



**Georgia Department
of Human Services**

Office of Information Technology

Information Technology Briefing

Cyber Security Training

Venkat R Krishnan, Deputy Commissioner, Information Technology



stronger families

FOR A STRONGER GEORGIA



Agenda

- Security threats are the new normal
- Steps we are taking at DHS: People, Process, Technology
- Mandatory training overview
- Quarterly training statistics for 2021:
 - Q1, January - March
 - Q2, April - June
 - Q3, July - September
- Cyber Dawg 2021 - Advanced Training For DHS Security Team
- Other Initiatives: YubiKey, Azure Information Protection
- Questions?



Security threats are the new normal

- Social engineering attacks, phishing attacks, and ransomware attacks are on the rise
- Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) are combating increased risks of malware, intrusion, and unauthorized data transfer
- COVID-19 highlighted the criticality of having the ability to respond quickly to a business disruption
- Home workspaces typically are more vulnerable to cyber threats
- Importance of cybersecurity training for employees - an organization's first line of defense - is more critical than ever



Steps we are taking at DHS

- **People:**

- Published guidance to the workforce on IT security best practices
- Annual mandatory information security awareness training via Learning Management System
- Quarterly mandatory cybersecurity training via Proofpoint
- Monthly anti-phishing campaigns and remedial training for phishing victims

- **Process:**

- Keeping computers and software updated and patched
- Conducting routine vulnerability scans and hardening security configurations to meet federal guidelines
- Mandating strong security in Data Sharing Agreements (DSAs), DHS websites, and data transfer protocols e.g. use Transport Layer Security (TLS) v1.2+
- Continually updating business continuity (BC) and disaster recovery (DR) plans; developing scenario-response playbooks



Steps we are taking at DHS (Continued)

- **Technology:**

- New PhishAlarm button to report phishing e-mails & suspicious e-mails
- Using BitSight to monitor security best practices of Agency's public-facing websites
- Using Trend-Micro Deep Security tool at NADC and for IES/Gateway to watch for indicators of compromise and block intrusion attempts
- Leveraging McAfee Active Response (MAR) tool across DHS workstations
- Enforcing security hygiene checks on computers connecting to VPN ensure current anti-virus/malware & patches
- Leveraging new GTA/GETS SOC* & SIEM* capabilities and event log correlation

(***SOC** = Security Operation Center; **SIEM** = Security Information & Event Management)



Mandatory Training Overview

- **DHS Proofpoint Security Education Platform**

- DHS/OIT-Security Team administers the platform and provide reports to Agency leadership
- GTA/ATOS have visibility to assist agencies and reports Agency's overall completion statistics to Georgia Cybersecurity Board & Governor's office
- Provides multiple, engaging formats to maximize knowledge transfer & retention: videos, interactive training, quizzes, game play scenarios, etc.
- Example training benefits:
 - Teaches users to exercise good judgment before clicking on hyperlinks in e-mails or downloading or opening e-mail attachments
 - Demonstrates how to avoid social-engineering attacks
 - Emphasizes access controls and provides techniques for strong passwords
 - Provides information on how to report incidents and suspected threats



Mandatory Training Overview (Continued)

- **Annual** mandatory information security awareness training
 - Delivered via DHS Learning Management System training platforms
 - Content is provided by DHS/OIT-Security Team and Office of Employee Development (OED)
- **Quarterly** mandatory cybersecurity training (via Proofpoint)
 - Assignments prescribed by Georgia Cybersecurity Board; assignments typically comprise 4-6 modules spanning ~60-minutes
 - Minimum agency completion threshold of 90% set by GTA and Georgia Cybersecurity Board
- **Monthly** anti-phishing campaigns and remedial training for victims (via Proofpoint)
 - Georgia Cybersecurity Board prescribes campaigns & remedial training assignments
 - Workers who fall victim to a mock phishing e-mail are assigned remedial training automatically



First Quarter (Q1) Cybersecurity Training

January—March 2021

- Quarterly Assignment:
 - Agency achieved **95.36%** completion rate with **9,194** participants
 - Training Modules:
 - e-mail Security on Mobile Devices
 - Attack Spotlight: Fraudulent Shipping Notifications
 - Mitigating Compromised Devices
 - URL Fundamentals
 - A Guide to Incident Reporting
- Anti-Phishing Campaigns:
 - January: **9,491** participants, **1.85%** fell victim, **66.4%** completed remedial training
 - February: **9,485** participants, **0.47%** fell victim, **68.89%** completed remedial training
 - March: **9,471** participants, **6.11%** fell victim, **94.65%** completed remedial training



