Texas Council Risk Management Fund

CYBER RISK CONTROL

Staying Safe Online

Use Strong Passwords

Make Passwords at least 16 characters, random and unique for each account. Remember that simple passwords can be guessed. Threat actors can also use software to 'break' less-complex passwords. Use a password manager that will store passwords in a secure manner.

Recognize and Report Phishing

Most online intrusions are a result of a user receiving a "phishing" message and downloading malware or providing their personal information to a scammer. Learn how to spot phishing attempts. Be mindful of the little details in the emails that can be a tip off to recognizing a phishing message. Report phishing messages using the prescribed method from your IT Department. Make sure the message is deleted after reporting.

Turn on Multifactor Authentication (MFA)

Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and applications. Using MFA will make your accounts more difficult to hack. Threat actors look for easy pickings.

Update Software

When devices, applications, or programs (particularly endpoint protection programs) notify us that updates are available, users should install them based on the maintenance procedures detailed from their IT Department. Updates close security holes and fix bugs in software. Your IT Department should strive to install updates automatically without user assistance.

To schedule a Risk Assessment visit, Incident Response Plan Table-Top Exercise, or for Cyber Risk questions, contact:

Lee Cain, Cyber Risk Services Advisor

Texas Council Risk Management Fund

10535 Boyer Blvd., Suite 100, Austin, Texas 78758

Direct: 512-427-2322

Cell: 512-619-1437

Email: Lee.Cain@sedgwick.com

Visit TCRMF.org/cyber-security for policy templates, cyber check lists, and best practices. Contact Lee Cain for log in credentials to access this secure area of the website.