

# SECURING THE MODERN WORKSPACE: MOBILE DEVICE CYBERSECURITY AND REMOTE ACCESS MANAGEMENT



# About CyberHawaii

**CyberHawaii** is an information sharing and analysis non-profit organization committed to developing and enhancing Hawaii's cybersecurity capabilities.

- CyberHawaii is committed to a whole community approach that will help to:
  - Mitigate cyber risks for all community members
  - Develop educational and workforce pathways for students
  - Augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations
  - Inform local decision makers about cyber security risks and solutions
- Founded 2016
- Part of CyberUSA network
- Supported by corporate memberships and grants



# CyberHawaii Members



# About CISA

Our **mission** is to lead the national effort to understand, manage, and reduce risk to our nation's cyber and physical infrastructure.

Our **vision** is a secure and resilient critical infrastructure for the American people.



# Administrative

- Enter questions into chat box
- Presentation being recorded & will be posted by CyberHawaii on their website
- The presenters have agreed that you can contact them after their presentations if you have questions or would like more information
- Please remain on mute during the presentation until designated Q&A sessions



# Presenters



**Al Ogata**

President & CEO  
CyberHawaii

[Al.Ogata@cyberhawaii.org](mailto:Al.Ogata@cyberhawaii.org)



**Jennilyn LaBrunda**

Cybersecurity Advisor  
Cybersecurity & Infrastructure Security Agency

[Jennilyn.Labrunda@cisa.dhs.gov](mailto:Jennilyn.Labrunda@cisa.dhs.gov)



# Agenda

- Mobile device security
- Remote Access Management
- Q & A



# Importance of Mobile Device Cybersecurity

- Keeping Devices Updated
- Strong Authentication
- App Security
- Network Security
- Device Protection
- Vigilance Against Phishing



# Keeping Your Mobile Device Up to Date

- **Update device Operating System (OS)**

- Security Patches and Bug Fixes
- Enhanced Security Features
- Privacy Protections

- **Update mobile Apps**

- Security Enhancements
- New Features and Improved Functionality

- **The Case for Automatic Updates**

- Continuous Protection



# Strengthen Mobile Device Authentication

- Enable Device Authentication
- Enable Two-Factor Authentication (2FA)
- The Importance of Strong, Unique Passwords Combined with 2FA



Something You Have

Like an authentication application or a confirmation text on your phone



Something You Know

Like a PIN number or a password



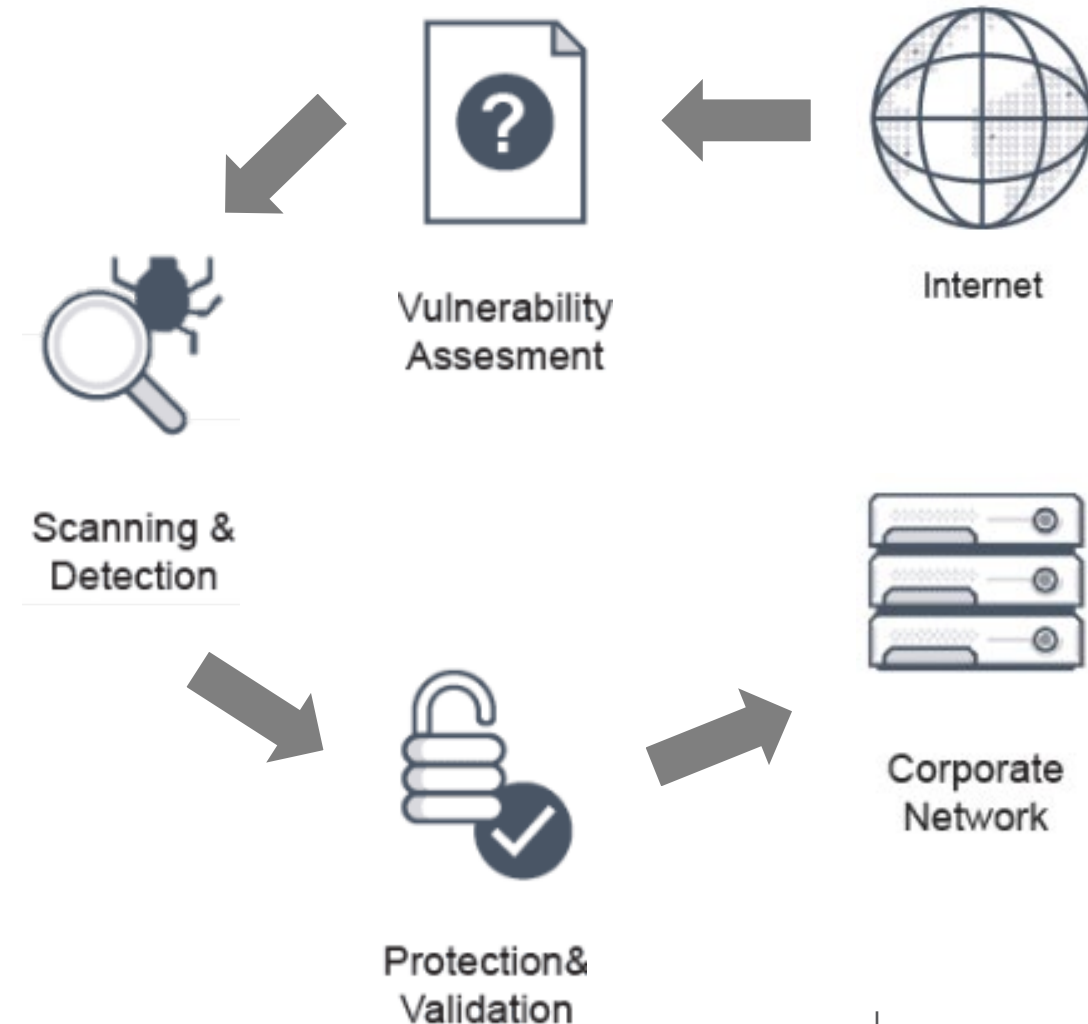
Something You Are

Like a fingerprint or face scan



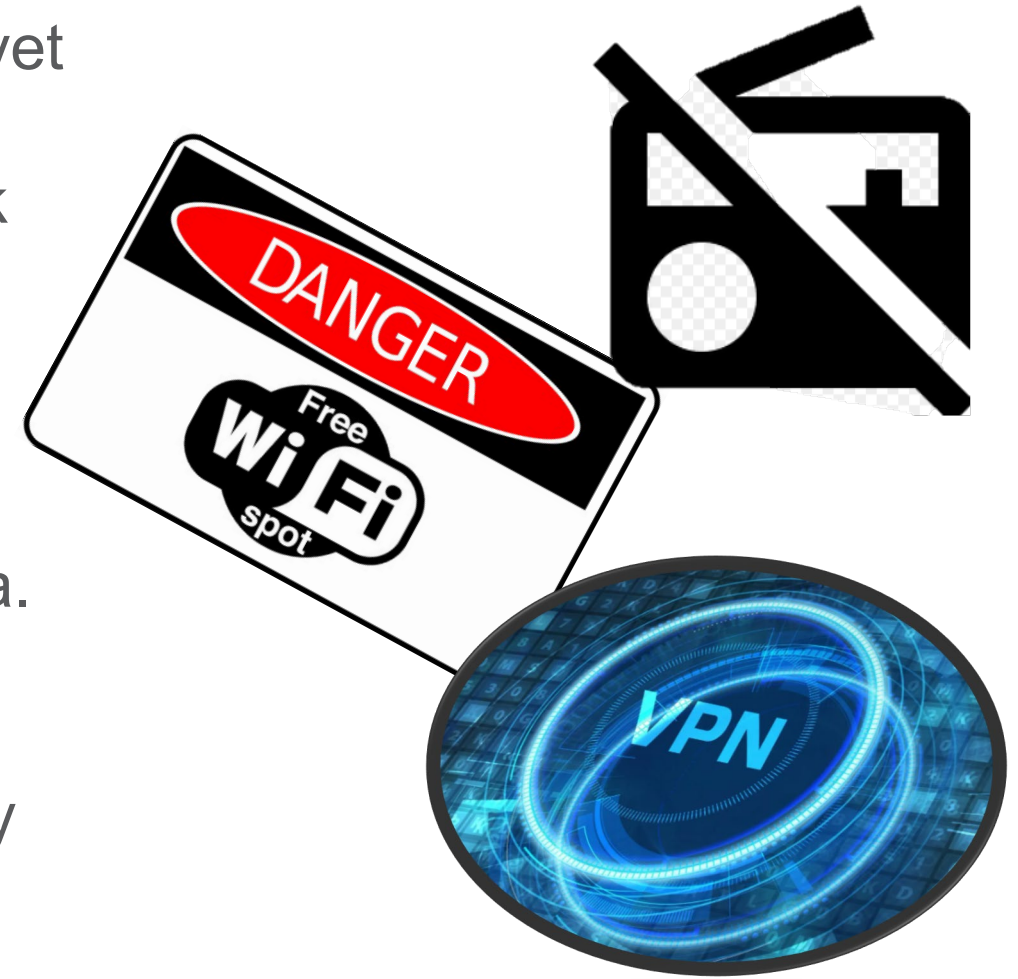
# Best Practices for Mobile App Security

- ❑ Use Curated App Stores
- ❑ Delete Unneeded Apps
- ❑ Minimize PII in All Apps
- ❑ Grant Least-Privilege Access
- ❑ Review Location Settings



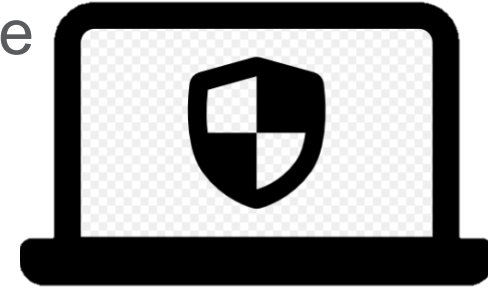
# Securing Mobile Network Communications

- **Reduce Attack Surfaces:** One of the simplest yet most effective ways to enhance your mobile device's security is to disable unneeded network radios.
- **Avoid Public Wi-Fi:** Public Wi-Fi networks are often unencrypted, meaning that anyone on the same network can potentially intercept your data.
- **Solutions:** Consider using your mobile data, which is generally more secure. If you absolutely must use a public network, protect yourself by using a Virtual Private Network (VPN).



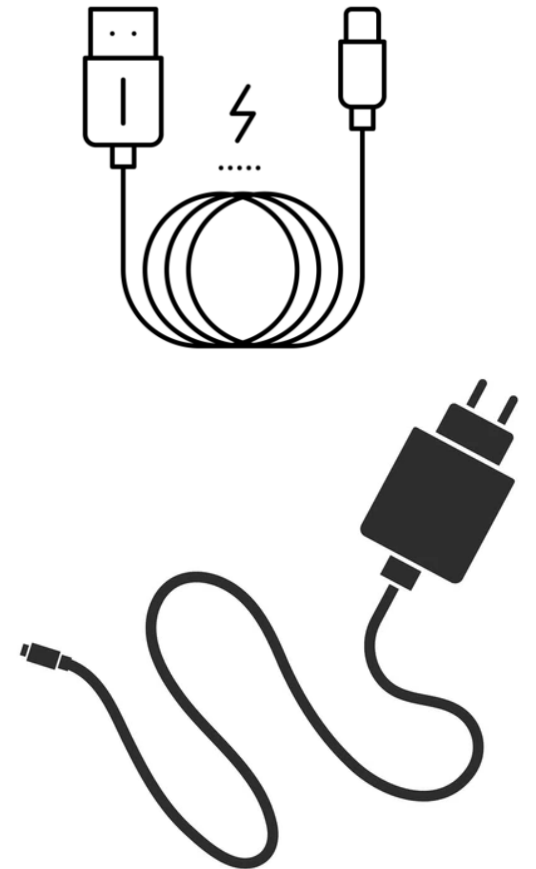
# Safeguarding Your Mobile Device

- **Mobile Threat Defense:** One of the first lines of defense for your mobile device is installing reputable security software.
- **Risks of Untrusted Equipment:** We all know the frustration of a low battery, but in the rush to charge our devices, it's important to be cautious about the equipment we use.
- **Protecting Data in Case of Loss:** Mobile devices are small, portable, and unfortunately, easy to lose. That's why it's crucial to prepare for the worst-case scenario—losing your device.



# Use Trusted Chargers and Cables

- **Use Only Trusted Chargers and Cables:** Ensure you use chargers and cables from reputable manufacturers. Avoid using public or unverified charging stations.
- **Malware Risks:**
  - Malicious chargers or cables can install malware on your smartphone.
  - This malware can bypass your phone's security features, potentially taking full control of the device.
- **Broader Impact:** An infected smartphone can spread malware to other systems which can lead to data breaches, loss of sensitive information, or broader security compromises.



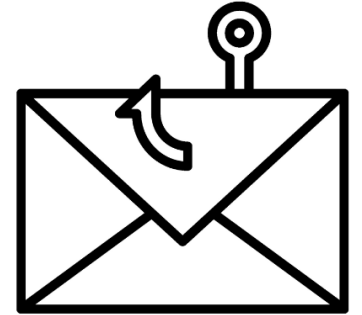
# Turn Your Device Off & On Weekly

- **Key Point: Turn Your Device Off & On Weekly**
  - Regularly rebooting your device can help protect against certain types of cyber threats.
- **Why It Matters:**
  - To prevent Spearphishing and Malware Installation
  - Rebooting can disrupt ongoing or potential spear phishing attacks aimed at installing malware.
- **Mitigate Zero-Click Exploits:**
  - Some zero-click exploits, which don't require user interaction to compromise your device, may be neutralized by a simple reboot.



# Phishing Protection on Mobile Devices

- **Phishing on Mobile Devices:** Cybercriminals know that we're all on our phones constantly.
- **Malicious Emails and Text Messages:** One common technique involves sending emails or text messages that appear to be from a trusted source.
- **Pause Before You Click:** Legitimate companies won't ask you to confirm sensitive information like passwords or credit card numbers through email or text.
- **When in Doubt, Don't Click:** Cybercriminals rely on quick reactions—they want you to act before you think.



# Introduction to Remote Access Management

- Definition of Remote Access Management (RAM)
- Importance in the context of increased remote work
- Importance of RAM in cybersecurity



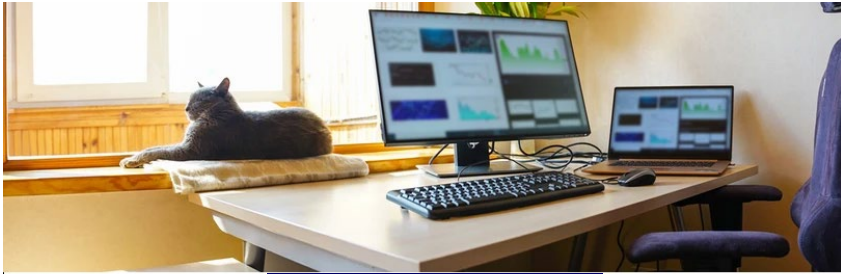
# Definition

- Access to an organizational information system by a **user** (or an information system) communicating through an **external**, non-organization-controlled network (e.g., the Internet)
- Access to an organizational system by a **user** (or a **process** acting on behalf of a user) communicating through an **external** network (e.g., the internet). Remote access methods include **dial-up**, **broadband**, and wireless
- Access by **users** (or **information systems**) communicating **external** to an information system **security perimeter**. Network access is any access across a network connection **in lieu of local access** (i.e., user being physically present at the device)

