Why Should I Care?

MOBILE SECURITY FOR THE REST OF US

10 Simple Things You Can Do to Protect Yourself and Your Organization from Today's Mobile Computing Threats



by VERACODE

Share this:

www.dbooks.org

Contents

Foreword 1

Part One: It's Scary Out There 2

Part Two: Whose Job Is It Anyway? 14

Part Three: 10 Ways to Secure Your Mobile Gadget 24

Special Offer ..... Inside Back Cover





FOREWORD

by Chris Wysopal
Co-founder, CTO & CISO of Veracode, Inc.

I've already accepted the fact that Bring-Your-Own-Device (BYOD) is a business trend that's here to stay. According to one report I recently read, just 23 percent of enterprise employees use company-sanctioned mobile devices only – meaning 77 percent of employees are using their own devices in some capacity to do their job.[1] As the Chief Information Security Officer (CISO) at Veracode I have experienced this trend firsthand and if it hasn't hit you yet, the BYOD tidal wave is coming your way!

We've created this mobile security book to help you successfully ride that wave. After reading this book you and your employees will learn, as we have at Veracode, it takes a coordinated effort between employees and IT/security personnel to truly secure mobile computing in the enterprise.

Formulating a BYOD policy is only one side of the equation – employee education is the other. Most business users simply aren't aware of the security threats facing them when they use their favorite mobile device at work. This book aims to increase that threat awareness level and ultimately convert your employees into willing participants in your organization's secure mobile computing or BYOD program.

This book lists 10 simple things that every business user can do to help protect their personal information as well as their company's data, IP and brand when they use their mobile devices at work. We've made every effort to make our mobile security story a fun one to read. Some of the details around the mobile security stack can be tedious, but it's hard to resist when the stack looks like a club sandwich!

We hope you and your employees find this book helpful, and we encourage you to share it with your colleagues. We'd also appreciate your feedback, so feel free to email us (info@veracode.com) or contact us on Twitter (@Veracode) with your comments.

Happy reading...



Chris Wysopal

www.dbooks.org

PART ONE

It's Scary Out There



Share this:



Our mobile devices are wonderful things.

Not only are they highly portable, they are essentially small computers themselves – allowing us to stay productive with apps, email and Internet access at all times. We use them on our commute, we take them when we travel, and increasingly, we bring them to the office with us. They store vast amounts of information and provide a critical gateway to the rest of the organization.

Unfortunately, **your favorite mobile gadget is inherently insecure**. Small and compact, mobile devices are easy to lose or steal. Yet the looming threats to mobile security are larger than petty thieves alone. Hackers and criminals who don't even need physical access to your device can crack its sensitive and confidential data. Unless proper precautions are taken, intruders can "sniff" personally identifiable information over wireless networks or worse still, install mobile malware – malicious applications that hijack your mobile device to do all sorts of nefarious things.

Your employer or service provider has supplied this booklet to educate you about the potential dangers of mobile computing and to impart **10 simple things you can do to protect yourself and your organization**.

To do this, we'll need some help.

www.dbooks.org

Joe IT here already knows a lot about mobile device security. It's his job to secure the corporate network and all of the hardware that runs on it, like laptops and servers. He's worried about all the smartphones, tablets and other mobile gadgets that are now accessing his precious network and the sensitive business data it protects.



May we also introduce Joe Worker, or "JW" for short. He's just like you. JW loves the portability and convenience of mobile computing, and carries his favorite gadget with him everywhere. He wants to use his personal device at work and can't understand why Joe IT shivers at the very idea.



Now that introductions are out of the way, let's look first at...

The Growth of Mobile Computing



42%

Growth of the smartphone market between 2010 and 2011. By mid-2013 smartphones could make up **50%** of overall mobile phone sales.[2]



40 MILLION

Number of tablets sold in less than 2 years, a feat which took the smartphone 7 years in the U.S.[3]

1 BILLION

Number of iOS and Android smartphones and tablets expected to be activated by the end of 2012. Since 2007 there have been more than **500 million** activated.[4]

3.1 BILLION

Estimated number of mobile broadband subscribers by 2015, compared to **848 million** The number today of mobile broadband subscribers worldwide surpassed that of fixed broadband subscribers at the end of 2010.[5]

40 BILLION

Estimation of how many applications have already been downloaded from the Apple iTunes store and Android Marketplace. The average smartphone user is beginning to spend more time in mobile applications than they do browsing the web.

www.dbooks.org

It's clear that consumers are going mobile in huge numbers. Now, they want that same great mobile experience they have at home to come with them to the workplace.



