Mobile Security Methods

Laptop computers, tablets, smartphones, and other mobile devices allow people to remain productive from various locations, such as at home or while traveling. This increased flexibility raises various security concerns that IT departments need to address. This reading provides information about the current security measures used to protect mobile devices.

Common mobile security threats and challenges

Many of the security threats associated with mobile devices are the same as those of traditionally networked devices, such as hacking and malware. However, mobile devices face additional threats that other devices do not.

Here are some threats facing mobile device security:

1. **Phishing**: Phishing attacks can use SMS messaging, email accounts, messages via numerous social media applications, or malicious links in browsers to target your mobile devices.
2. **Malicious applications (malware)**: Malware can take the form of apps designed to collect and transmit personal and corporate information to third parties.
3. **Insecure Wi-Fi and “meddler in the middle” attacks**: An attacker places themself in the middle of two hosts that think they're communicating directly. The attacker may monitor the information from these hosts and potentially modify it in transit. Open or "free" Wi-Fi hotspots are especially susceptible to meddler in the middle and similar attacks.
4. **Poor update habits for devices and apps**: An example is failure to install security patches regularly deployed through software and firmware updates. Unpatched devices and applications often contain exploits and vulnerabilities that attackers may use to collect sensitive data.

You can imagine how all these issues could threaten confidentiality, integrity, or access (the CIA triad)—but confidentiality is of particular concern for mobile security.

Security measures used to protect mobile devices

There are several security measures in place to protect mobile devices from these security concerns.

Screen Locks

Screen locks are methods for preventing unauthorized access to a device. They can be particularly effective for diminishing risks associated with the loss or theft of the device. These measures include:

- **Facial recognition**: uses a device’s camera to unlock the device once the user’s face is recognized

- **PIN codes**: uses a sequence of four or more numbers to unlock the device
- **Fingerprint recognition**: matches a user's fingerprint with a saved image of the fingerprint to unlock the device
- **Pattern uses:** uses a pattern that users must trace to unlock the device

Remote wipes

Remote wipes are methods to remove data from a device remotely. Remote wiping is another way to diminish risks associated with the loss or theft of a device and include:

- **Locator applications**: apps that help users find lost devices
- **OS updates**: security patches regularly deployed through Operating System updates (as well as firmware and application updates)
- **Device encryption:** encryption techniques that protect the device from unauthorized access
- **Remote backup applications**: apps that allow administrators to remotely remove applications that compromise security
- **Failed login attempt restrictions**: stops access, either completely or for a set period of time, after too many failed attempts to log in
- **Antivirus/Antimalware**: software packages for mobile devices often offered by the same vendors as desktop Antivirus programs
- **Firewalls**: either devices or software that check incoming network traffic and keep out unwanted traffic

Policies and procedures

IT departments establish policies and procedures to ensure users don't make security mistakes. They typically include mobile-specific policies such as acceptable use guidelines, preferred mobile security practices, and security platforms or services.

Once IT staff and management collaborate to build a mobile security policy, there is still work to do. Organizations must find the best way to outline this policy and communicate it to users. A policy is only effective if users understand and adhere to it.

Key takeaways:

As your organization embraces the advantages of mobile devices and wireless networks, your IT security strategies must account for the specific risks, vulnerabilities, and threats associated with mobile computing by:

1. Monitoring for common mobile security concerns such as phishing, malicious applications, insecure Wi-Fi, and poor upgrade habits and applying the current methods for addressing them
2. Implementing security measures to protect mobile devices like screen lock and remote wipes
3. Providing clear mobile security policies and procedures and communicating them to users

Citations:

#	Title	Link
1	Top 4 mobile security threats and challenges for businesses	https://www.techtarget.com/searchmobilecomputing/tip/Top-4-mobile-security-threats-and-challenges-for-businesses
2	The ultimate guide to mobile device security in the workplace	https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace
3	What Is the CIA Triad? Understanding the significance of the three foundational information security principles: confidentiality, integrity, and availability.	https://www.f5.com/labs/articles/education/what-is-the-cia-triad