Security Awareness Training Schedule – 2026

This document outlines the proposed 2026 Security Awareness Training Schedule, designed to strengthen the City's cybersecurity posture through consistent, targeted learning opportunities. The schedule includes monthly training topics and quarterly phishing simulations.

Calendar Layout – Monthly Training Topics and Learning Objectives

Month	Training Topic	Learning Objectives
January 2026	Phishing	Recognize phishing emails, identify red flags, understand reporting procedures.
February 2026	Malware	Explain malware types, understand infection vectors, learn prevention strategies.
March 2026	Physical Security	Increase awareness of tailgating, badge usage, and device protection responsibilities.
April 2026	AI & Deepfakes	Understand risks of generative AI, identify deepfakes, avoid AI-driven scams.
May 2026	Social Engineering	Recognize manipulation techniques and practice verification procedures.
June 2026	Multi-Factor Authentication (MFA)	Learn MFA best practices and understand how MFA reduces unauthorized access.
July 2026	Ransomware	Understand ransomware behavior, prevention, and incident reporting steps.

August 2026	Removable Media	Identify risks associated with USB devices and learn safe handling procedures.
September 2026	Insider Threats	Recognize risky behavior, understand internal risks, and learn reporting pathways.
October 2026	Data Privacy & Security	Apply correct data privacy practices, classify data, and protect PII.
November 2026	Business Email Compromise (BEC)	Identify impersonation attempts and understand financial workflow protections.
December 2026	Password Security	Apply strong password practices, use passphrases, and secure MFA recovery settings.

Quarterly Phishing Simulations

- Q1 Simulation – March 2026
- Q2 Simulation – June 2026
- Q3 Simulation – September 2026
- Q4 Simulation – December 2026