WaTech
Washington Technology Solutions

Cybersecurity Awareness Training Program Update

Agency responsibilities for IT system users:

- ✓ Ensure **all users** are aware of basic information security.
- ✓ Enroll **all users** in refresher training and require training completion at least **annually**.
- ✓ Enroll **new users** in training and require training completion **within 30 days** of their start date.
- ✓ Maintain training records and **annually** certify compliance with the WaTech's security standards and policies.

Awareness Training Policy SEC-03 was 141.10 (1.4, 2.1, 4.5)

Adopted: November 28, 2023

Cybersecurity Awareness Training Objectives

- ✓ Reduce cyber risks.
- ✓ Enhance data protection.
- ✓ Build a security culture.
- ✓ Strengthen overall security.
- ✓ Prevent incidents.

IT training platform and content:

- ✓ Legacy training content sunset date May 31, 2024.
- ✓ WaTech will provide new training content annually beginning July 1, 2024.
- ✓ Agencies must request authorization from WaTech's state Chief Information Security Officer to use third-party training platforms and content.

Learning Center enrollment:

- ✓ Agencies define audiences (training groups) and deployment schedules.
- ✓ Agencies must submit a Zendesk ticket with the Department of Enterprise Services (DES).

Cybersecurity Awareness Program Content

- Information security basics.
- Password and access management.
- Protection from malicious code.
- Email phishing and other threats.
- Proper data handling and the consequences of unintended exposures.
- Social engineering.
- Recognizing and reporting incidents.
- Social media threats.
- Uses of personal information technology – internet of things.
- Information security and privacy policies.
- Protection of information assets.

Cybersecurity Awareness Program Reporting

Agency Reporting:

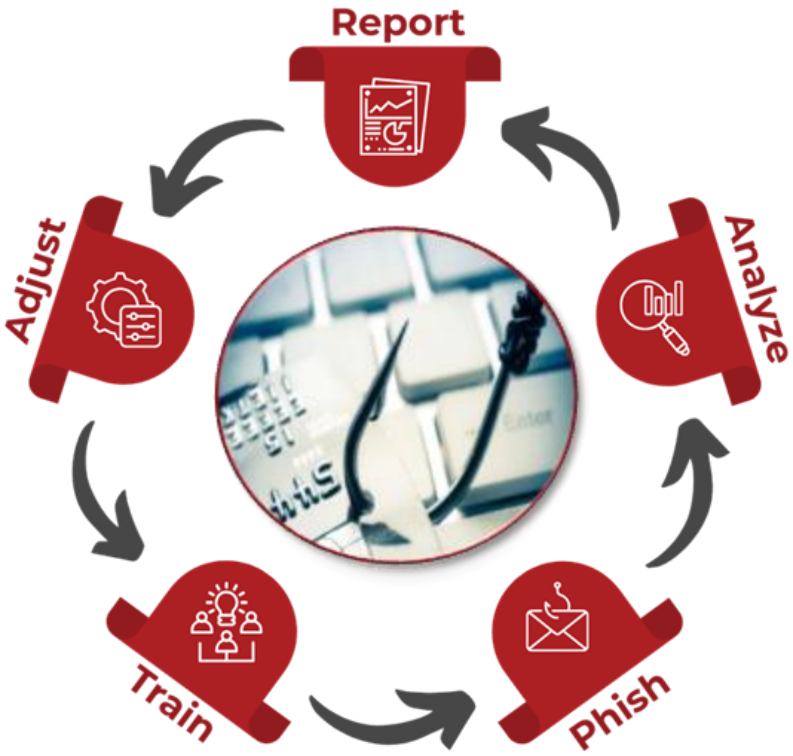
- ✓ Program training cycle based on **fiscal year (July – June).**
- ✓ **Compliance expectation – 85% of employees complete training.**
- ✓ First compliance report due to WaTech – **September 2025.**

Current Employees:
Agencies will decide when their employees take the training.

New Employees:
Completion within 30 Days of employment.

What is Phishing?

Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malicious software.



Phishing Simulation Benefits

- Increased awareness.
- Risk mitigation.
- Improved security culture.
- Compliance Requirements.
- Protection of intellectual property.
- Enhanced trust.