

Safeguard Your Entire Organization



**CYBER
FLORIDA**
the FLORIDA CENTER FOR CYBERSECURITY

The Arruda Group provides risk mitigation to alleviate exposure both internally and externally.

Take Action

Grow Your Organization

Rest Assured

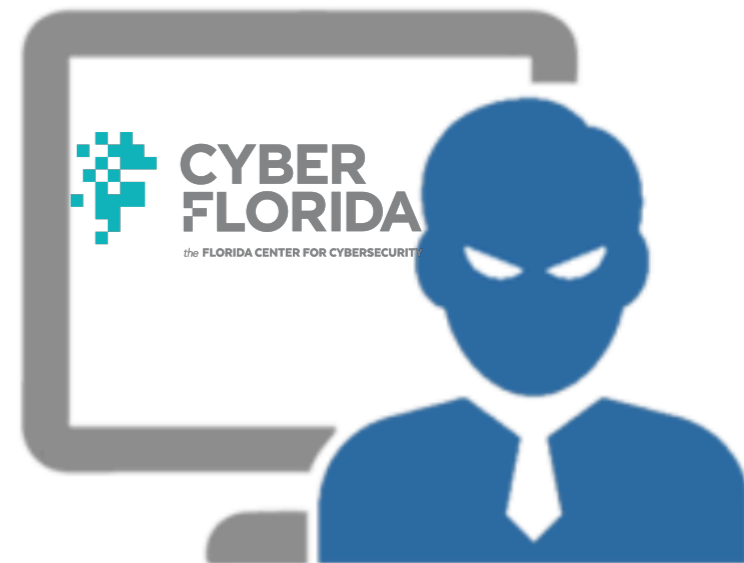
Network Noise

STACY M. ARRUDA

STACY M. ARRUDA

Objectives

- Listen to the Noise
- Incident Response Plan
- Intelligence
- PIO
- Mitigation



Overview

Scope

Approximately 2 hour instructor facilitated// discussion based event

Purpose

Discuss the importance of threat intelligence, coordination, collaboration, information sharing, cyber insurance, Incident Response Planning, and response capabilities to a significant Cyber incident.