Joe IT, you can certainly understand why JW loves his iPad. But JW, you need to appreciate that IT organizations are struggling with how to advise employees about securing their smartphone or tablet before it's used as a business tool. Allowing staff to use any mobile device they choose is becoming a differentiator for companies seeking to hire great employees, but it can become a nightmare for the IT department who is responsible for protecting valuable customer data and company intellectual property (IP).



I certainly don't understand the danger here!
I mean, it's a smartphone.
Nobody attacks mobile phones.



Actually JW, they do.

Some hackers and criminals follow the crowd because they want to victimize the largest number of people possible. Other cyber criminals follow the money, sniffing out financial spoils from the unprotected. Your smartphone, if unprotected, makes you easy pickings and if it's connected to your organizations network it simply becomes a conduit to all the proprietary data stored there. With mobile usage reaching critical mass, ensuring the security of your mobile device has never been more important.

It is not inconceivable to predict a future where smartphone and mobile device usage becomes the de-facto standard for businesses and consumers alike, surpassing the use of desktop and laptop PCs.

We're not there yet, but we're heading in that direction.

Unfortunately, one could argue we're presently in a state of mobile insecurity.



www.dbooks.org

Good point, Joe IT.
To understand the threat better, it's important to review some more stats on...

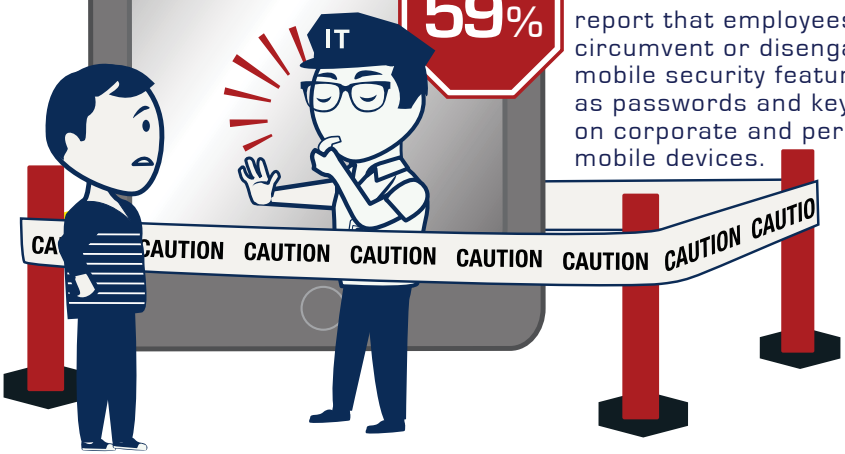
The State of Mobile Security

According to one recent study of IT professionals: [6]

51% of the organizations surveyed had experienced data loss from employee use of insecure mobile devices, within the past year.

59% reported that their organizations experienced an increase in malware infections as a result of insecure mobile devices in the workplace.

59% report that employees circumvent or disengage mobile security features, such as passwords and key locks, on corporate and personal mobile devices.



In fact, a single successful mobile attack can cripple your favorite device, result in the loss of personal or business data, open the door to possible identity theft or worse, result in financial loss to either you or your organization.

Consider the potential damage:

One study examined 855 data breaches in 2011 alone that were responsible for 174 million records stolen.[7]

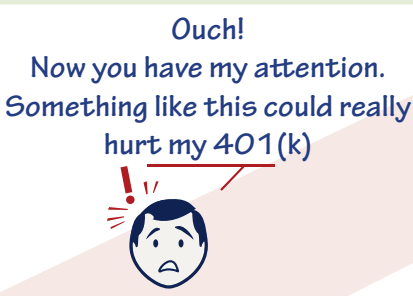


The costs of a single data breach are daunting: now up to $194 per compromised record, or an average $5.5M per incident.[8]



You certainly don't want your mobile device to contribute to those statistics.

