CYBER SECURITY TIPS AND TOOLS
MOBILE SECURITY

Frosty Walker
Chief Information Security Officer
Texas Education Agency
Frosty.Walker@tea.texas.gov
(512) 463-5095
The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESC’s, TEA and the private sector.
Texas Gateway
https://www.texasgateway.org/

Cyber Security Tips and Tools
Wireless Infrastructure
Mobile Devices
Basic Information Security Concepts

- Confidentiality
- Integrity
- Availability
- Information Leakage
- Denial of Service
- Illegitimate Use
- Accountability
Basic Communications Issues

- Content Privacy
- Location Privacy
- Linkability between sender and recipient
Basic Objects to Protect

- Information
- Meta-data
Basic Elements

- Hardware
- Operating Systems
- Applications
Wireless Infrastructure

2 or 3 unique wireless networks

• Guest
• Employees BYOD
• Institution owned mobile devices
Mobile Devices

- Laptops
- Tablets
- Smartphones
- USB devices
WHAT IS STORED ON YOUR MOBILE DEVICE THAT YOU DON’T WANT OTHERS TO SEE?

Files on your memory card
Contacts
SMS messages
Pictures
Call/System logs
GPS location
Control over your microphone or camera
Phone identity number
MOBILE DEVICE VULNERABILITIES

- Physical access.
- Social engineering.
- "Rooted" or "jailbroken" devices.
- Bluetooth, Wi-Fi, infrared, or other short range wireless connectivity.
- Email.
- SMS.
- Third-party applications.
- USB or memory cards.
- Operating system vulnerabilities.
- MySQL database vulnerabilities.
- GPS/location information.
- Camera and microphone.
- Cached credentials.
- Downloads.
MOBILE VULNERABILITY MITIGATION

• Mobile device management
• Remote wipe, remote lock, and the GPS location services in case device is lost or stolen
• Anti-malware and endpoint protection (personal firewall)
• Secure connection (VPN) to the workplace
• Strong authentication
• Digitally signed third-party software
• Separation of personal data from work data
• Protection from theft and data loss
• Protection of the data and company network in case the device is lost or stolen
• Download policies to prevent downloads from unknown sources
• Policies against rooting/jailbreaking devices
• Record of ESN of every device
MOBILE DEVICE MANAGEMENT

- Device provisioning in enterprise including enrollment and authentication
- Remote device lock or wipe
- Account management
- Turn on/off device features
- GPS, Wi-Fi, and cellular device location
- Remote software deployment
- OS/application/firmware updates
- Application management
- Secure backup and information archiving
- Secure, encrypted "container" on device to segregate organizational access and data
- Jailbreak or root access protection
Laptops

Whole Disk Encryption

- Microsoft BitLocker
- Apple FileVault
Tablets

Encryption

- IPad - encrypted by default
- Android - Manual but easy to implement via Settings and Security
Smart Phones

Encryption

- iPhone - encrypted by default when using passcode
- Android - Manual but easy to implement via the Settings under Security

E-MAIL

Outlook has a free application for both iPhone and Android users which works with Outlook and other email apps
USB Drives

Encryption

• Microsoft – BitLocker can encrypt USB drives
• Apple – Disk Utility can encrypt USB drives—be sure to backup drive first as all data will be erased
Questions?