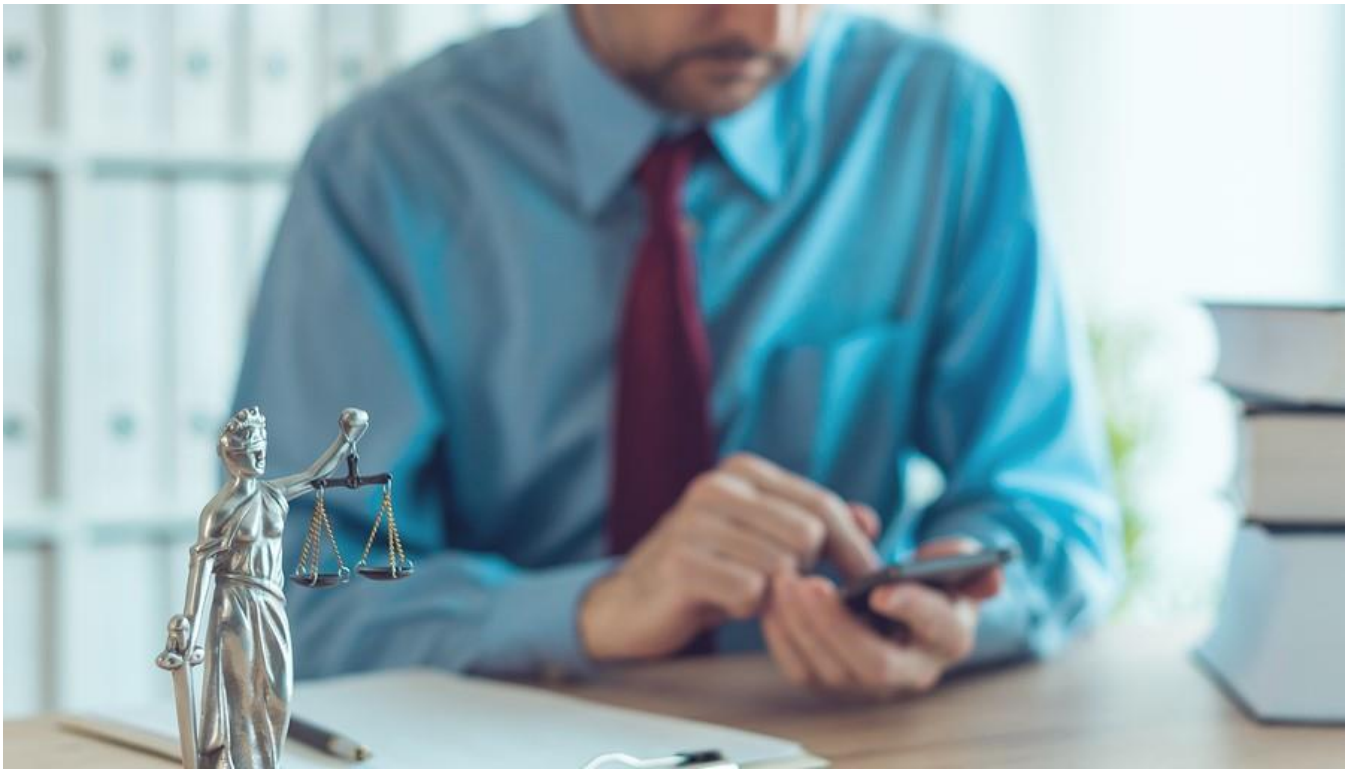
Law Firm Mobile Security Best Practices



Like most businesses, law firms have seen an increased mobile workforce in recent years. Mobile access increases employee ability to communicate with clients and coworkers quickly, as well as access documents on the run. But it also raises security concerns. Incorporate law firm mobile security best practices to protect sensitive business and client data.

1. Employ Mobile Device Management (MDM)

The industry offers a host of MDM options to help your law firm get a handle on mobile security. Choose an MDM system that allows you to specify which devices can access the network, as well as what applications they can access. Then use the MDM to:

- Limit access by role or department – "One size fits all" has no place in mobile access. Limit access to only those applications and data needed for users to accomplish their jobs.
- Allow access only to devices with a secure OS – Apple, Android and other providers continually update their security protocols. Allow access only to those devices that have installed recent updates.
- Create whitelists or blacklists – Most MDMs allow organizations to create a whitelist of acceptable apps or a blacklist of potentially dangerous apps. In 2017, for instance, Google identified and eliminated over 700,000 rogue apps from the Google Play Store. Restricting application access proves particularly important in a BYOD environment.

- Remote lock and wipe – Enable remote lock and wipe for all mobile devices used for business purposes. This allows you to protect sensitive data from compromise through a lost or stolen device.

2. Install Updates to OS and Apps

Vendors regularly release patches to the operating system and mobile apps to enhance security and introduce new functionality. These updates can prove critical to protecting mobile devices against emerging cyber threats. Turn on automatic updates to ensure that devices stay current.

3. Mandatory Multi-factor Authentication

According to a recent Verizon study, 33 percent of companies reported a compromise caused by a mobile device. And yet, too many users fail to properly secure their smartphones, tablets and other mobile devices. They either use weak passwords or no password at all.

To protect your network and data from unauthorized access, make multi-factor authentication (MFA) mandatory on all mobile devices. Combine strong passwords with biometrics and/or security tokens.

4. Encryption

While reputable cloud storage providers typically provide file encryption, they often retain the decryption key. Consequently, anyone with access to a user account can access the data. Experts recommend adding an extra layer of protection by encrypting sensitive files before uploading them to the cloud.

5. Regular Backups

You back up PCs and servers regularly. Apply that same logic to mobile devices. With more users conducting work on smartphones and tablets, these devices have become highly attractive targets for cyber criminals. In the event of ransomware, malware or a lost or stolen device, backups allow users to recover deleted or compromised data quickly.

6. Conduct Regular Security Audits

As with any cyber security solution, you should conduct regular audits of your mobile security strategy. Audit all devices, networks, apps and security programs. Review mobile policies and security protocols, updating as necessary to cover changes in technology or threats. Check permissions defined through the MDM to ensure proper access controls.

7. Provide Regular Training for Employees

Through onboarding and periodic training, emphasize mobile security awareness with all employees. Make them aware of security policy updates and best practices. For instance, teach them to recognize phishing attempts and avoid public Wi-Fi at all costs.

Implement Law Firm Mobile Security Best Practices Now

Your employees depend on mobile access, and your law firm depends on data protection. Contact eMazzanti today to determine the appropriate mobile security solution for your firm. Our legal IT security experts will help you implement best practices for network and endpoint security.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 500 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
Partner of the Year
ShoreTel Sky Partner of the Year