The University of Texas Rio Grande Valley™

Information Security Office

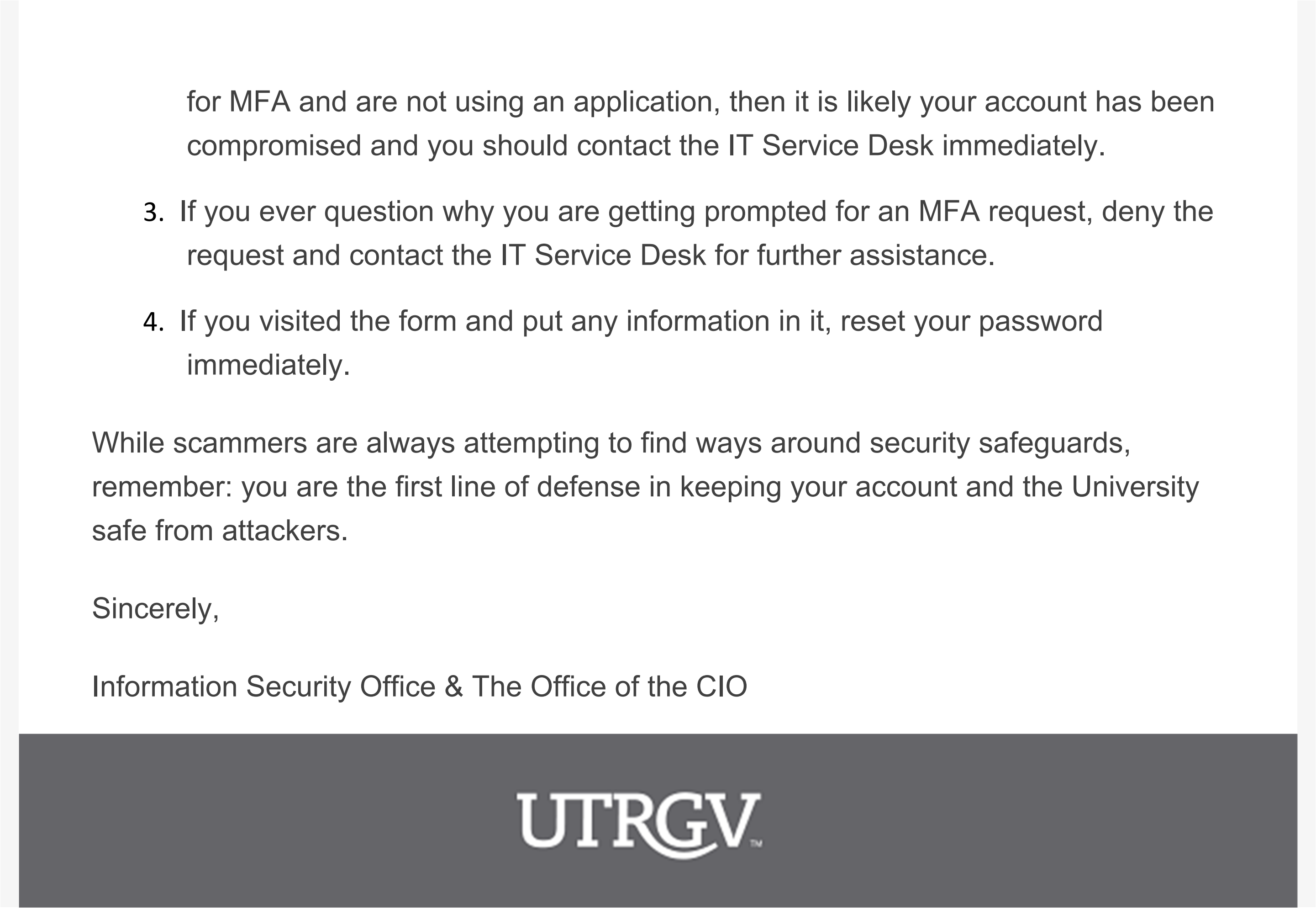
Dear UTRGV Faculty and Staff,

A new phishing scam is currently affecting UTRGV and many other organizations. This scam tricks users into compromising their credentials and successfully attacks when they unsuspectingly authorize the multi-factor authentication (MFA) request. **Please be vigilant and only approve MFA requests when you are actively seeking to access your email or another MFA-protected application off campus.**

This phishing message differs from the typical phishing scam in that it does not use a hyperlink to try and get you to “give up” credentials or other sensitive information. Instead, this scam asks you to copy and paste the URL from the message into a web browser, which takes you to a Google form. Once the attackers have your information, they then seek access to your email. Since multi-factor authentication is in place for email, you will receive an MFA request to authorize access.

Please know that this scam can be stopped if you remember the following:

1. MFA is only required for email access when you are not connected to the UTRGV network.
2. Only authorize an MFA request when you knowingly attempt to access a resource that requires MFA. This means that if you are prompted for MFA to access your email when you are on the UTRGV network or if you are prompted



for MFA and are not using an application, then it is likely your account has been compromised and you should contact the IT Service Desk immediately.

3. If you ever question why you are getting prompted for an MFA request, deny the request and contact the IT Service Desk for further assistance.
4. If you visited the form and put any information in it, reset your password immediately.

While scammers are always attempting to find ways around security safeguards, remember: you are the first line of defense in keeping your account and the University safe from attackers.

Sincerely,

Information Security Office & The Office of the CIO

UTRGV