Besides the threats of data loss, financial robbery and ID theft, victimized enterprises risk potential lawsuits from disgruntled users, regulatory action from government bodies, and severe damage to their brand and reputation. For public companies, data breaches can hammer their valuation. After its widely reported breach incident in March 2012, **Global Payments** stock dropped 13 percent before trading was halted.[9]





www.dbooks.org

Among all organizations that reported the source of breach incidents in 2011, **40 percent** were traced back to application security issues such as cross-site scripting and SQL injection.[10]

But I download all my apps from the official marketplace. What do you mean they aren't secure?

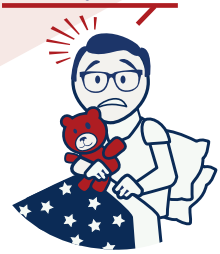


Unfortunately JW, the security controls that the app marketplaces have in place to vet the safety of their offerings are woefully inadequate. Apple strictly controls its app store and inspects which apps are approved for listing, but it's not clear exactly what security measures they are checking for. Android is more open with more distribution channels including third-party marketplaces. While choice is good for Android users, app security is an afterthought – it's up to the community of users to "report suspicious apps". That approach has been a boon to malware authors. Even security researchers were startled to find that Android malware (malicious apps) grew **3,325 percent** in 2011 alone.[11]

No need to worry. I'd never buy a malware from my app store.



This is the kind of stuff that keeps me up at night…



App stores have been very quick to remove malware once discovered, but that's typically after the damage is done. They need to get serious about vetting code before it is made available for download. Users can't rely on the "halo effect" of a reputable app store or trust fellow user reviews to rate the reputation of app vendors when it comes to mobile code security. In some app stores, legitimate apps have been pulled down by hackers, corrupted with malware, and then reposted without the original publisher's knowledge.

You may think you are installing a harmless game or utility, then… Gotcha!



That's right. Malicious apps behave in insidious ways.

That innocent looking app might in reality be:



Hidden spyware that tracks your activities like texting, emails, calls, location, contacts, or browsing history – and sends it all to the crook.



Malware that actually generates unauthorized premium rate calls, texts or purchases – all charged to your wireless bill.



Phishing screens that look like legitimate logins to a known service like online banking or social networks but are instead clever methods to steal your credentials.



Processes that run completely in the background, conceal themselves, or lie in wait for certain behaviors like an online banking session to strike.

www.dbooks.org

Wow, nasty stuff.
You mean while I'm playing sudoku,
my smartphone might be playing
fast and loose with my privacy?



Not only your personal information, but maybe your organization's as well. If you're bringing your iPad and smartphone on the road with you, connecting remotely to the office network or email server, sending confidential files and other sensitive information back and forth, carrying the customer list with you, or any number of other normal workplace behaviors – you're putting the whole organization at risk.

Guilty as charged… I guess.
But I don't know how to secure my smartphone.
That's what I have Joe for, isn't it?

