TechTarget | SearchMobile Computing

PRO+ Content

# Overcoming Common Mobile Data Security Hurdles

## In this guide



## In this e-guide:

**As mobile devices and applications continue to flood the business landscape, the security holes that these consumer devices pose  put your entire enterprise network at risk.**

**Fortunately, there are a number of steps you can take to not only heighten your mobile data security, but overcome common hurdles.**

**In this exclusive mobile security guide, discover why mobile data security should be at the top of your priority list, strategies you can take to protect your assets and specific threats that you can’t afford to overlook.**

In this guide



# Make mobile data access and security top priorities

http://searchmobilecomputing.techtarget.com/tip/Make-mobile-data-access-and-security-top-priorities

There are millions of applications in businesses and public app stores, and they all have at least one thing in common: data.

The sheer volume of apps, plus the recent explosion in smart technologies and the Internet of Things, is a recipe for exponential data growth. But, ironically, mobile workers still have a hard time accessing the data they need.

There are many ways to provide mobile data access, but it's difficult to determine which is best for a company and its users. Will an app that serves as a connection to back-end systems suffice, or should IT administrators extend mobile data access to users' devices? And how will admins ensure mobile data security?

Starting down this road typically comes with more questions than answers, but there's a simple to-do list that can get things rolling. First, decide if data needs

## In this guide



to be available offline; then determine how to make that a reality. Throughout the process, make sure mobile data security is a priority.

### Offline mobile data access

Internet access is nearly ubiquitous for most organizations and their employees in the United States; 87.4% of Americans have Internet access. Many companies assume that employees always have access to the Internet, and to the corporate network via virtual private network or a comparable method, but that simply isn't the case. Companies must consider offline data possibilities in their mobility plans.

Businesses must also consider that employees who usually have Internet access sometimes end up disconnected from the Web. For example, Wi-Fi on airplanes becomes more prevalent by the day, but it's not yet standard, particularly on smaller regional aircrafts. For the road warriors in an organization, this can amount to a lot of lost time and productivity. Many employees who work on the go expect access to their information anytime, anywhere and on any device, and that sometimes includes offline mobile data access.

How to make mobile data available, online or off

How to keep mobile data secure

In this guide



To decide what needs to be offline-enabled, consider the audience: Is it a sales force that needs the ability to constantly interact remotely, or does the application target internal personnel who travel occasionally? Simple questions such as these serve as a starting point. If users don't need offline capabilities, then don't build in the complexity. If data does need to be available offline, companies must decide what that data is, how important is it to the organization and how to secure it.

## The lowdown on improving mobile data security

http://searchmobilecomputing.techtarget.com/feature/The-lowdown-on-improving-mobile-data-security

If users are going to work on a variety of endpoints, IT departments better know how to ensure mobile data security.

Mobile data can be compromised in a variety of ways: something as simple as a lost or stolen device without a passcode or as complicated as a malicious app that enters an organization's network through a user's smartphone. No matter where the threats come from, there are ways to at least minimize the risks.

## In this guide



The mobile data security battle is fought on two fronts: on devices themselves and when data is in transit between devices and apps. Take some time to learn how to strengthen the defenses against mobile security breaches with hardware and software encryption, containerization and more.

**How does hardware encryption work?**

Encrypting mobile hardware is the first line of defense against lost or stolen devices. Encryption completely scrambles any data on a device and the only way to unscramble it is with a pass key.

Every operating system is a little different with encryption. Apple's iOS features a file system with the OS information and user data written to flash memory. It also uses a factory-assigned device ID and group ID with the device user's passcode so only that passcode can unencrypt data on the phone or tablet.

Even though Android allows for encryption, not every device manufacturer creates hardware that supports it. Users can turn encryption off accidentally or deliberately with a factory reset on Android devices.

**What does software encryption add to mobile data security?**

## In this guide



If hardware encryption is making sure to lock the front door, then software encryption is taking any valuables in the house and locking them away in a safe. Even if hackers get through the device passcode they need a second passcode to access certain data or apps.

Software encryption can be much more specific than hardware encryption, allowing IT admins to pick and choose the specific information they want to protect. It requires OS-supplied interfaces or third-party functions to encrypt individual programs such as an email client or Web browser on a device.

