SAMSUNG

White Paper:

10 Smart Ways to Keep Your Personal and Work Mobile Data Safe

Introduction

Navigating your personal or work life without a smartphone has become unthinkable — and using one device for both work and personal needs is now the norm.

Increasingly, employers are issuing smartphones to most or all full-time employees today as a core business tool. While in highly regulated industries these devices may be strictly limited to corporate use, most other businesses allow personal use outside of work hours.

And, if your company doesn't issue you with a smartphone, the chances are you are using your personal phone for work-related tasks.[1]

Using one phone for work and life can improve productivity and make it easier to manage our busy schedules. But storing both work and personal information on one device can also put you and your company at risk.

More Risk, Little Protection

63%

of mobile users admit that the amount of sensitive and confidential data on devices has increased significantly in the past two years.[2]

55%

say they have concerns about work-related data they have stored on their devices.[3]

But only

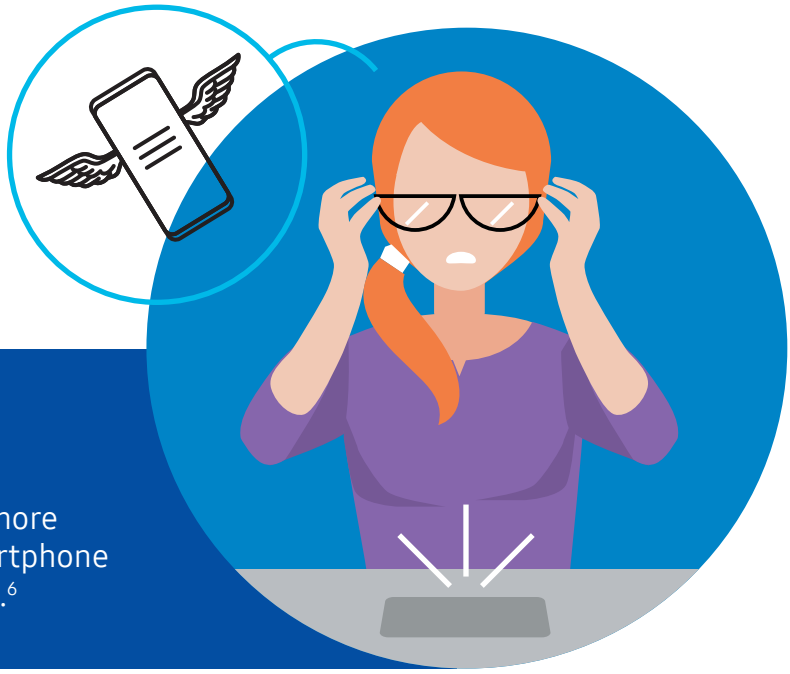
49%

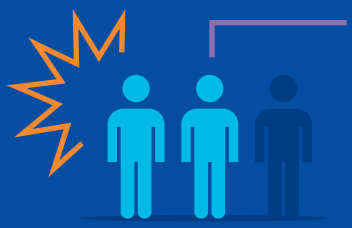
of mobile users take any steps to protect mobile data.[4]

Understanding Mobile Security Risks

One of the biggest threats to your personal and work data is having your device lost or stolen. It's akin to losing your wallet — or worse. Indeed, two-thirds of mobile users worry more about losing their mobile device than their wallet — and of those who have lost their device, 81 percent said the experience was highly disruptive.[5]

The best way to protect yourself against these threats is to be proactive.





2/3

of mobile users worry more about having their smartphone stolen than their wallet.[6]

Consider these 10 steps you can take to improve your mobile security, thus better protecting your data and thwarting would-be hackers.