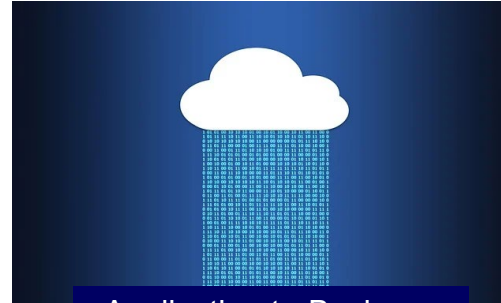


[https://csrc.nist.gov/glossary/term/remote\\_access](https://csrc.nist.gov/glossary/term/remote_access)

# Typical Scenarios



Work from Home



Application-to-Business



Mobile Work



Business-to-Business



Technical Support



Mobile/BYOD



Image Source: Shutterstock & PixelBay

# Controls in RAM

- **Identity & Access Management (Who has access to What)**
  - Authentication
  - Authorization
  - Access Control
- **Data Transmission (Securing data in motion)**
  - Encryption
  - VPN (Virtual Private Network)
- **Networking (Securing the Perimeter)**
  - Network management
  - Monitoring and Logging
- **End Point security (Securing devices outside of firewall)**
  - Monitoring
  - Physical Security
  - Situational Awareness
- **Zero Trust Model**



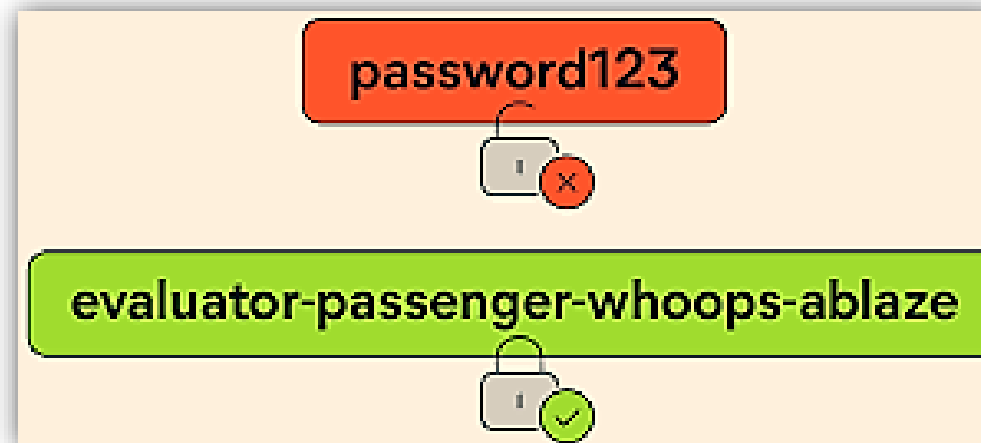
# Access Control

- **Definition:** Managing who can access resources, when, and from where
  - Policy
  - Minimum Necessary
  - Role based access
- **Access is not Trust**



# Authentication

- Definition: Verifying user identity
- Methods:
  - Passwords and passphrases
  - Multi-Factor Authentication (MFA)
  - Biometrics
  - Out of band



# What Else Should I Know About MFA?

## Multifactor Authentication (MFA) Hierarchy



### SMS or Voice MFA

- Text Messages (SMS)
- Voice Message



### App-Based MFA

- Mobile Push Notification Without Number Matching
- One-time Password (OTP)
- Mobile Push Notification With Number Matching
- Token-based OTP



### Phishing-Resistant MFA

- FIDO
- Public Key Infrastructure (PKI)-Based



# Phishing Resistant MFA (FIDO)

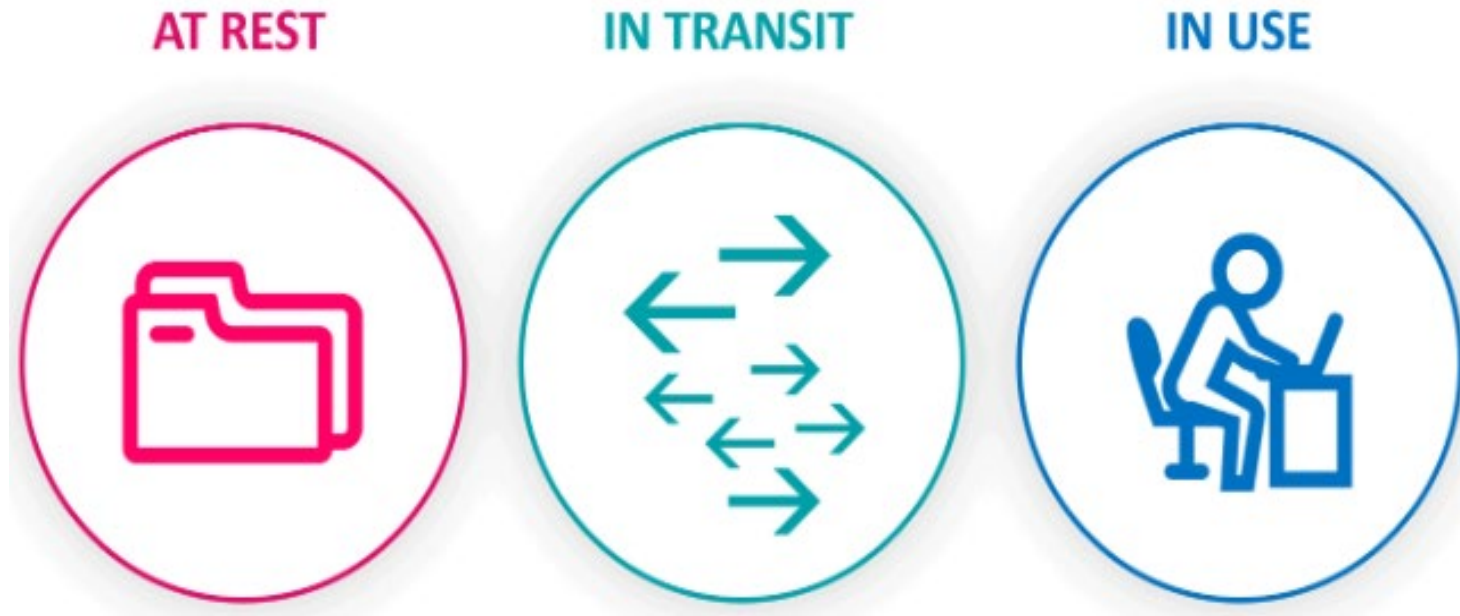
- Questions to ask
  - What resources do I want to protect from compromise?
  - Which users are high-value targets?



# Encryption

- Confidential & Proprietary information should be encrypted in transit & at rest
  - Always encrypt passwords
- Types of Encryption:
  - In transit
    - SSL/TLS
    - End-to-End Encryption
  - At rest
    - Hardware
    - Software
  - In use
    - File level encryption
    - File locking

## THE THREE STATES OF DATA



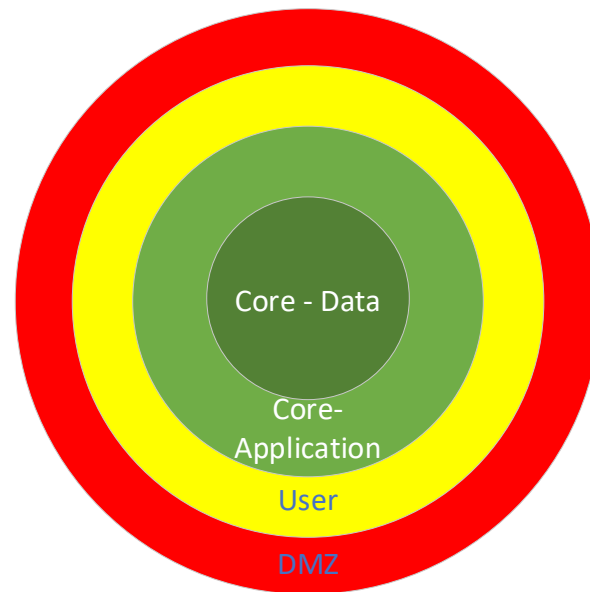
# VPN (Virtual Private Network)

- Secure connection method for remote users
- Benefits of Using a VPN:
  - Encrypts data in transit
  - Masks user location
- Best Practices for VPN Configuration



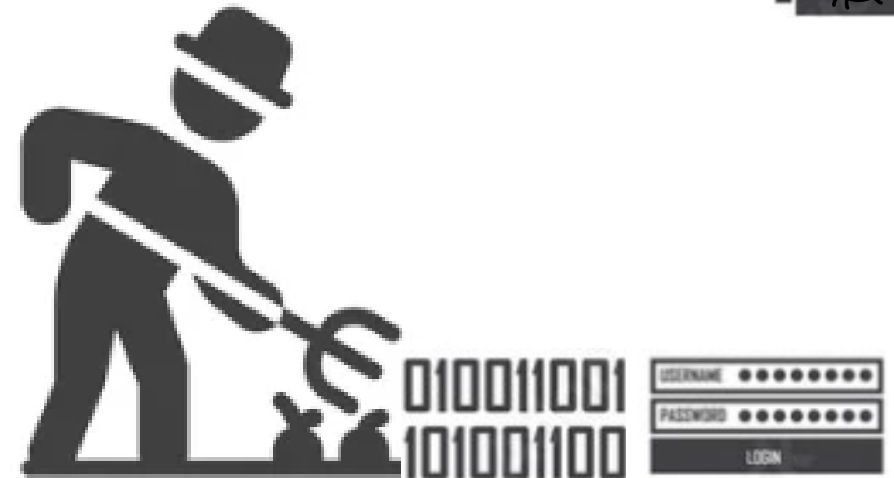
# Network Management

- Router/firewall configuration
  - Secure firewall
  - Designate firewall zones & IP addresses
  - Configure access control list
  - Setup other firewall functions if desired (i.e., DHCP, NTP, IPS)
- Zone Architecture
  - Core
    - Application
    - Data
  - User
  - DMZ



# Monitoring and Logging

- Monitoring user activities
- Tools and Techniques:
  - Logging
  - Auditing
- Role in Incident Response



\*\*\*Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), CISA, FBI, NSA, and international partners are releasing Best Practices for Event Logging and Threat Detection\*\*\*



^^Mitigate Living Off The Land (LOTL) attacks^^

# End Point Security (Physical)

- Remote devices (such as laptops) can be in unsecured environments
- Policy to manage end points
- Security
  - Operate in physically secured environment
  - Secure devices when not in possession – do not leave in car, even if locked
  - Screen lock & session time out
  - Do not load unauthorized software
- Data Privacy
  - Situational awareness – visual, verbal
- Continuity
  - Environmental hazards



# Zero Trust Model

- Overview of the Zero Trust Security Framework
- Key Principles:
  - Never trust, always verify
  - Continuous monitoring and validation
- Benefits in RAM



# Conclusion

## Key Takeaways

- **Implement Strong Security Measures:** Use robust authentication, encryption, and access control methods to protect sensitive data.
- **Adopt a Zero Trust Model:** Ensure no user or device is trusted by default, and continuously monitor and refine your security practices.
- **Stay Vigilant and Informed:** Regularly update software, be aware of phishing threats, and create a culture of continuous security improvement.

## Call to Action

- **Enhance Your Cybersecurity Posture:** Take immediate steps to implement the strategies discussed today.
- **Encourage a Culture of Security:** Promote awareness and vigilance within your organization.





For more information:

[www.cisa.gov](http://www.cisa.gov)

**Questions?**

Email: [\*\*jennilyn.labrunda@cisa.dhs.gov\*\*](mailto:jennilyn.labrunda@cisa.dhs.gov)

Phone: **808-260-3143**

Email: [\*\*al.ogata@cyberhawaii.org\*\*](mailto:al.ogata@cyberhawaii.org)

Phone: **808-778-4725**