Rules of Engagement

Participant Roles and Responsibilities

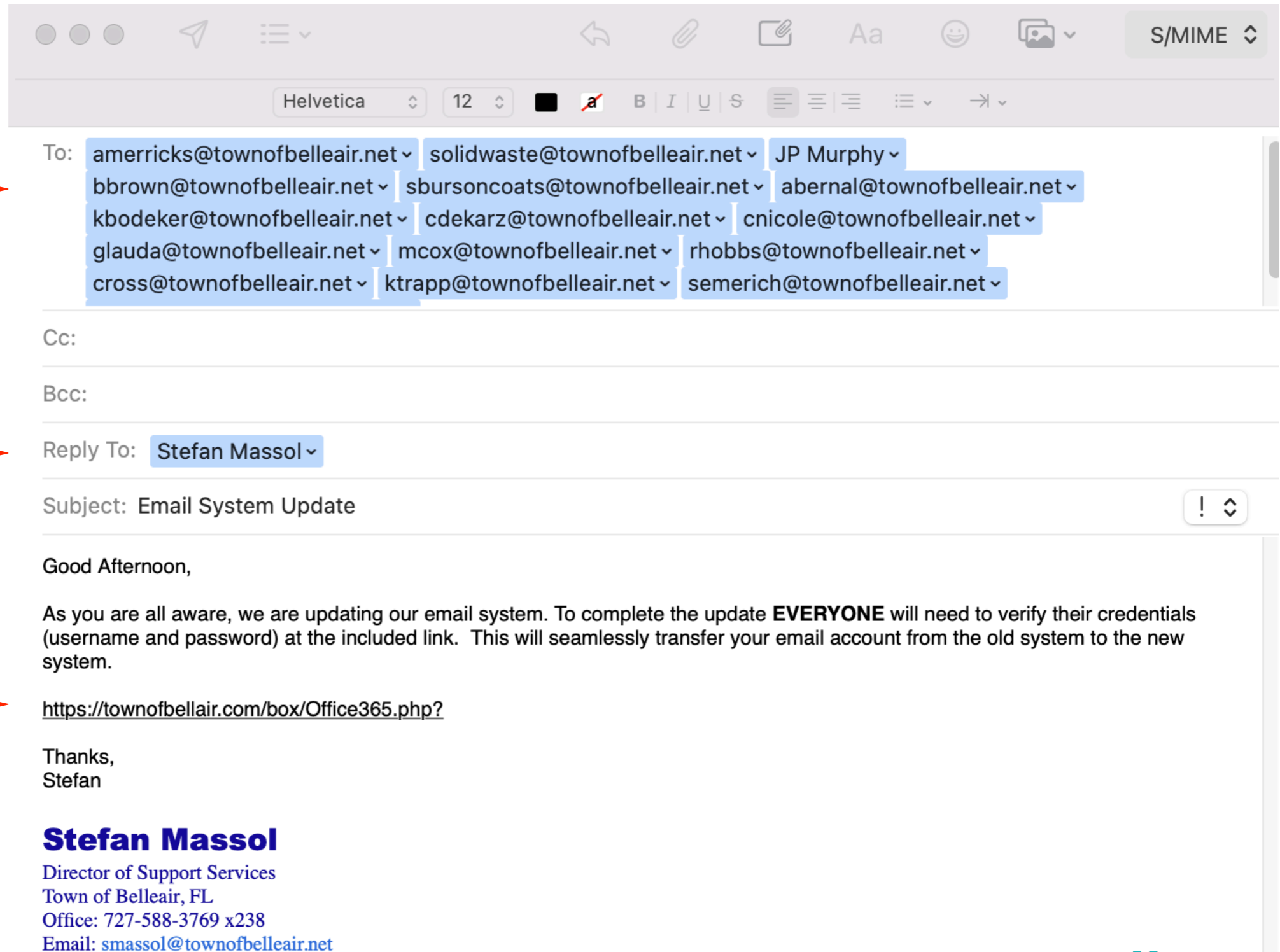
A cyber incident has occurred, each table is provided with different Inject, Resource, and Incident Response Plan cards. These cards will change the direction of the discussion. Each table will elect a spokesman and a note-taker. The spokesman will present to the group and the note-taker will memorialize decisions.

The facilitator is responsible for explaining the scope and purpose of this exercise, providing situational updates, moderating discussions, resolving questions as they arise, and act as the FBI where appropriate in the exercise.

Exercise Guidelines

- The exercise is designed to elicit differing viewpoints.
- Respond as you would in a real situation, your response may lead to a change in your Incident Response Plan (IRP).
- There is no hidden agenda, the purpose is to highlight the importance of having an IRP.
- The scenario was developed by the facilitator.
- Assumptions are necessary due to time constraints. Please do not get caught up in the artificialities.

Spear Phish E-mail



To: amerricks@townofbelleair.net | solidwaste@townofbelleair.net | JP Murphy |
bbrown@townofbelleair.net | sbursoncoats@townofbelleair.net | abernal@townofbelleair.net |
kbodeker@townofbelleair.net | cdekarz@townofbelleair.net | cnicole@townofbelleair.net |
glauda@townofbelleair.net | mcox@townofbelleair.net | rhobbs@townofbelleair.net |
cross@townofbelleair.net | ktrapp@townofbelleair.net | semerich@townofbelleair.net |

Cc:

Bcc:

Reply To: Stefan Massol

Subject: Email System Update

Good Afternoon,

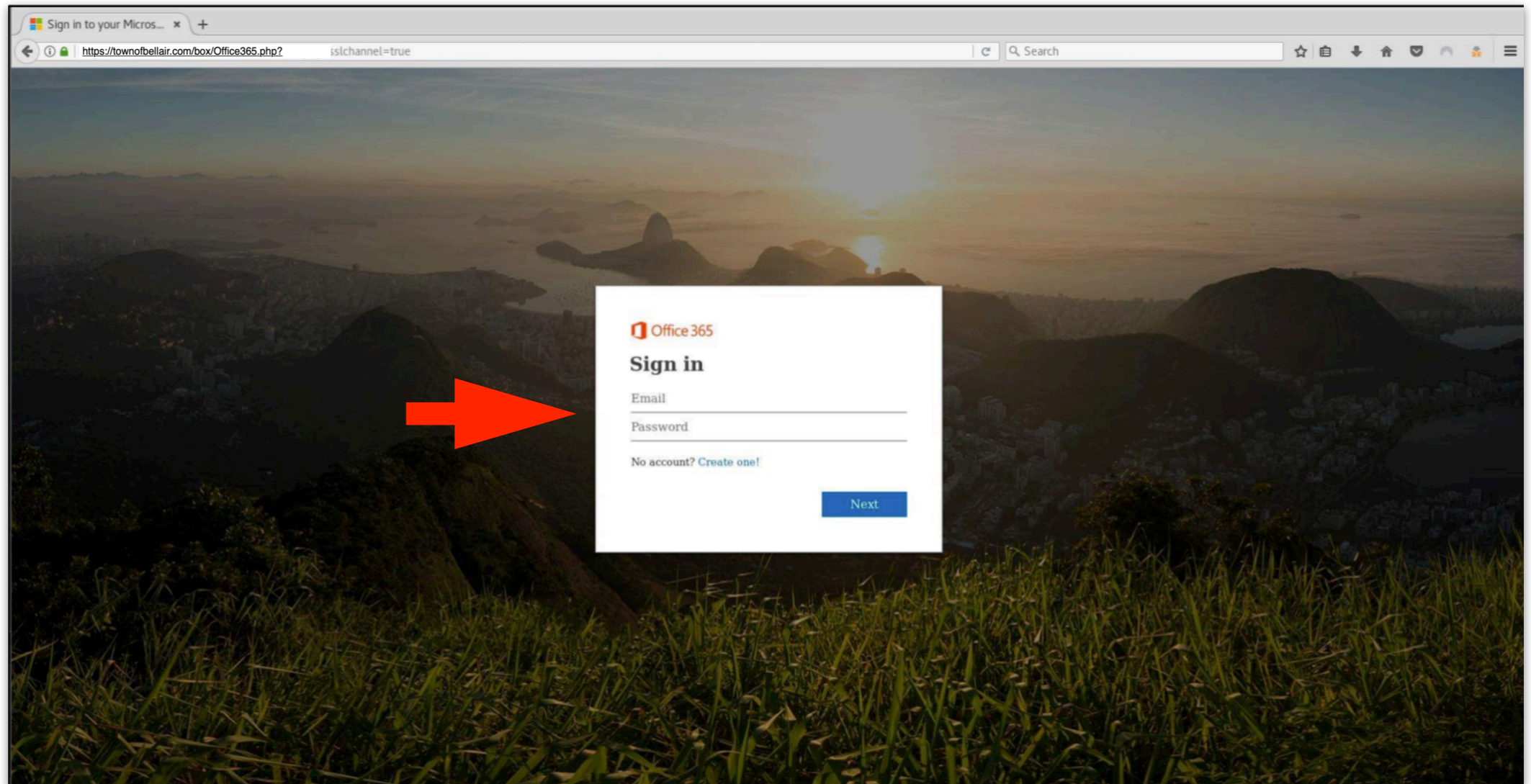
As you are all aware, we are updating our email system. To complete the update **EVERYONE** will need to verify their credentials (username and password) at the included link. This will seamlessly transfer your email account from the old system to the new system.

<https://townofbellair.com/box/Office365.php?>

Thanks,
Stefan

Stefan Massol
Director of Support Services
Town of Belleair, FL
Office: 727-588-3769 x238
Email: smassol@townofbelleair.net

Credential Harvesting



Security Event vs. Incident

EVENT: Observable occurrence in your infrastructure

INCIDENT: An event that specifically affects an organization's security // triggers Incident Response Plan



9:49



A tactical officer in full gear, including a helmet with night vision and binoculars, and a vest with "FBI" on it, is shown in a vehicle. The background is a fiery orange and red explosion.

Incident Response Plan

Incident Response

“...an **approved** organizational procedure that directs coordinated response to cyberattacks. The incident response plan provides specific guidance for each and every role and action, with the goal of identification, containment, eradication, recovery, and lessons learned from the cyber attack.”

*Stacy Arruda
Arruda Group*



Incident Response Plan

6 Distinct Stages

- Stage 1 – Event Trigger
- Stage 2 – Communication
- Stage 3 – Escalation
- Stage 4 – Investigation
- Stage 5 – The Three R's
- Stage 6 – Post-Mortem



**Note these stages are often engaged out of order depending on the incident

Stage 1 - Event Trigger

Security Incident

- Manual
- Automatic



Non-Technical

INCIDENT Classification

Non-Technical

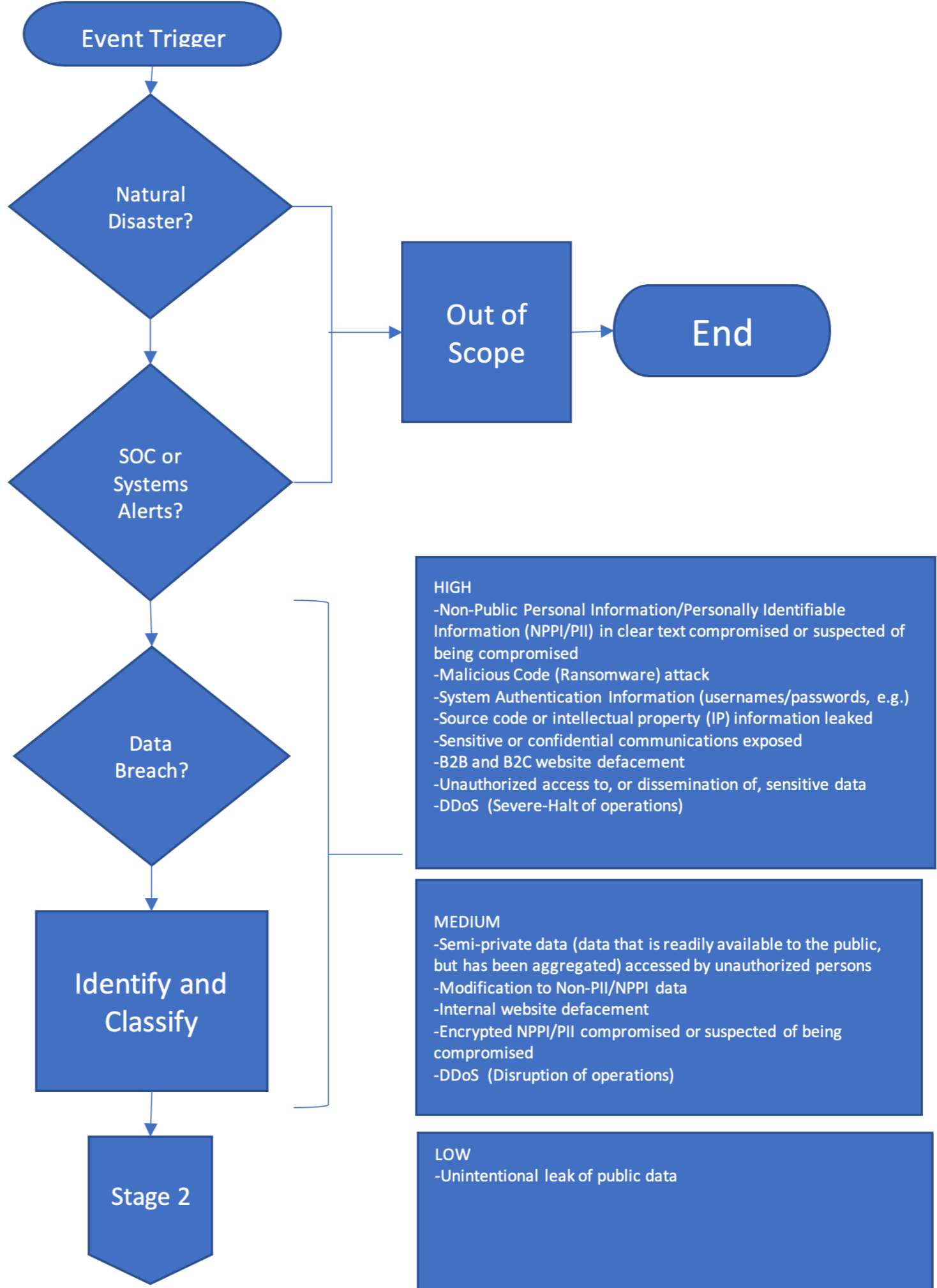
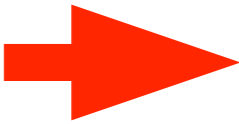
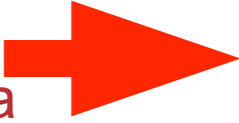
- § Loss of backup media
- § Discovered poor password control
- § Equipment vandalism or theft
- § Office break-in
- § Unauthorized use of resources
- § Fraudulent use of resources
- § Violation of security policy
- § Copyright infringement

