The University of Texas Rio Grande Valley

Information Security Office

Dear Students, Faculty, and Staff

As the Russian – Ukrainian conflict continues, we have detected state-sponsored and organized crime groups launching opportunistic cyber-attacks.

While the most common form of attack continues to be phishing emails, several other attack vectors are becoming more prevalent. Including Smishing (phishing via text message/SMS) and repeatedly using compromised credentials to send multi-factor authentication (MFA) requests until the targeted user accepts an MFA request.

While it is important to always be on guard, the current world situation reminds us that we must be extra vigilant to protect ourselves from cyber threats.

You are critical to the defense of UTRGV. Please stay especially vigilant and remember:

- Don't click on links or open attachments until you have carefully considered and verified the source.
- If you receive an MFA prompt that you did not initiate, do not accept it.
- Take your time. Hackers use urgency as a weapon. When in doubt, delete the message and move on.
- If you click on / open / enter something and get concerned, contact the IT Service Desk immediately.
- IT will never ask for your password. Never give it out over the phone, text, or email.
- Never let anyone else use your password or credentials.
- Don't re-use passwords. Attackers use passwords from one area to get into others, so use a different password on every site.

UTRGV has strong controls that prevent thousands of these messages from reaching your mailbox every day, but skilled attackers know how to avoid detection. We're counting on your care and diligence; please feel free to reach out with any questions.

Sincerely,

Information Security Office and the Office of the Chief Information Officer