Step 1. Lock Your Phone Screen and Use Strong Passwords

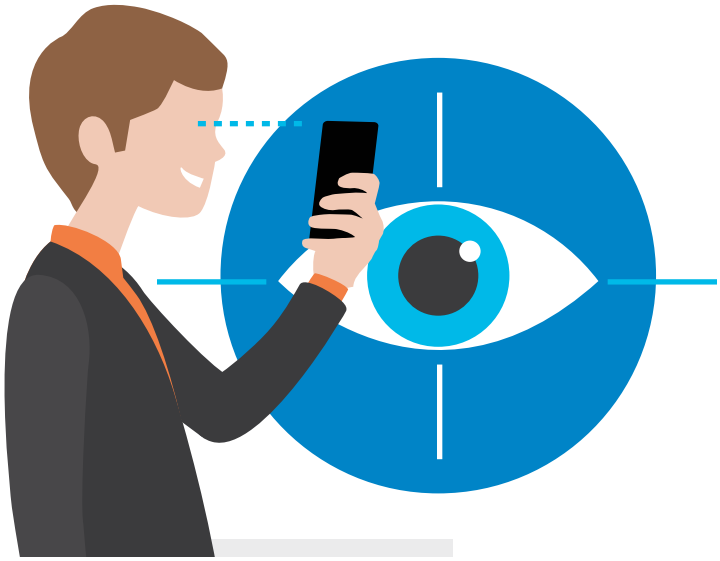
1/3

Android smartphones aren't secured with a lock screen passcode.[7]

The most basic level of protection you should have on your mobile device is the lock screen. Without one, anyone can access your personal and work data, including financial and retail apps that may provide direct access to your bank accounts or other highly confidential information.

Set Your Lock Screen Password

If you're currently part of the one-third of mobile users without a lock screen passcode,[7] you can set one up in your phone's settings. Select "lock screen" and then pick your preferred method, such as a PIN, password, or on some devices, such as the Samsung Galaxy S8 and Note8, fingerprint or iris scanning. Using two methods — such as a password and an iris scan — adds another layer of security and is highly recommended. Never use a pattern unlock, though, because these can easily be replicated from smudge patterns.



Don't Reuse Your Passwords

Consider this: Hackers reused a Dropbox employee's password they harvested from breaching LinkedIn to then access Dropbox's corporate network and steal user credentials.[8] Having one password and set of login information, or even a handful, may be easier for you to remember, but it also makes it much easier for hackers. Even if you follow the password best practices, if you reuse that password on an unsecured site, every account that uses that password — from your corporate email to your bank accounts — is now accessible to hackers.

Replace Your Passwords With Biometrics

You can reduce the need to remember multiple unique passwords by using iris or fingerprint scanning technology instead to access your accounts. Samsung Pass offers secure access using biometric authentication technology such as fingerprint or iris scanning. Once Samsung Pass is enabled on your smartphone, you can choose to sign into any website or many supported apps using biometrics.

What Are Biometrics?

Biometric authentication is increasingly viewed as a more secure alternative to traditional passwords and passcodes. Biometrics offers a quick way to unlock your mobile device or access accounts without having to remember multiple, complex passwords; it also provides options for protecting your device with two forms of authentication.

Types of Biometrics

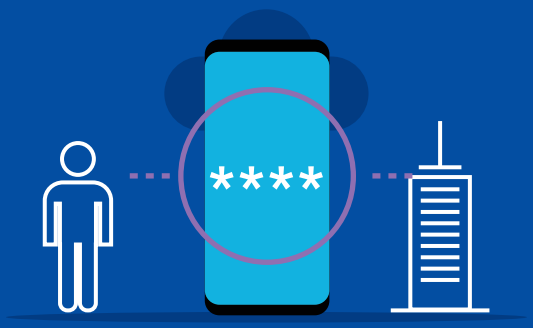
Facial recognition:
A fast and convenient way to access your device, but is not the most secure biometric option.

Fingerprint scanning:
Unlock with a quick touch. More secure as fingerprints are highly unique and difficult to replicate.

Iris scanning:
The most secure biometric authentication method and is almost impossible to replicate, allowing you to unlock your device with a look.

68%

of users say they have shared passwords across personal and work accounts accessed by mobile devices.[9]



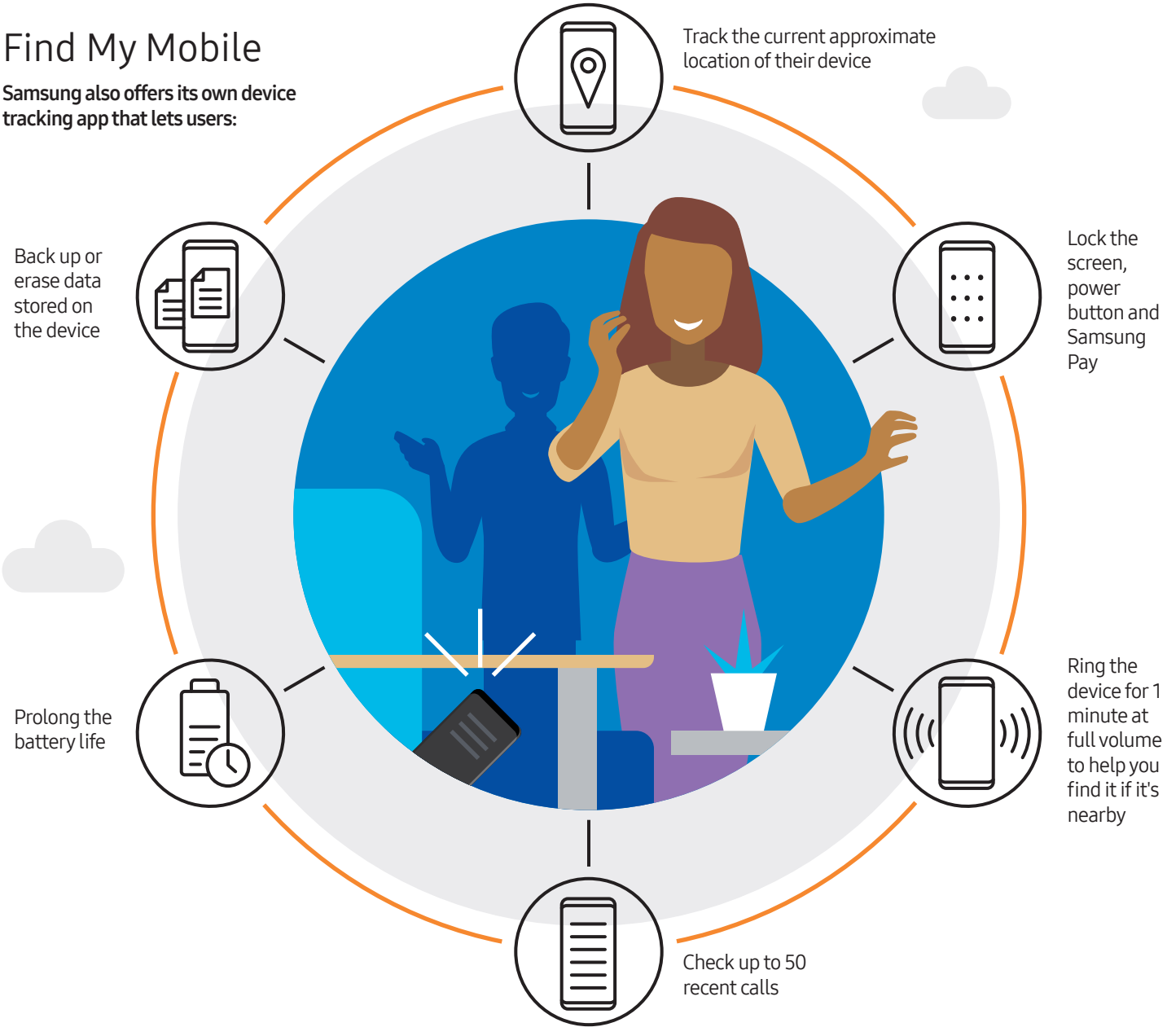
Step 2. Enable Device Tracking on Your Phone

Whether you lose your device somewhere in your house or leave it in the back of an Uber, having a way to track its location can help you quickly locate and regain control of your device.

To find your missing smartphone, you can use Google's Android Device Manager, even if you don't have the app installed. Once you've told the Device Manager to find your missing phone, it'll use the GPS tracking in it to locate its whereabouts. It'll provide the time it was located, the location and the accuracy range.

Find My Mobile

Samsung also offers its own device tracking app that lets users:



Step 3. Download Apps From Trusted Sources

With over a million apps to choose from and new ones hitting the market every day, there's an app for almost everything you want to do from your mobile device. However, malicious apps infected with malware or aggressive adware are pervasive, and it's important you use caution when downloading apps to your mobile device.

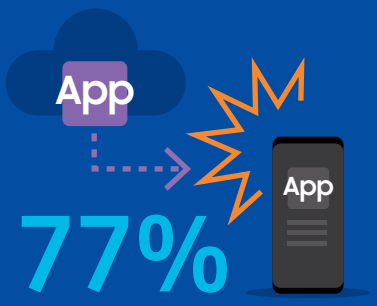
Here are three key rules to follow when it comes to downloading apps:

1. Consider the source of the app. Download apps only from trusted sites such as Google Play. Additionally, your company may have its own app store or use Google Play for Work to support common productivity and business-oriented apps in a secure environment.

2. Remain cautious even when downloading from a trusted site. Even with strict screening processes, Google has had to pull hundreds of infected apps that made it through the screening process from its store.

3. Be aware of what permissions your app is asking. Most apps' requests for permission are harmless, such as a flashlight app asking for access to your camera flash. However, be aware of what permissions the app is seeking and whether it's necessary to the app's function. For instance, if that same flashlight app is seeking permission to access your contacts, you should be wary of installing the app.

It's important you use caution when downloading apps to your mobile device.



77%

of smartphone owners reported downloading apps other than the ones that came pre-installed on their phone.[10]

90%

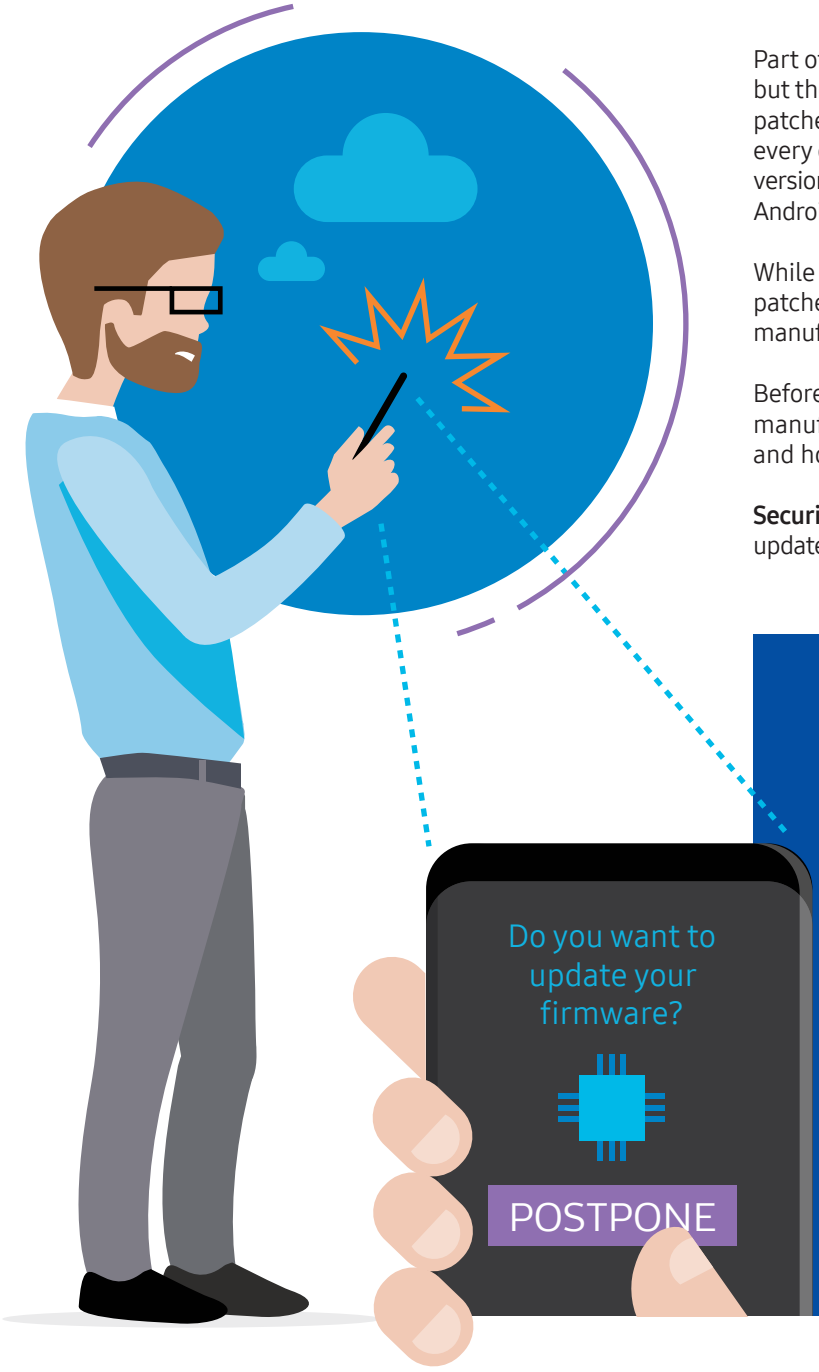
of app downloaders said how their personal data will be used is "very" or "somewhat" important to them when they decide whether to download an app.[11]

60%

of these app downloaders had chosen not to install an app when they discovered how much personal information was required in order to use it.[12]

Step 4. Keep Your Device Software Updated

Devices that aren't kept up-to-date with the latest patches are susceptible to malware attacks. A recent study by Skycure found that 71 percent of mobile devices still run on security patches more than two months old.[13]

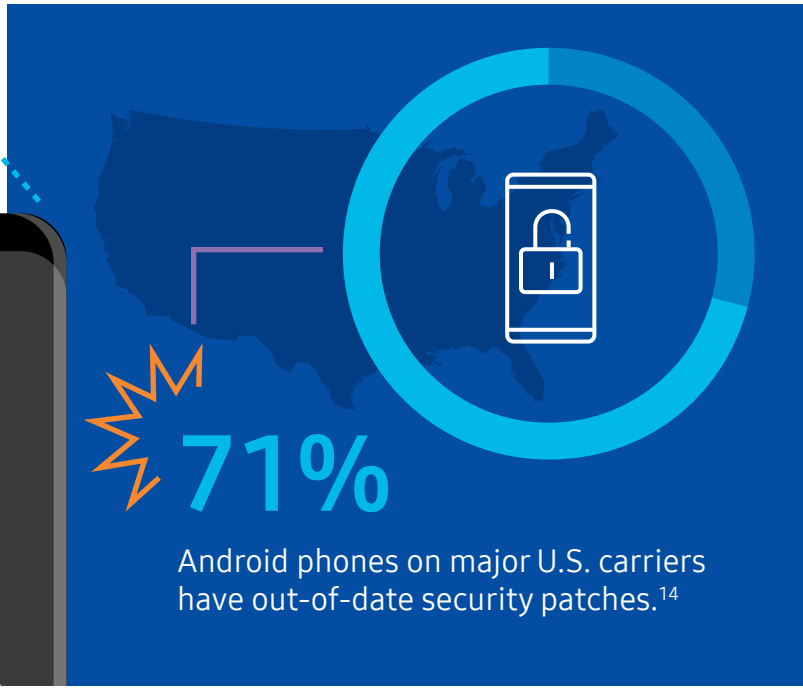


Part of the fault lies with users who don't install the updates, but there are other factors at play. Although Google releases patches every month, in an open-source Android environment, every device manufacturer implements a slightly different version of the OS on their phones. This means that different Android device models may have different security vulnerabilities.

While Samsung has committed to providing monthly security patches for its current set of devices, not all Android device manufacturers provide regular updates.

Before purchasing a device, research providers and manufacturers so you know which ones apply updates and how often.

Security Best Practice: If your device is no longer receiving updates from the manufacturer, it's time to upgrade your device.



71%

Android phones on major U.S. carriers have out-of-date security patches.[14]

Step 5. Encrypt Your Storage

Another basic level of protection your mobile device should have is on-device encryption. Devices with encryption store information — including your photos, text conversations, emails, documents and more — in a scrambled format that is only unscrambled when a device's lock screen passcode is entered.

As of 2015, Google began requiring that Android manufacturers enable encryption on all devices out of the box. However, Google has waived this requirement on some entry-level devices where encryption would slow the performance of the device considerably.

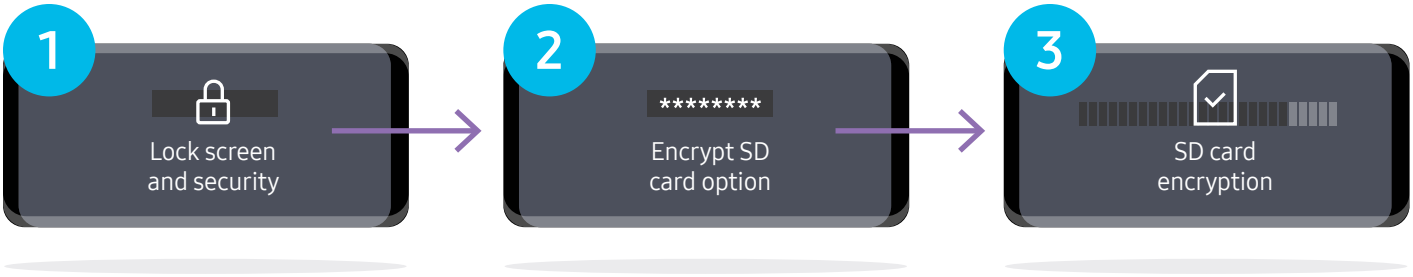
How Do You Encrypt Your SD Card?

Much of your data may be stored on your phone's SD card. Android users can encrypt this vital data through the Settings menu. First, select Lock screen and security" then tap on the "Encrypt SD card option."

After entering your phone's master screen unlock passcode, encryption will begin on your SD card. Remember that once encrypted, the card can only be read on the device that encrypted it and if the phone is reset to factory settings, it will be unable to access the data on that card.

The encryption process may take up to a several hours, depending on the card's size and contents.

Security Best Practice: Upgrade your mobile devices every two to three years to ensure you have the latest hardware security technology on your device.



Step 6. Back Up Your Files and Phone Settings

If your device is lost or stolen, you may never see it again. According to a recent study from Kensington, only 7 percent of lost devices are ever recovered.[15] Issues with malware may also force you to reformat your device back to factory settings, wiping away your files and personalized device settings.

Even if you already store your photos, music and other personal data in a cloud-based storage, make sure you've also backed up your phone settings so you don' t have to manually reinstall apps or configure your home screen to your preferences.

For Samsung device users, Samsung Cloud saves both your mobile data and device settings. You only need to sign into your Samsung account on your device; no separate cloud app is necessary. If you lose your device, restoring your data and settings is simple. From the home screen layout and its apps, to the alarm and Wi-Fi settings, Samsung Cloud restores everything back to the way you had it.

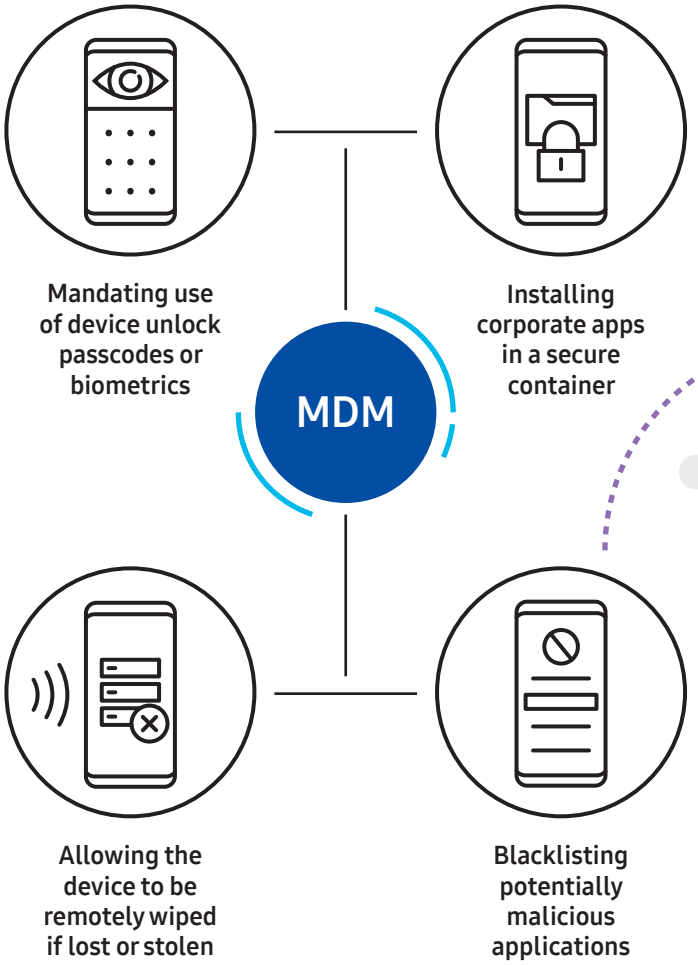
Security Best Practice: Best practice is to automate the backup of your files and device so you don't have to worry about it. If you can't do that, then make sure to back up your device 2-3 times a week.

Step 7. Understand Your Company's Device Management Policy

Whether your company embraces a BYOD policy or issues you a corporate-owned device, most employers want to have some control over securing their data on your device.

A mobile device management (MDM) solution allows your employer to enforce certain controls on what you can or cannot do with your device to ensure users don't bypass company policies.

MDM solutions vary in their capabilities, and employers vary in how much control they want to exert over employee devices, so it's important to understand the policies and controls in place where you work. Here are some of the most common control features of an MDM solution:



Many of the policies mandated by IT departments mirror best practices for general users, but in the context of a corporate structure, they may restrict usage in slightly different ways. Understanding these limitations allows you to operate as efficiently as possible within the context of those guidelines.

Step 8. Don't Root Your Device

Rooting or jail breaking a device is the process of removing the security limitations imposed by the operating system vendor.

Rooting or jail breaking a device is the process of removing the security limitations imposed by the operating system vendor. This grants full access to the operating system and its features — giving the user more control over their device — allowing them to install a variety of new unapproved programs, customize their device's functions and operations, and tailor their device at a fundamental level.

It also means that the security of the device is undermined and that all apps, including malicious ones, can access the data owned by other applications. Mobile devices can also be rooted by hackers, but typically this requires physical access to the device, as remote rooting is extremely rare.

Most companies prohibit the use of root-enabled devices. If you choose to root your device, you don't simply increase its vulnerability to malware — you may be at risk of noncompliance with your company's mobile device policies. Rooting a device will also void the phone's warranty.

Samsung Knox

Receiving the most "Strong" ratings of any mobile security platform in a report from Gartner,[16] Samsung Knox provides built-in defense-grade security right out of the box. Anchored in the device's hardware, Samsung Knox protects the device from the moment it boots up all the way through launching an app. In fact, Knox includes strong protections against any attempt to root the device and takes a number of steps if it detects such tampering. The Knox Tamper-Evident Fuse indicates whether the device has ever booted up in a non-allowed state and, once tripped, will never allow it to enter the "Secure World" of protected data and applications.

Step 9. Separate Work and Personal Data

Having one device for work and play makes life simple, but comes with security and privacy concerns for both you and your employer.

To preserve personal privacy while securing company data, some businesses deploy enterprise-grade data separation solutions like Samsung's Knox Workspace, which ensures the partitioning of work and personal use.

Create Personal Security and Privacy

Your employer may not offer a solution to separate work and personal data, or they may, but you still want an extra level of security and privacy for your personal data. Samsung's Secure Folder, available on the Galaxy S8 and Note8, offers the ability to easily separate and secure data and applications.

Secure Folder leverages the enterprise-grade security offered by the Samsung Knox platform, including data encryption, to create a secure area on the device where you can add apps and other content, such as documents, photos and files. The Secure Folder can only be accessed through a password or biometric authentication, such as iris scanning or fingerprint scanning, set up by the original Samsung account user. The folder comes with an added layer of protection through integration with Samsung Cloud, which creates a secure cloud backup system isolated from other general backup files.

In the Settings folder, under Lock screen and security, you can tap Secure Folder to start the process. Effectively, you will set up a separate storage entity secured by passcode or biometric authentication, in which you can install completely separate versions of apps that won't share any data or login info with the versions already installed on your phone. With Secure Folder, you can store data and check email, social media and financial information in a safe ecosystem.

Step 10. Use a Virtual Private Network

Public Wi-Fi hotspots are popping up almost everywhere, but lack of authentication makes it easier for hackers to gain access, leading to malware infections and data theft.

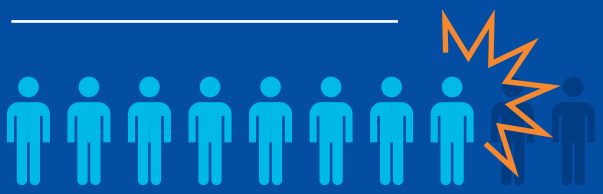
Access to free Wi-Fi has paralleled the explosion of mobile device usage. Public Wi-Fi hotspots are popping up almost everywhere — coffee shops, airports, hotels and more — and they're convenient to use because they don't require a password. However, this lack of authentication also makes it easier for hackers to gain access, leading to malware infections and data theft.

While the best practice would be to avoid using unsecured Wi-Fi completely, this isn't always practical for mobile professionals. If you do need to hop on a free hotspot, the only reliable protection — which is also recommended by the Identity Theft Resource Center — is to always use a VPN. A VPN encrypts the connection, keeping your data safe and preventing your device from being tracked.

Most mid-to-large companies offer a VPN solution for employees to access corporate systems. If you don't already have one on your device, check with your employer to see if they have one you can use. If your employer doesn't offer one, free and low-cost personal VPN solutions are available.

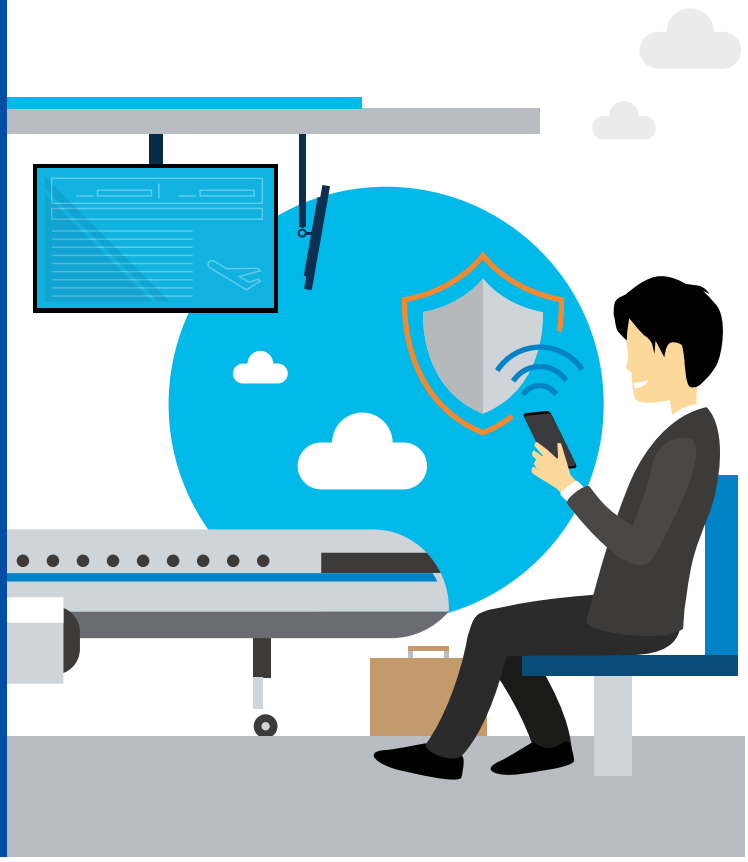
Security Best Practice: Turn off Wi-Fi when it's not being used. This will prevent your device from searching for a nearby hotspot and connecting to it without your verification.

3 Riskiest Locations for Public Wi-Fi, Ranked by IT Leaders[17]



79% of people who connect to the internet via Wi-Fi are aware it can lead to identity theft.[18]

27% but only 27% use a VPN to protect themselves.[19]



Conclusion: Work and Play Securely

Protecting your personal and work data is a continual effort that requires your active participation. But given the consequences of identity theft or the loss of irreplaceable data, such as putting your job at risk if your carelessness endangers confidential company information, taking these extra is steps worth it to ensure that you can work and play on one device securely and productively.

Learn more: Samsung Mobile Security for Business Users

Footnotes

1. Here's the Problem With Companies That Allow Employees to BYOD – "Bring Your Own Devices," Jessica Smith. Business Insider. July 13, 2015,
2. How Much Is the Data on Your Mobile Device Worth? Ponemon Institute. January 2016.
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. PSA: 34% of You Aren't Even Using a Lockscreen Passcode, Robert Triggs. Android Authority. Jan. 21, 2016.
8. Dropbox Employee's Password Reuse Led to Theft of 60m+ User Credentials, Kate Conger. Tech Crunch. Aug. 30, 2016.
9. How Much Is the Data on Your Mobile Device Worth? Ponemon Institute. January 2016.
10. Apps Permissions in the Google Play Store, Kenneth Olmstead and Michelle Atkinson. Pew Research Center. Nov. 10, 2015.
11. Ibid.
12. Ibid.
13. Mobile Threat Intelligence Report: Q4, 2016. Skycure. 2016.
14. Ibid.
15. BYOD Creates Greater Security Risks. Kensington Inc. November 2014.
16. Knox Receives the Most "Strong" Ratings of Any Platform in Gartner Mobile Security Report. Samsung Business Insights. April 13, 2016.
17. 2017 Mobile Security Report. iPass. 2017.
18. Users Know the Risks, But Connect to Wi-Fi Hotspots Anyway, Sead Fadilpašić. BetaNews. Aug. 18, 2016.
19. Ibid.