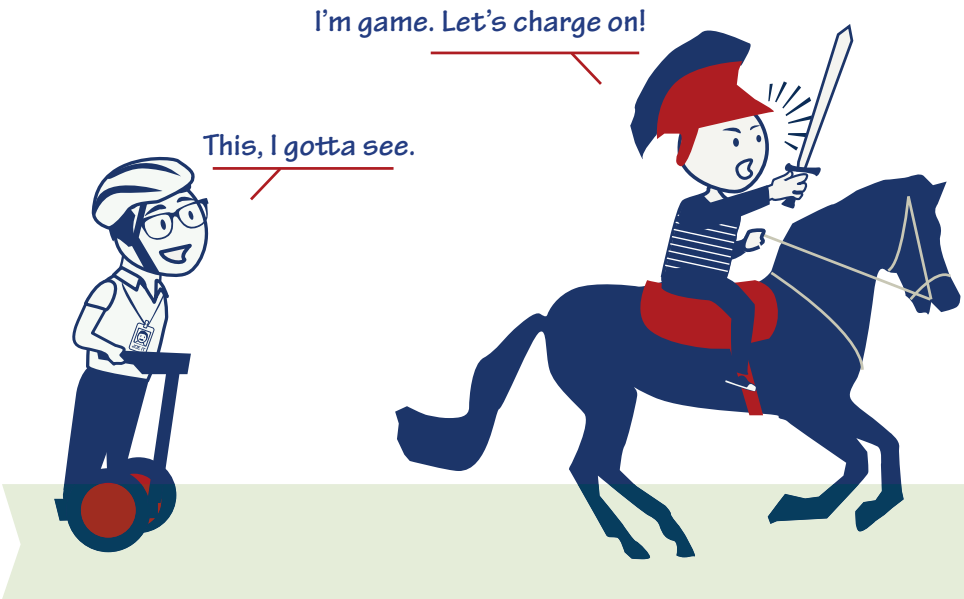


I can help…
but I can't follow you around all day.
I need help from you too.



It doesn't matter if you work in sales, HR or accounting – **it's everybody's responsibility to protect the organization's sensitive data**. Neither of you would want confidential information about your customers falling into the wrong hands, would you? IT can lead the mobile security charge, but Joe can't be expected to take on complete and full responsibility – especially if it's your personal mobile device.

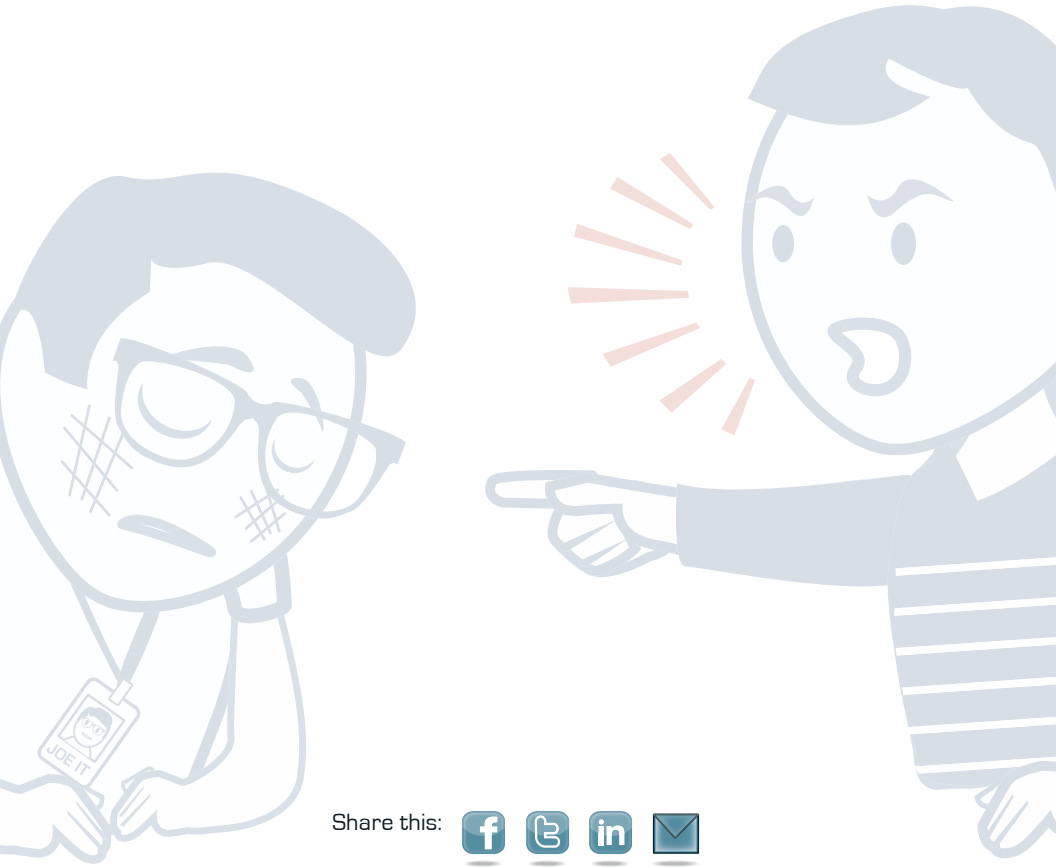
Maybe it would be helpful to review the roles each party plays in the mobile security problem? Then you'll see how each of us plays our part in securing the organization's data from those who would do us harm.



www.dbooks.org

PART TWO

Whose Job is It, Anyway?



Share this:

Similar to the PC security market,

there are a number of players responsible for delivering mobile security. These include:

1. Mobile telecom service providers that own the infrastructure (e.g. AT&T, Verizon)

2. Hardware manufacturers that provide the devices (e.g. Apple, Samsung, LG)

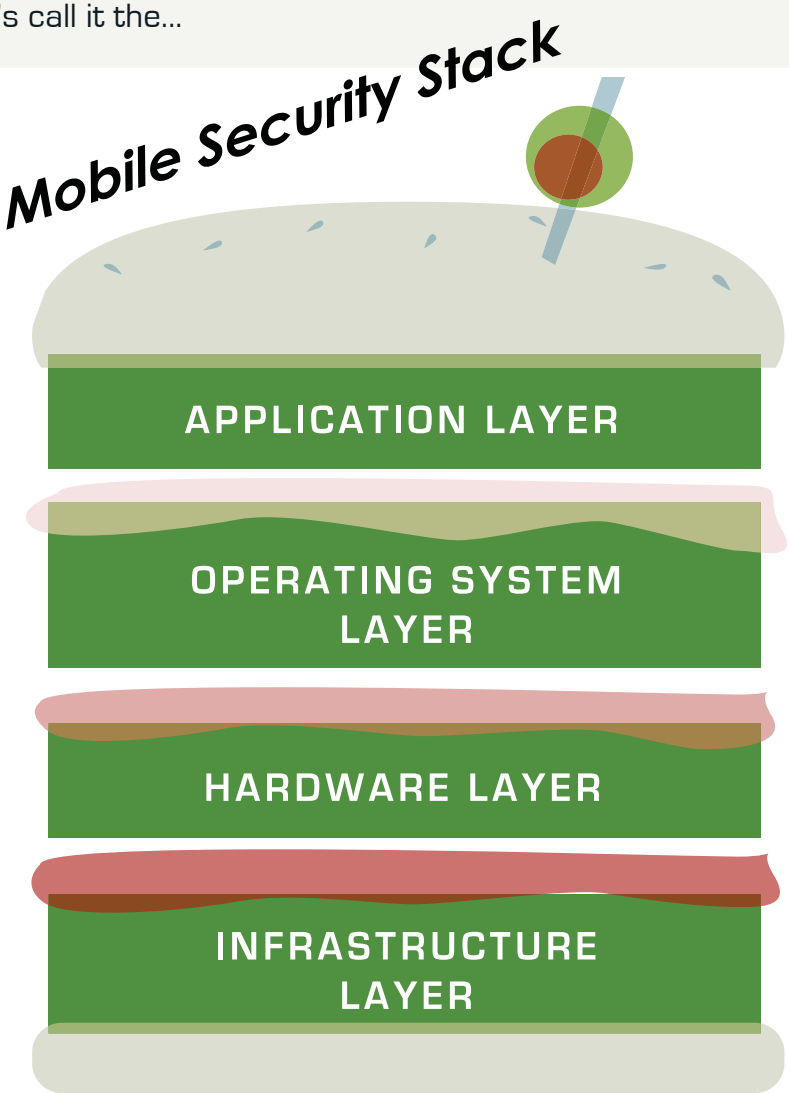
3. Mobile operating system (OS) vendors that provide device software (e.g. iOS by Apple, Android by Google)

4. Mobile app developers (e.g. too many to count, but think Rovio, the creators of Angry Birds)



www.dbooks.org

It's helpful to think of these 4 layers as a stack; let's call it the...



That kinda reminds me of a club sandwich. Yum. It must be getting close to lunchtime!



The upper layers of the stack rely on all of the lower layers to ensure that their components are appropriately safe.



At the bottom **Infrastructure Layer**, mobile voice and data carriers helped define the foundational communication protocols that allow services such as short message service (SMS) for texting and the competing CDMA and GSM standards for connecting voice calls, among others. Security flaws or vulnerabilities discovered at this tier can affect everyone who has a mobile device.





The actual mobile device comes into play at the **Hardware Layer**, which defines the security of the physical equipment, such as your smartphone or tablet computer. The end user may own the device, whether a consumer or a business user like JW, but is at the mercy of the manufacturer for its physical security. Each hardware device relies on something called "firmware" to integrate these two layers above and below. Flaws and vulnerabilities at this layer affect all users of that particular device make or design.



