City of Edinburg
Department of Information Technology (DoIT)
Cybersecurity Awareness Program (CAP)

Introduction
The City's Cybersecurity Awareness Program (CAP) is dedicated to educating end users and safeguarding our critical infrastructure against cyber threats. Through effective risk management, containment, and breach eradication, we aim to foster a culture of cybersecurity readiness. By establishing a shared governance model and providing essential tools, we fortify the City's defenses against evolving cyber risks.

Purpose
CAP educates City employees on cybersecurity fundamentals, common threats, vulnerabilities, and best practices to safeguard sensitive information. Targeting all City personnel utilizing internet-connected devices, local networks, servers, emails, databases, and other City technology, the program equips employees with practical strategies to mitigate risks both at work and at home.

What is included in CAP
CAP offers various training programs conducted throughout the fiscal year, supported by a comprehensive set of policies. Initiated during HR orientations, CAP training is mandatory for all new hires utilizing City technology. Upon successful completion of CAP training, access to City resources is granted by the Department of Information Technology (DoIT).

DoIT also disseminates a monthly Cybersecurity Awareness Newsletter containing safety reminders, valuable information, and resources. Additionally, DoIT hosts monthly in-person cybersecurity training sessions named "Coffee Hacks and Cyber Attacks" for interested employees. At the cybersecurity awareness coffee mornings, we go beyond traditional training methods to provide a hands-on experience that resonates with our staff. Employees gather to witness firsthand the vulnerabilities that threaten our digital world. Using readily available tools like the Flipper Zero, Rubber Ducky USBs, OMG cables, and Raspberry Pi's with Linux platforms such as Kali and

Parrot, we shed light on the ease with which threat actors can operate. Our team showcases password cracking techniques, credential harvesting, and the alarming simplicity of compromising devices.

Another vital component of CAP is the use of Knowbe4 for quarterly phishing campaigns. Detecting and avoiding phishing attempts are crucial aspects of strong cybersecurity. These campaigns assess users' vulnerability levels and awareness of phishing attacks, covering various examples such as phishing emails, spear phishing, link manipulation, fake websites, malware, and mobile phishing (smishing).

In today's dynamic digital landscape, maintaining cybersecurity awareness is important to protect the City's infrastructure. By sharing our expertise, we aim to create a ripple effect of cyber-resilience, preparing individuals beyond our organization to navigate the digital landscape securely.

“Our commitment to safety and integrity underscores our top priority in empowering employees and fortifying our defenses against cyber threats” says I.T. Director Danny Vera.

Contact Danny with questions at dvera@cityofedinburg.com or 956-388-1805.

"Coffee Hacks and Cyber Attacks" program logo: