In the above example, the threat actor spoofed "IT DeskControl" for a display name; however, looking more closely at the actual sending address [*noreply@flonicrusampic*] proves it did not originate from an @rwu.edu account. Unfortunately, validating the sending account is not straightforward when using mobile devices as they typically default to show only the display name over the actual address. **Rule of thumb: big red flag if the sender displays as an RWU user but the subject field includes the external flag [EXT].** If you are still suspicious, forward the email to spam@rwu.edu. This step will open a Mediatech ticket to inspect the message and contents.

Keeping your identity and restricted data safe by spotting the early signs of phishing emails is

the best way to avoid online scams. Unfortunately, cybercrime remains a lucrative business, and the lack of international laws makes it very hard to prosecute cyber criminals in foreign countries. **We need to play a good defensive game, so please keep your cyber shield up by visiting RWU's cyber training portal and complete any outstanding modules.**

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.