Are you following this so far?

I really am trying, but not hearing anything so far that's under my control.



www.dbooks.org



Hang in there!

Next is the **Operating System Layer**. The OS is the software running on your device that allows communication between the device firmware and its installed apps. Many mobile users are familiar with their OS because Apple and Google make a big deal every time they roll out a major update to iOS or Android. In Apple's case, they control both the hardware and its OS, while the Android OS runs on devices from many different manufacturers. Google lets device manufacturers make their own customizations to the OS on their hardware, so this further complicates mobile security issues. OS flaws and vulnerabilities are very common and tend to be a ripe target for attackers that want to reap widespread havoc.





IT can definitely help secure hardware and OS, er...on approved devices, of course.

Finally, at the top and closest to the mobile end user is the **Application Layer**. This is JW's primary entry point to everything that is possible to do with his smartphone or tablet.



Now we're finally getting to something I care deeply about: ME.



Apps and services at the application layer communicate with the outside world by sending data all the way down the stack and over the telecom network or the Internet. Security flaws and vulnerabilities at this layer generally originate from:

1. Coding flaws in the mobile apps themselves; or
2. Poor implementation of available mobile security measures.



Poor **end user education** on secure mobile computing practices is often to blame. You could also argue that wireless carriers should do more to protect their customers, that hardware manufacturers should take more responsibility, that Apple or Google should protect their OS better to leave less to chance. But we really can't control them.



www.dbooks.org

We all have a stake in mobile security because of all the compelling reasons we've already covered.

What IT can control is how your organization confronts mobile security issues. Joe is responsible for enterprise mobile policies, mobile device management, service provider selection, approved software distribution and the organization's overall security posture. How IT trains employees on safe mobile computing practices and security policies is dictated by whether they sanction "approved devices only", or allow workers like JW to bring his own device to work, commonly called BYOD.



Let's review the facts.

Application security flaws generally result from coding errors in applications that are either shipped with or installed onto a mobile device. Sanctioned mobile applications need to be tested and certified secure, and then whitelisted for use. Joe, if your IT group is developing custom apps for your mobile workforce, then you need to listen to this next part...

Well, we have started to develop more of our own mobile apps, but why is testing so important?



The software vulnerabilities now corrupting mobile apps are many of the same code security flaws that have been common in web applications for years. These include insecure storage or transmission of sensitive data, improper cryptographic algorithms, hardcoded passwords, and backdoored applications.

As a data point, **42 percent** of Android applications contain hard-coded cryptographic keys, making it trivial for an attacker to compromise them.[12] All enterprise development teams, whether in-house or outsourced, need to scan their mobile apps regularly for these common flaws and then fix them... preferably before deployment, but even in production is better than taking no action.



Yeah Joe, make sure that your buffers don't flow over onto your algorithms.

OK, we should security test our mobile portfolio, I'll grant you that. But are you going to let JW off the hook that easy?



www.dbooks.org

No, but with end users it's all in the approach, Joe IT. It's too easy to throw your hands up and say that they just don't care. Watch this.

JW, if we asked you...

- ✓ Would you want to have your email stolen or your contacts pillaged?
- ✓ Would you knowingly hand over your personal info to an identity thief?
- ✓ Would you intend to give private financial data to a criminal?

Would you...

Argh!

Make it stop! Of course I wouldn't choose any of those things!



So speaking as a mobile user, you want to keep your confidential data safe? Guess what, all users do. No one goes on vacation and leaves their front door unlocked and the windows open. If you were robbed as a result of this oversight, folks would say you got what you deserved. It's time to start protecting our smartphones just like we all learned a decade ago to protect our laptop and PCs from online threats. One look at the sobering facts on rising mobile attacks may have convinced some readers. Making it an easy checklist next might convince others, if you know what I mean...

I do know one thing about JW. He's a gadget guru. Maybe he'd actually like discovering some of the cool security features of his smartphone. Maybe we can help him become a mobile power user?



Oooo, a **power user**. Now yer talkin, Joe! I'm into anything that will extend my control and assert my dominance. Kneel before me!