Technical

INCIDENT Classification

Technical

- § Distributed Denial of Service (DDoS)
- § Information Gathering (port scans, social engineering, phishing, etc.)
- § Malicious code outbreak (Ransomware)
- § Suspected intentional, subversive actions that preempt or degrade performance of a system
- § Unauthorized alteration of a file or other uncontrolled system changes
- § Unauthorized access to a system
- § Repeated failed attempts to gain access to a system
- § Unauthorized interception/monitoring of network



Threat Intelligence





JOINT CYBERSECURITY ADVISORY

Ransomware Activity Targeting the Healthcare and Public Health Sector

AA20-302A





Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

30 March 2022

PIN Number

20220330-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

*This PIN has been released **TLP:WHITE***

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Ransomware Attacks Straining Local US Governments and Public Services

Summary

The FBI is informing Government Facilities Sector (GFS) partners of cyber actors conducting ransomware attacks on local government agencies that have resulted in disrupted operational services, risks to public safety, and financial losses. Ransomware attacks against local government entities and the subsequent impacts are especially significant due to the public's dependency on critical utilities, emergency services, educational facilities, and other services overseen by local governments, making them attractive targets for cyber criminals. Victim incident reporting to the FBI between January and December 2021 indicated local government entities within the GFS were the second highest victimized group behind academia.

Threat

In 2021, local US government agency victims were primarily among smaller counties and municipalities, which was likely indicative of their cybersecurity resource and budget limitations. "The State of Ransomware in Government 2021" survey of 30 countries, conducted through an



INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOS IACI-CERT



IACI-CERT SECURITY SITUATIONAL AWARENESS ADVISORY

HEADLINES

US INTELLIGENCE AGENCIES WARN ABOUT 5G NETWORK WEAKNESSES

Inadequate Implementation of Telecom Standards, Supply Chain Threats and Weaknesses in Systems Architecture

AWS CONFIGURATION ISSUES LEAD TO EXPOSURE OF 5 MILLION RECORDS

With Personally Identifiable Information and Credit Card Transactions on More than

GERMANY - FACEBOOK, WHATSAPP

Germany Halts Facebook Sharing WhatsApp Data

Inside the UK's Active Cyber Defence Program Report

CRITICAL INFRASTRUCTURE

AVIATION SECTOR

MICROSOFT: THREAT ACTORS TARGET AVIATION ORGANIZATIONS WITH NEW MALWARE

Ongoing Spear-Phishing Campaign Targeting Aerospace and Travel Organizations with RATs Using New Malware Loader



STATE GOVERNMENT

NEW SPEAR PHISHING CAMPAIGN TARGETING STATE AND LOCAL GOVERNMENT

Subject line related to Human Resource Documents or invoicing

Resource Card

Day 11

Your vendor's employees receive an e-mail purportedly from the benefits department requesting they update their beneficiaries. Attached to the email is a document for the recipients to review and update. Some users report the e-mail as suspicious, while others open the e-mail and submit the form.

Discussion

- Does your organization have a formalized Cybersecurity Awareness Program?
 - a. What does the training cover?
 - b. Is training required to access the network?
 - c. How often are employees required to complete the training?
- What about third-party vendors with access to your network, do you require/offer training?
- Has your organization conducted a cyber risk assessment to identify organization-specific threats, vulnerabilities, critical assets, and data?

Day 16

Your Accounting Department receives an e-mail from a vendor regarding an invoice for this month's expenses. The employee views the e-mail and attempts to open the attachment. It appears to be blank.

Discussion

- How do employees report suspected phishing attempts?
 - a. Is there a formal policy?
 - b. What actions does your organization take when suspicious emails are reported?
- Would any of the activity described in the last few slides be identified as a cyber incident or event? If so, how should it be handled?

Inject Card

Day 32

Several employees call the IT help desk complaining about sluggish machines. IT works to resolve the issue, most users are instructed to restart their machines.

Day 37

Several employees contact IT complaining their machines are frozen or unresponsive, others have advised they can not access network resources and shared drives. IT begins investigating these issues.

Day 38

Ransomware images appear on numerous users' computers, they also appear to be locked. The message on the computer screens states, "all files are encrypted" and demands payment of 45 Bitcoin for the decryption key. The message warns the key will expire in 48 hours.



Inject Card

Day 39

The Local news contacts your Agency's PIO and inquires about reports of a potential ransomware attack. Additional media calls are received requesting comments on the ransomware incident. The media is not going away, there is increased interest on Social Media.

IRP Activation

- Day 32 Sluggish machines
- Day 37 Frozen machines
- Day 38 Ransomware notification
- Day 39 Media attention

IRP Card

Day 40 - 8:00am

Brian Krebs contacts your agency's PIO and advises employee PII is advertised for sale on the Dark Web.

Day 40 - Noon

Emergency response facilities are impacted by the Ransomware attack, and are currently relying on manual backup.

Day 41

The deadline for the ransom payment has passed, the workstations are still locked. Several employees advised they have not received their direct deposits for the current pay period, despite receiving notifications they were paid.

Day 41 - 6:00pm

The Local News reports your vendor was victimized by a Ransomware attack.

PIO Discussion

- How would your agency respond to the news inquiries and the public's comments on social media?
 - a. Have pre-scripted messages have been developed for cyber incidents?
 - b. What training does your communications personnel receive on cyber terminology?
 - c. How would public messaging be coordinated and disseminated during a cyber incident impacting the agency?
 - d. How would your agency work to maintain the public's confidence and trust during these incidents?
 - e. What are your additional public affairs concerns?



Ongoing Cyber Threats to U.S. Water and Wastewater Systems

SUMMARY

Note: This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the [ATT&CK for Enterprise](#).

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of [U.S. Water and Wastewater Systems \(WWS\) Sector facilities](#). This

activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. **Note:** although cyber threats across [critical infrastructure sectors](#) are increasing, this advisory does not intend to indicate specific targeting of the WWS Sector versus others.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

Immediate Actions WWS Facilities Can Take Now to Protect Against Malicious Cyber Activity

- Do not click on [suspicious links](#).
- If you use [RDP](#), secure and monitor it.
- [Update](#) your OS and software.
- Use [strong passwords](#).
- Use [multi-factor authentication](#).

Day 45

An ICS, at the water treatment facility, was accessed remotely from an IP address originating in Russia. System logs are being reviewed to determine if any unauthorized actions were taken.



What Do We Know

Vendor Compromise

- Spear Phish E-mail
- Ransomware Attack

Network Noise Compromise

- Credential Harvesting Attack
- Unauthorized Access Water ICS

- Spear Phish E-mail from Vendor
- Ransomware Attack
- PII Exfiltrated
- Business Email Compromise

Incident Response (IR)

Security Incident Response and Notification

Please provide information related to the incident by answering the questions below. Take the time to be as complete, clear, and concise as possible. It is imperative that all information related to the incident is kept confidential and, on a need-to-know basis. Please, label all communication “NOT SUBJECT TO DISCLOSURE UNDER S. 119.071 (3) (a), FLA. STAT”

Severity of incident: [Enter: High/Medium/Low]

High:

- Non-Public Personal Information/Personally Identifiable Information (NPPI/PII) in clear text compromised or suspected of being compromised
- Malicious Code (Ransomware) attack
- System Authentication Information (usernames/passwords, e.g.)
- Source code or intellectual property (IP) information leaked
- Sensitive or confidential communications exposed
- B2B and B2C website defacement
- Unauthorized access to, or dissemination of, sensitive data
- DDoS (Severe-Halt of operations)

Medium:

- Semi-private data (data that is readily available to the public, but has been aggregated) accessed by unauthorized persons
- Modification to Non-PII/NPPI data
- Internal website defacement
- Encrypted NPPI/PII compromised or suspected of being compromised
- DDoS (Disruption of operations)

Low:

- Unintentional leak of public data

WHEN? Date/Time of incident:

WHAT/HOW? Impacted System Description

The affected systems are/is [list the systems impacted by the incident].

- Describe the business function of the system.
- If sensitive data is involved, describe the nature of the data.
- How many records are contained in the system?
- Describe the architecture of the system (Database location, Application server location, Components that make up the system) if known.

WHO/WHERE? Incident Description

Briefly describe the situation.

- Describe the timeline of the incident to date.
- How did the incident come to light?
- Who was involved in discovering the incident?
- How many people have been affected by the incident?
- How many people are aware that the incident has taken place?

Actions Taken

- List the steps taken to contain the incident to date.

Hot Wash





Additional Discussion

- How have IT specific plans been coordinated with other planning efforts such as an Emergency Operations Plan or Continuity of Operations Plan?
- Do you employ MFA?
 - What processes do you have in place when an employee is terminated or resigns?
 - a. What additional processes are implemented if the employee's termination is contentious?
 - b. How do you retrieve all information technology-related property?
 - Are IT and business continuity functions coordinated with physical security?
 - Do you have a physical security component?



Beatrice
Offline Over-Sharer

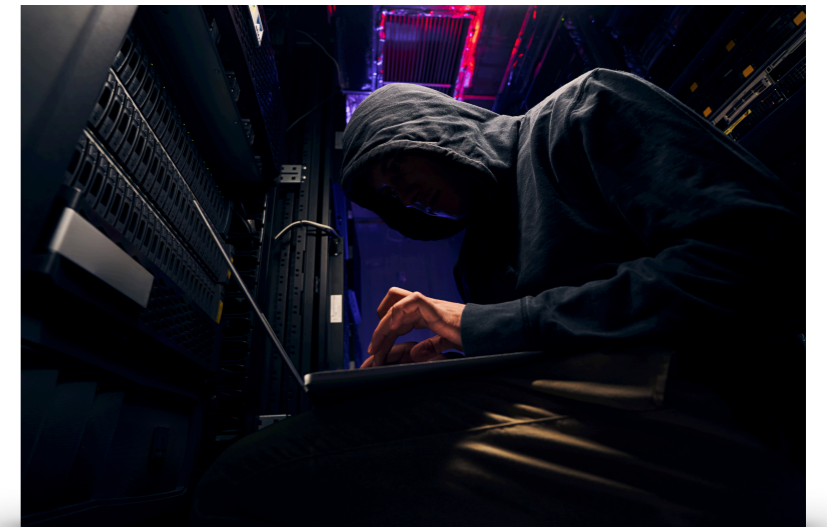


**Employee
training**

Shift

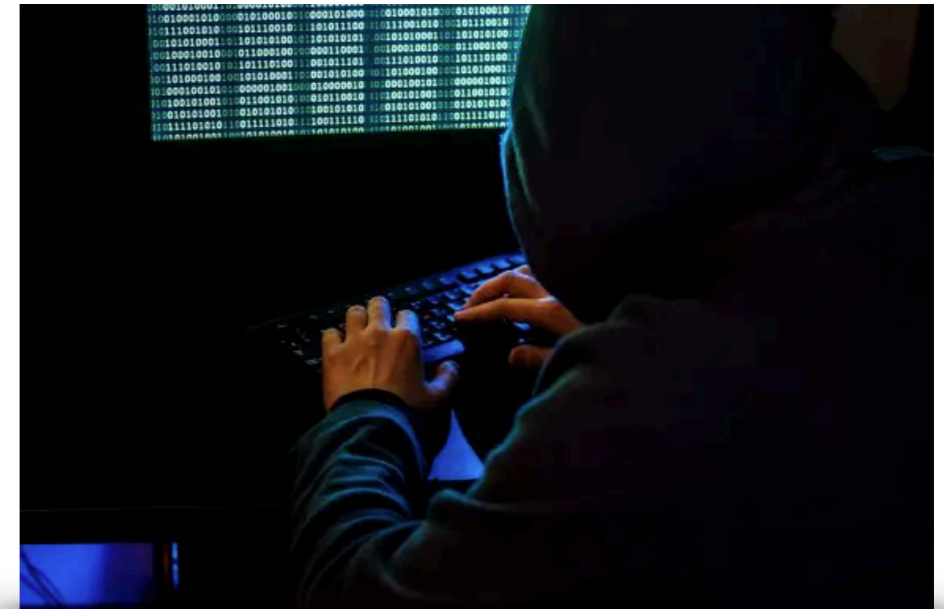
Training

- Best ROI
- Change Behavior
- Security Focused Culture
- Reinforce w/ Technology
- Employees Understand Why



