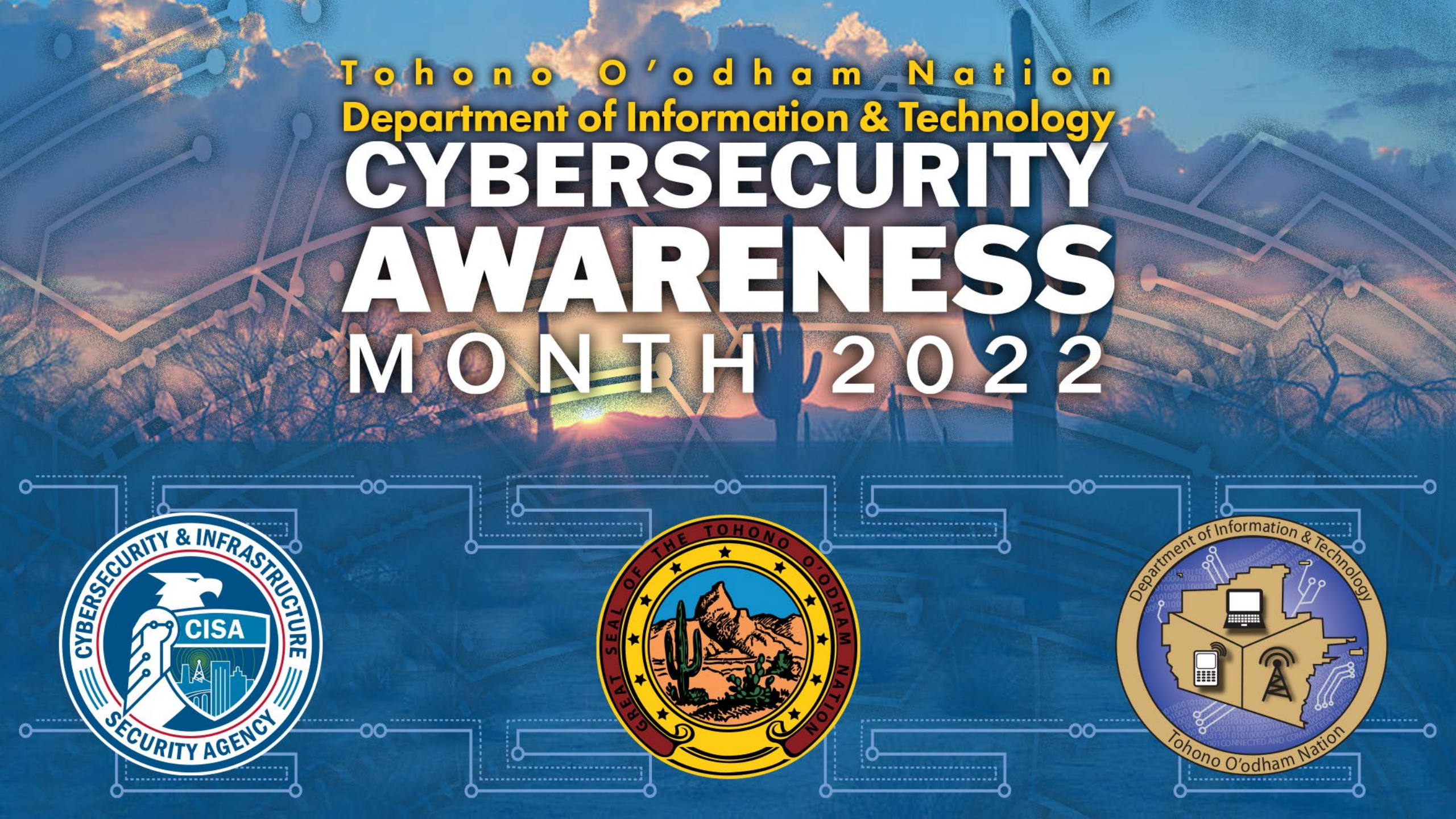
