DEPARTMENT
of REVENUE

DEMYSTIFYING CYBERSECURITY

Ananias Williams III
Chief Information Officer
5/22/2024

AGENDA

- Why cybersecurity is a growing challenge
  - Cyber Threats
- How you can minimize cybersecurity risk
  - Cybersecurity Awareness Training
  - Cybersecurity & Infrastructure Security Agency (CISA)
- Case Study

A GROWING CHALLENGE

Cybersecurity is a growing challenge due to emerging technologies and threats, which continue to evolve.

- Threat actors using AI
- Nation states conducting cyber activities
- Cyber activities related to global conflicts
- Technology advancements in malware
- Remote workforce

CYBER THREATS

- **Phishing** - use of convincing emails or other messages to trick users into opening harmful links, downloading malicious software or providing sensitive information (ex. login credentials, financial information, personal details).
- **Malware** - a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Email is the most common path for malware.
- **Ransomware** - a type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access.

https://www.nist.gov/itl/smallbusinesscyber/guidance-topic

CYBERSECURITY AWARENESS TRAINING

A process that educates employees about cybersecurity, IT best practices, and regulatory compliance.

- **Purpose** - educates employees on how to avoid phishing, social engineering cyberattacks, recognize potential malware behaviors, report possible security threats, adhere to company IT policies and applicable data privacy and compliance regulations.

https://staysafeonline.org/programs/cybersecurity-awareness-month/

CISA - STAYING SAFE ONLINE

Use basic cyber hygiene practices to make smart decisions whether on the job or at home. The below are encouraged by CISA's Cybersecurity Awareness Month campaign, which is to have individuals implement four action steps to increase online security.

- **Recognize and report phishing** - if a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update software** - if you see a software update notification, act promptly. Turn on automatic updates when possible.
- **Strong passwords** - use passwords that are long, unique, and randomly generated.
- **Turn on Multi-Factor Authentication (MFA)** - enabling MFA makes it significantly less likely to get hacked.

CISA - CYBER AT HOME

Cyber threats can disrupt essential services and potentially impact public safety. Organizations face significant financial loss when a cyberattack occurs. Cybercriminals often rely on human error (ex. failing to install software patches or clicking on malicious links to gain access to systems).

- **Use only approved tools** - use approved software and tools for business, including approved video conferencing and collaboration tools to initiate and schedule meetings. Unapproved free tools may make your system vulnerable.
- **Secure your meetings** - take precautions to ensure your virtual meetings are only attended by intended individuals.
- **Secure your information** - tailor your security precautions appropriately to the sensitivity of data. Only share data necessary to accomplish the goals of the meeting.
- **Secure yourself** - take precautions to avoid unintentionally revealing business and personal information. Ensure home networks are secured.

CISA - CYBER BASICS

- **Treat business information as personal information** - business information typically includes a mix of personal and proprietary data. Do not share personally identifiable information (PII) with unknown parties or over unsecured networks.
- **Don’t make passwords easy to guess** - as “smart” or data-driven technology evolves, it is important to remember that security measures only work if employees use them correctly. Smart technology runs on data, meaning devices such as smartphones, laptops, wireless printers, and other devices. Take proper security precautions and ensure devices are correctly configured to prevent data breaches.
- **Stay up to date** - keep software updated to the latest version available as per guidelines; turn on automatic updates and set your security software to run regular scans.

QUESTIONS?

Ananias Williams III
Chief Information Officer

1800 Century Blvd. NE, Atlanta GA 30345
Ananias.WilliamsIII@dor.ga.gov