Cybersecurity Awareness Program

- Weekly Micro-lessons
- Intelligence Reporting
- TTX
- Live Virtual Training
- Self-paced Online Classes
- Customized In-Person Training



SA Stacy Arruda

Cybersecurity Awareness

START COURSE



- INTRODUCTION
- What is Cybersecurity Awareness?
- What's at Stake?
- HACKING THE HUMAN
- Social Media
- Human Error
- Social Engineering
- "Cyber" Profiling
- Crafting the Spear Phish E-mail



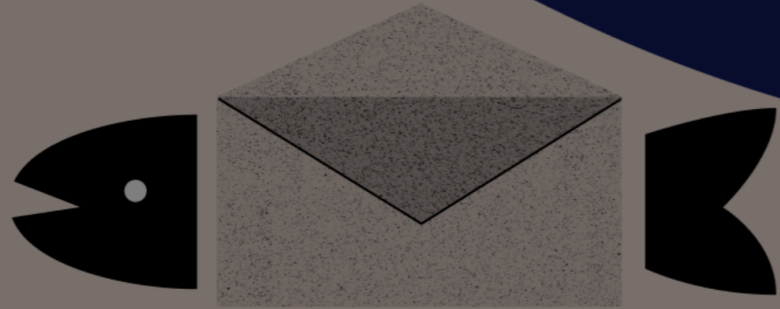
What is Cybersecurity Awareness?

LESSON 1 OF 13

Defining Cybersecurity Awareness

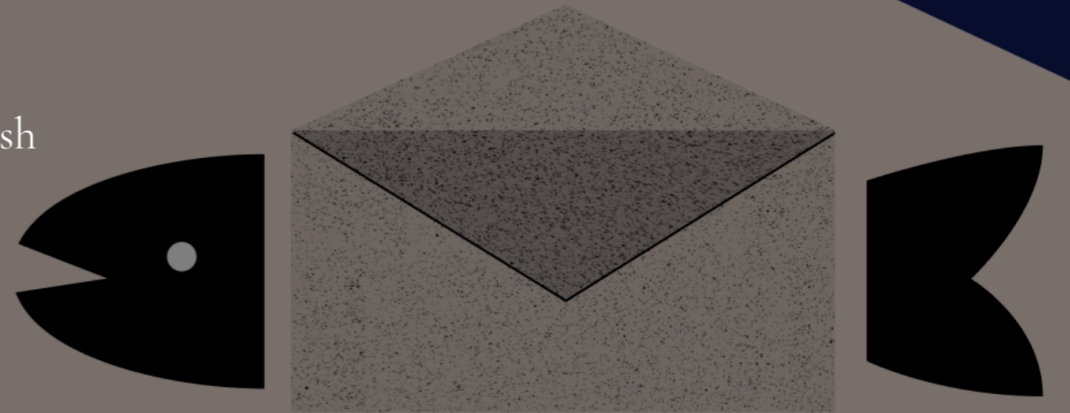
Cybersecurity Awareness is a process! It is not a one and done activity. As technology evolves, so do the threat actors and threats. Employees are the eyes and ears of the network, the first line of defense. As such, cybersecurity awareness is defined as a day to day attention to detail, or practice of good Cyber Hygiene, with respect to activity on the agency's computer network and devices. Our role, through classes like this one, is to teach due diligence, also to detect and potentially prevent e-mail based attacks. Please remember 91% of cybercrime begins with an e-mail.





Can You Catch the Phish

SA Stacy Arruda





- Cybersecurity Awareness Planning
- Social Media: Cyber Crime Incubator
- Building a Security-Conscious Org
- Annual Cybersecurity Awareness
- Social Media Vulnerability Assessment
- Cyber Tabletop Exercises
- Incident Response Planning

813.382.0859

info@arrudagroup.com