Second Quarter (Q2) Cybersecurity Training

April—June 2021

- Quarterly Assignment:
 - Agency achieved **94.95%** completion rate with **8,313** participants
 - Training Modules:
 - URL Training
 - PIN and Password Protection
 - The Ransomware Attack
 - An Urgent Request
- Anti-Phishing Campaigns:
 - April: **9,334** participants, **3.3%** fell victim, **68%** completed remedial training
 - May: **9,166** participants, **3%** fell victim, **85.2%** completed remedial training
 - June: **9,335** participants, **5.2%** fell victim, **76.6%** completed remedial training



Third Quarter (Q3) Cybersecurity Training

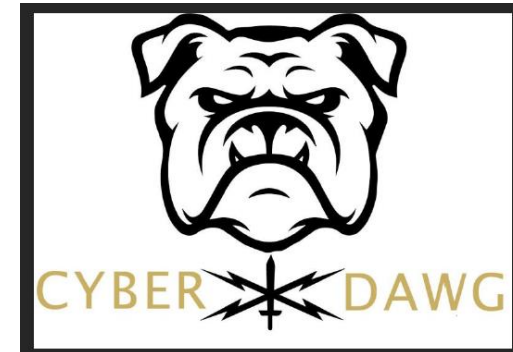
July—September 2021

- Quarterly Assignment:
 - Agency achieved **92.38%** completion rate with **8,725** participants
 - Training Modules:
 - Anti-Phishing Phil
 - Safe Social Networks
 - Physical Security
 - A Step Too Far
 - Fake News
- Anti-Phishing Campaigns:
 - July: **9,183** participants, **19.87%** fell victim, **53.6%** completed remedial training
 - August & September campaigns were suspended by GTA Office of Information Security due to technical problems.



Cyber Dawg 2021

- Cyber Dawg 2021 advanced training simulation for security practitioners
- Conducted 9/12/21 – 9/17/21 at the Georgia Cyber Center in Augusta, Ga
- Comprised cyberattack/defense role-play to simulate IT infrastructure
 - Exercises included cyber and social media attacks
- Participants included:
 - DHS/OIT-Security team
 - Multiple state agencies
 - Two foreign partners (Argentina, Republic of Georgia), and
 - The Georgia National Guard
 - Recent graduates of a training program from Scientific Research Corporation (SRC)
- Participants were involved in all aspects of security operations including incident response, security analysis, policy, configuration management, help desk, media relations, legal, etc.



Other Initiatives:

Yubikey, Azure Information Protection

- YubiKey
 - Multi-Factor Authentication (MFA) is required for DHS O365 and VPN access
 - Complies with State mandate & Federal regulations (IRS 1075, MARS-E, CJIS)
 - 4,323 YubiKeys have been issued; Approximately 45% of DHS workforce now have a YubiKey
 - Agency achieved 100% compliance with State MFA directive via YubiKey/Okta Verify
- Microsoft Azure Information Protection (AIP)
 - AIP will be used to classify & protect documents (confidentiality & access control)
 - E-mail, Teams, OneDrive, SharePoint, Word, Excel, PowerPoint, hard drive, etc.
 - AIP will augment the current DHS O365 e-mail protection levels using Data Classification Taxonomy e.g.
 - Encrypt Only, Do Not Forward, DHS–Agency Confidential, DHS–Agency Confidential View Only
 - Engaging Microsoft to help in implementing AIP in the GETS environment



Questions?

Contact:

Venkat R. Krishnan

Deputy Commissioner & CIO,
Information Technology

Department of Human Services

e-mail: **Venkat.Krishnan@dhs.ga.gov**

Phone: 404-615-2945

Randy C. Coleburn

CISO and Assistant Deputy Commissioner,
Information Security & Compliance Technology

Department of Human Services

e-mail: **Randy.Coleburn@dhs.ga.gov**

Phone: 470-259-5301

Shirlan C. Johnson

Deputy CISO and Senior Information Security
Assurance and Compliance Manager

Department of Human Services

e-mail: **Shirlan.Johnson@dhs.ga.gov**

Phone: 404-655-8371

