Roger Williams University

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

In past INFOSEC briefs, we typically highlight cybersecurity trends and tactics to stay safe while online. This month's message hits much closer.

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.

The shutdown announcement of Lincoln College last May is one example of the damage that can follow these types of cyberattacks.

1. Mark suspicious emails as "phishing."

   If you're uncertain about an email and need to have it checked, please forward it to 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. Only send the original email (not a copy) as it contains the original header IT uses to determine its validity.

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

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

2. 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. 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.

   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.

Follow Roger Williams University Information Technology on Twitter and Facebook for alerts, technology notifications, tips, and news.