

**From:** [All University](#) on behalf of [Information Technology](#)  
**To:** [All-University Mailing List](#)  
**Subject:** [ALL-UNIVERSITY] RWU INFOSEC Monthly Briefing [September]  
**Date:** Thursday, September 22, 2022 11:13:22 AM  
**Attachments:** [image001.png](#)

---



## Information Security [INFOSEC] Briefing

Phone: 401-254-6363 E-Mail: [mediatech@rwu.edu](mailto:mediatech@rwu.edu)

---

### September - 2022 Cybersecurity Focus

**RWU.EDU is an active target!** In past INFOSEC briefs, we typically highlight cybersecurity trends and tactics to stay safe while online. This month's message hits much closer. **In recent weeks, the University encountered unprecedented phishing attacks!** This pattern is often a precursor to more malicious intentions, such as ransomware. The tactics in these phishing emails are sophisticated and are often part of a multi-phase attack. Capturing endusers email addresses, passwords, and cell phone numbers is the first phase. This is followed by attempts to hack endusers Multi-Factor Authentication (MFA) codes. If MFA is compromised, the threat actors now have full access to that user's entire O365 account. This includes email, phone numbers, and their OneDrive which can be used to host and distribute malware.

**A single compromised account can significantly disrupt RWU's business!** [The shutdown announcement of Lincoln College](#) last May is one example of the damage that can follow these types of cyberattacks. **Our frontline defense starts you YOU!**

#### **Please take a moment to review these tips for staying safe:**

1. Mark suspicious emails as "phishing." **Below are instructions for reporting phishing as well as additional action to take.** If you're uncertain about an email and need to have it checked, please forward it to [spam@rwu.edu](mailto:spam@rwu.edu). If the message is deemed malicious, IT security will reach back to you and ask you to mark the email as phishing. **Please note:** Only send the original email (not a copy) as it contains the original header IT uses to determine its validity.

#### **Phishing Reporting Instructions:**

**O365 email client: Select the email message (LF click), followed by a RT click (iPad user press and hold email message). You should then see a "Report" option. Under this option, select "Report phishing."**

#### **Additional Actions**

1. If you receive an email with the sender's display name reflecting an RWU employee

(provost, dean, president, etc.) but shows **[EXT]** in the subject, please mark it as "phishing" or send it to [spam@rwu.edu](mailto:spam@rwu.edu) to have it checked.

2. **Do not let curiosity get the best of you!** If you receive an email hyperlink to download a file, please call the person to validate that they legitimately shared a file with you. We are finding hacked O365 accounts from other universities and K12 schools used as staging sites to distribute malware.
3. **Phishing for credentials.** IT does not send emails asking users to "update" their accounts. Although the University sends reminder emails to users when their password is about to expire, we will not ask you to "update" the account. When it's time for a password reset, it's best practice not to use a hyperlink embedded in an email. Instead, go to <https://passwords.rwu.edu> and follow the steps to "Change Password."
4. Multi-Factor Authentication (MFA) is the last line of defense. This safeguard provides a final barrier against compromised passwords. **If you receive unsolicited DUO push notifications on your mobile device, someone with your username and password is likely attempting to access your account.** [Resetting your password](#) will stop generating DUO push notifications on your mobile device. Be aware that threat actors typically perform a series of back-to-back login attempts that generate multiple DUO push notifications. They anticipate you'll eventually hit the "accept" button.

We appreciate your awareness and cooperation as we continue to keep RWU safe! [Now is an excellent opportunity if you have not completed your cyber training.](#) It only takes 10-15 minutes to complete.

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](http://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.