**What are some common mobile application vulnerabilities?**

Mobile applications are a hive of potential security problems. Bad data storage practices, which are common with inexperienced developers who use clear text or XML to code apps, are just one example. When a developer uses these languages, hackers can uncover everything stored in an app by simply extracting a file attached to the app and searching for whatever they want to know. To make matters worse, if the app is connected to a company's back-end systems the hacker has an easy pathway into the rest of the network.

Malware is another common problem with mobile applications, especially on Android devices. Users can sideload apps with Android so IT has no control over what users put on their phones. Malicious app developers are crafty enough to trick many users into downloading dangerous apps with shady tactics such as disguising their apps with popular names. As a result, IT should always require antimalware on Android devices.

**What do users need to know about mobile security?**

Just like users know not to open emails they don't trust, it is important they know what to look for in untrustworthy apps. To prevent unauthorized device access, IT must educate users about permissions. If an app is asking to access information that doesn't seem necessary to the app's function, a red flag should go up. IT must also instruct users to have multiple passwords. That way if a device is stolen, hackers only gain access to one app or profile, not everything on the device.

**How can containerization help?**

A key cog in the mobile application management machine, containers separate enterprise apps from the rest of a user's device. If a user downloads a malicious

app, the containerized enterprise apps are protected from any nefarious actions the malicious app takes. Admins can prevent certain functions, such as copy and paste, within a containerized app to keep users from moving sensitive data into an unprotected app. They can also wipe the data within application containers without worrying about deleting anything else on a user's device.

Containers are not perfect, though. They often require mobile device management tools to be in place and can block certain app functions so an app cannot connect to a user's contact list.

## These mobile data security threats are more than just hype

http://searchmobilecomputing.techtarget.com/opinion/These-mobile-data-security-threats-are-more-than-just-hype

There is a lot of hype around mobile data security threats, so IT admins need to weed out the risks and determine what it really takes to protect corporate data on mobile devices.

Once devices can access corporate applications and data, they become an immediate threat to security. Employees can easily lose mobile devices.

## In this guide



Passcodes aren't foolproof, and many users don't even bother with one in the first place.

Mobile vendors continue to increase the security of both hardware (by improving microprocessors, sensors and biometrics) and software (by adding security capabilities to operating systems, browsers and email clients). Still, there are plenty of security challenges to deal with when valuable corporate data crosses the network to the Web or the cloud. So, what are the most salient mobile data security threats, and which can IT admins worry about less?

There are a few areas where the hype around mobile data security is very real. For instance, there are many potential attack surfaces that IT needs to protect -- Bluetooth, NFC, Wi-Fi, GPS, to name a few. Organizations are especially vulnerable to data leakage when employees use unauthorized personal file sharing services such as Google Drive or Dropbox for work purposes.

Other mobile data security threats, such as device loss, use of unapproved mobile applications and lack of password protection, continue to grow as well. They are some of the key contributors to data loss. The portable nature of mobile devices makes them vulnerable to theft, making it critical for IT to be able to remotely lock down and wipe them.

## In this guide



BYOD in particular can make it difficult for IT admins to or perform a data wipe or restrict employees' access to certain corporate data; users own the device, so organizations need to determine what admins can legally do. Without thorough policies in place, IT may not be able to take the necessary steps to secure corporate data on employee-owned devices.

But other security measures are less crucial. Mobile devices are certainly vulnerable to malware and viruses, but with each successive OS release, device manufacturers expand their exploit mitigation features. Handset OEMs have also added capabilities that can prevent exploited software from doing further damage to a device, such as the ability to prevent modified OSes from booting, kernel integrity monitoring and more robust sandboxing and containerization mechanisms.

There is inevitable hype around mobile data security threats with each high-profile security breach that occurs, but it is important to note that virtually none of those breaches are related to mobile devices. Despite the aforementioned hardware and software security elements, neither an ideal hardware configuration nor one type of network protection can reliably catch all threats. Investing in IT staff with mobile-first security expertise is important, as is

## In this guide



implementing the appropriate infrastructure to enable secure remote access to pre-existing data stores and application platforms

## In this guide



# Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers—a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

## Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia