MOBILE SECURITY

CONVENIENCE AT A COST

Mobile devices can do more, store more, and share more than ever before. But the growing use of mobile devices and remote access to Firm information introduces new risks to the security of our confidential information. Hackers and thieves have adapted their tactics and now target mobile devices with increasing success.

MORE FEATURES, MORE ACCESS, MORE RISK

Not all the information on your device should be accessible with a single finger swipe. Because we access our devices so often, many of us shut off important security features or enable certain convenience features that put information at risk. It is critical we strike the right balance between the convenience of mobile device features and the management of risks inherent with their use.

SECURITY RISKS

Weak passcode requirements

A strong passcode is the first line of defense against unauthorized access to the information on your device. Even more important than a strong passcode is how often you require its use.

Best Practice: Create a 6- to 10-digit passcode, and if your device allows, incorporate letters and special characters, or even fingerprint and photo identification. Set an inactivity timer or screen lock for the shortest available time interval and require use of a passcode as often as you can, especially to download or delete apps.

Loss and theft

No one intends to lose a device, but how you prepare for that possibility and how quickly you report the loss can dramatically reduce the likelihood of an information breach.

Best Practice: Never leave mobile devices unattended, especially in a parked vehicle. Report loss or theft as soon as possible so steps can be taken to secure the device and wipe data.

Geolocation settings

Hackers can use stored geolocation information in conjunction with other content on your device to reveal even more sensitive information.

Best Practice: Turn off location tracking by default and only enable it for individual apps that absolutely require this feature.

Email management

If you have multiple email accounts on one device, it's easy to inadvertently create and send an email using the wrong account, which poses a risk to information security.

Best Practice: To ensure that work-related emails are always sent from the correct account, designate your Firm email account as the default. Avoid directing personal emails and work-related emails to a combined email display.

AI assistants

Data generated through these assistants—including email addresses and physical locations—is stored on the host's servers, under disclosure agreements that violate our duty to maintain client confidentiality. These assistants may also bypass your passcode lock to respond to commands, leaving sensitive information at risk.

Best Practice: The highest level of security is to disable AI assistants altogether. At a minimum, make sure your settings do not allow the assistant to bypass your lock screen. Also, be mindful of your physical surroundings when using these assistants to avoid eavesdropping.

FINDING A BALANCE

If not used with caution, mobile devices pose a serious risk to our security efforts. Familiarizing yourself with how certain features make your devices vulnerable will help you reduce the risk of exposing private and confidential data. Understand and maintain our security policies when handling sensitive information on your mobile device and report any suspicious activity or loss immediately. Use strong passwords and be aware of your surroundings when working on mobile devices. Disable features like Siri and lock-screen notifications that might reveal sensitive information or bypass security measures. Avoid clicking unfamiliar links and use secure wireless connections. Install current versions of the operating system and apps to reduce opportunities for security breaches.