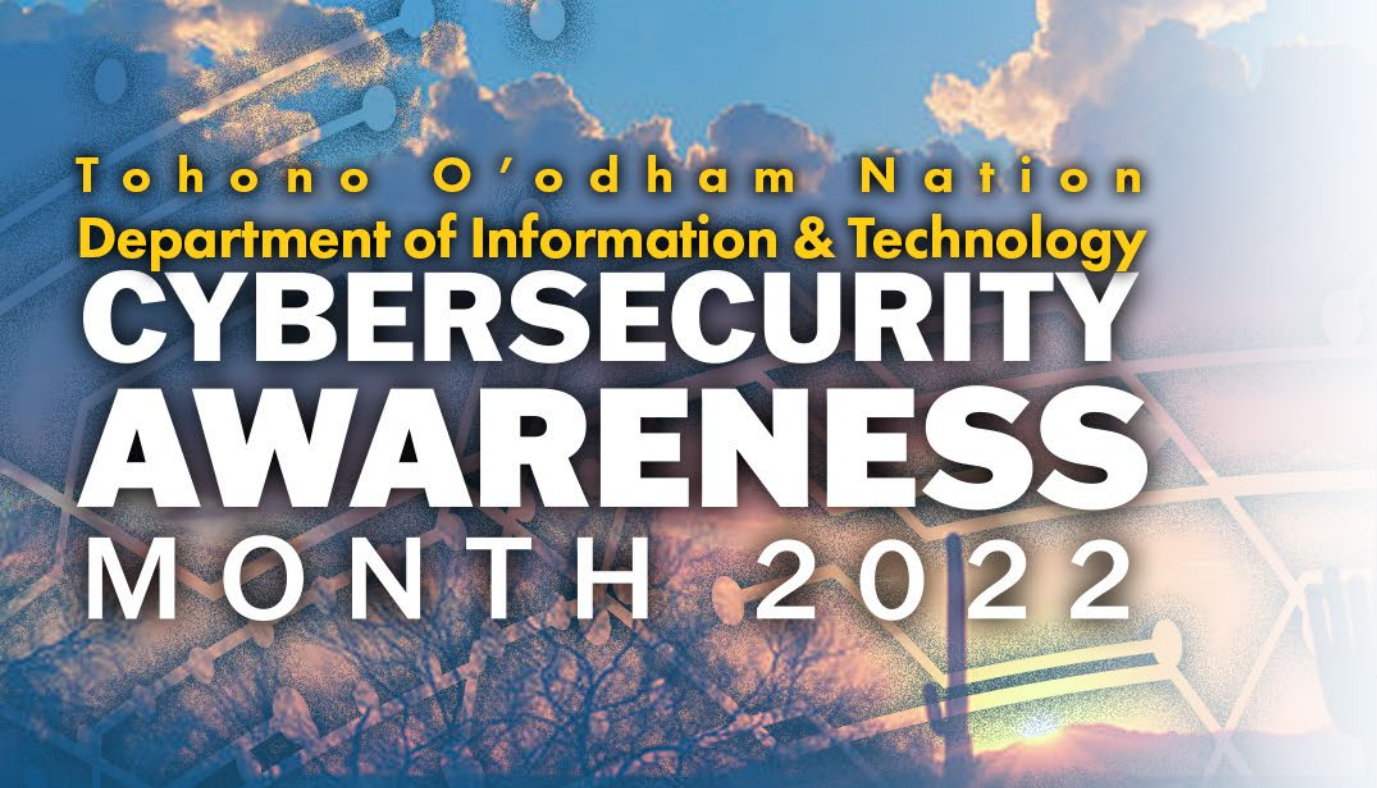

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY
AWARENESS
MONTH 2022
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
GREAT SEAL OF THE TOHONO O'ODHAM NATION
Department of Information & Technology
Tohono O'odham Nation



Overview

- **Four weeks of bite size portions pertaining to cybersecurity**
- **Week 1** is an overview of cybersecurity and what it entails
- **Week 2** will cover passwords
- **Week 3** will cover patching
- **Week 4** will cover phishing and other attacks on end users
- **There will be an overall presentation in November with a Q & A**

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

What is Cybersecurity

- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.
- In today's world, technology is reliant on the internet
- The workforce and personal use is becoming more reliant on the internet being available.
- While remaining available it is important to ensure that data maintains it's integrity and confidentiality

Why is cybersecurity important

- As the world becomes more "online", sensitive data is being sent across the world wide web
- Personal information, credit card information, HIPAA data can be stolen if not protected.
- The initial entry point for a ransomware attack (ingress) often takes the form of a compromised website delivered through a phishing or targeted attack.
- By clicking a link in an email, visiting a malicious site, or being social engineered, all it takes is for one person to fall for the malware and an entire organization can be compromised

Why is cybersecurity important (cont)

- Remote desktop protocol, bring-your-own-PC, and virtual private network vulnerabilities and misconfiguration are becoming the most common entry points for ransomware attackers.
- The pandemic led to more remote work which only increased the attacks of ransomware and other types of malware
- As most incidents start from end-user, it is important to educate everyone on how to protect themselves
- While there is no guarantee, that you won't become a victim, you can learn how to protect yourself from most types of attacks

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Ask yourself these questions

- How much of your daily life relies on technology?
- How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?
- Have you been a victim of malware?
- What are you doing to protect yourself?

Types of common attacks

- Ransomware- This type of attack deals with encrypting an individuals or companies data and demanding payment to release it
  - Usually request payment in bitcoin to not be traced
  - There are 'good' and 'bad' players who might or might not release data after payment
  - $155,000 average payment
- Data breaches- This type of attack deals with the stealing of data either to the individual or a company.
  - 90 percent of these attacks start from a phishing email.
  - User gives up password to threat which then uses to infiltrate the system
  - These types of attacks can take months to detect, by then it is too late
  - Often times ransomware attack is used to cover up a data breach
- Insider threats- employees, contractors, guests who have direct access to the network
  - Stealing of data

Who has been affected by cybersecurity incidents?

- According to a study by security firm Sophos,[3] 51 percent of all surveyed businesses were hit by ransomware in 2020, though the number of cases dropped to 37 percent in 2021.[9] This number varies with the size of the company, with larger companies being more at risk.
- Millions of users across many different platforms
  - Facebook and other social media platforms
  - Phishing attempts
    - IRS
    - Bank apps
    - Usually threatening of money
  - Even streaming apps have been hacked
  - Most likely caused from poor password policy

Well known and costly incidents

- TJ Max- data breach
  - Personal data of over 45 million customers
  - Caused by shady IT employees
  - Bad practices
- Target- data breach
  - 45 million customers affected
  - Caused by HVAC system poorly patched
- Colonial Pipeline- ransomware attack and data breach
  - Caused entire pipeline to be shut down affecting millions
  - Hackers stole data and then placed ransomware attack on systems
  - 'good' threat because they released the encryption keys when paid
  - Caused by faulty VPN password

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Why would they want to attack us?

- Other tribes, hospitals and Casinos have been victims of malware attacks resulting in millions of dollars in recovery costs
- What type of data can we have in our systems:
  - Enrollment data
  - Accounting information
  - Bank information
  - Every department stores some type of data in our systems
  - Do you know what type of information your department stores?

How is DoIT protecting the data?

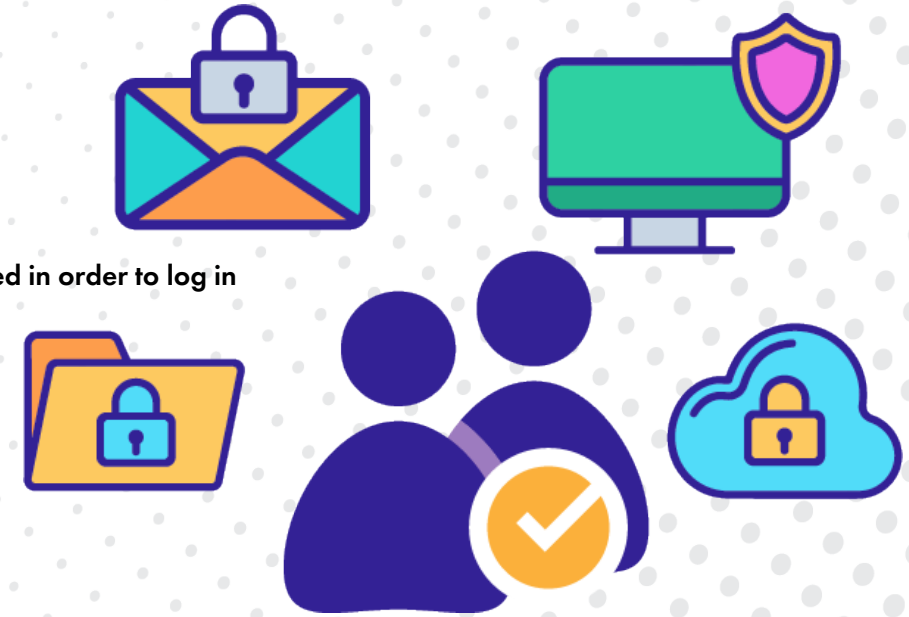
- Currently in place:
  - For email:
    - Email web appliance: that scans email for malicious content and filters spam based on score
    - Email archiver: that archives all email coming into the system, in case of loss of email data
  - Advanced firewall:
    - Besides controlling basic ports, there is an application aspect that allows us to restrict malicious software such as bots and malicious sites
    - Other features that allow us to monitor attacks and react to instances
  - Password policies
    - Requiring passwords to be set every 60 days
    - Locking out of account after a few wrong attempts- brute force attacks
    - Education on not sharing passwords
  - Least privilege concept-
    - Restricting access to only who needs access to documents
    - Restricting permissions of user accounts to only what they should be able to do
    - Reviewing of permissions necessary and cleaning out old accounts

Protecting continued

- Patching- the updating of machines
  - Windows update servers are automatically set to download and apply to user machines on a weekly basis
  - Working on making sure other applications are patched
    - Adobe
    - Chrome
- Backup important data
  - Important to identify where the important data is located
  - File servers, email, sql servers are backed up

Current and future plans

- Microsoft 365 implementation
  - Greatly enhances our security stance
    - Allows us to protect machines inside and outside of the network
    - Allows access to many more consoles from a security standpoint
  - Allows us to set up Multi-factor Authentication
    - Rather than the common password and user name, another type of authentication is needed in order to log in
    - As computing speed increases- username and password is not enough
  - Allows the nation to be able to share information amongst each other from anywhere
    - With that said, security posture needs to be strengthened
    - Ability to monitor data that is being shared
- Scanning software
  - To allow us to ensure all machines are properly patched
  - Gives us a baseline of where we stand from a security standpoint
- Cybersecurity awareness software
  - Allows us to perform email campaigns in order to educate users that need training
  - Also provides Doit to see how our procedures stand up to incidents



Future plans

- Off-site or offline backups
- Implementing MFA
- M365 implementation
- Stronger password requirements
- Instrusion detection and prevention

Current and future

- We are working on updating our current procedures to better adapt to cybersecurity incidents
  - Such as notifications and how we deal with incident
- Strengthening our posture in order to obtain cybersecurity insurance as it is becoming a necessity
- Continue to provide training and remediation to end users
  - Not just yearly but shooting for monthly
- It is not "if" but more so of when we will get attacked.

Upcoming presentation and datasheets

- Password-
  - Password best practices
  - Password keepers
  - Passphrases vs standard passwords
  - MFA
  - DoITs policies