I meant becoming an authority on good mobile security practices, someone I can partner with to make the organization more secure. I fear we are creating a monster here…



JW, let's give you the power to secure your own mobile device. We've developed a checklist of **10 quick things** you can do today to develop these important skills, so let's get started...

www.dbooks.org

PART THREE

10 Ways to Secure Your Mobile Gadget



Share this:

So now that you guys are seeing eye-to-eye

er... somewhat, it's time to review the **10 simple things** that every mobile user can do right now to secure their smartphone or other device from hackers and criminals.



Wait! Let me grab a pencil.

Security features come built into every mobile device, you just need to start using them. Now there are some differences between the major mobile platforms. Generally speaking, Apple's platform is delivered to users in a secure state with little guesswork necessary, while Google Android allows for more options with user control, but also greater user responsibility for mobile security. For the purposes of this discussion, let's just say "smartphone", but realize that we're talking about any mobile gadget such as a tablet.

Most of these protections can be implemented with zero to little impact on your smartphone's performance. This is how they break down:

- ✓ **4** of the tips cover settings on your device
- ✓ **4** of the tips are safe behaviors to adopt
- ✓ **2** of the tips require additional software for your device



I'm more than happy to help JW set up any of these, especially those last couple.

www.dbooks.org

Tip 1 Use Password Protected Access Controls

All mobile devices come with the ability to set a lock requiring a passcode or pattern for access. Yet it's amazing how some mobile users don't employ even this basic safety feature! It may take you a couple extra seconds to unlock your smartphone before using it, but it could take a thief a very long time to figure out your PIN. Phones that aren't locked lay bare a treasure trove of personal information – email, contacts, addresses and access to social networks and apps that may contain financial data.

If you are already using an **access PIN,** hopefully you have picked one that's easy to remember but hard for others to guess – so not your street address or child's name. The strongest passwords are a combination of numbers and letters, and the longer the better.





Try to pick an association that only you would know, and that won't be personally identifiable with you. On most devices you can set the idle interval you want the phone to wait before it locks, that way it's not shutting you out all the time when not in use.

PINs aren't the only locking mechanisms in use. Grid-based **pattern locks** work fine, but they leave smudge marks on the touchscreen that may be easier to guess than passwords. Some devices are rolling out **facial recognition** as an access mechanism, but this technology isn't perfected yet so it's not recommended.

Newer phones now offer full **device encryption** for the file system itself. Apple's is built in, but Android requires users to enter yet another passcode which, if forgotten, can accidentally wipe all your data. Many tablets also provide locking mechanisms for USB file sharing (such as syncing files with a PC), so set those PINs as well so a stranger can't just walk up and plug in. And remember that encrypted data on your mobile device may no longer be encrypted when transferred to your PC.

Check! I'll be sure to use password access from now on. Don't want my kids playing games on my phone when I'm not around!



Not to mention your mobile contains a lot of sensitive and confidential info about our organization, JW.



Um, yeah, that too.



We don't have the space here to cover all screen and key lock options and exactly how to set them on your particular device. Refer to your user manual, or start by looking in the general settings to locate these functions. For most users however, basic access controls should be enough.

www.dbooks.org

Tip 2

Control Wireless Network & Service Connectivity

Your mobile device is primarily a communications tool, we understand that. It connects you to all of the information you can ask for. But did you know that your smartphone's default settings may be connecting to nearby Wi-Fi networks automatically? Especially if you've asked it to download new email as it arrives.

Some of these networks, like in airports or neighborhood coffee shops, may be completely open and insecure. Did you know that hackers have demonstrated the ability to sit in a public place and "sniff" out information transmitted by connected mobile devices nearby?



Yikes! I hadn't thought of that. Do I need to keep my eye out for suspicious girls with dragon tattoos!?!

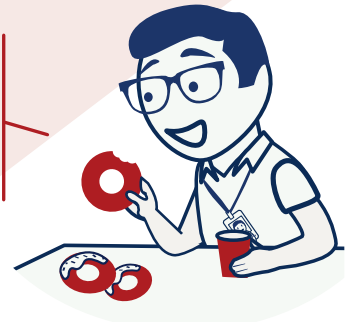


It's probably time better spent to set wireless options to manually connect.

Joe's right. **Turn Wi-Fi off completely** and turn it on only when you need it, which will also save your battery power. If you leave it on to connect automatically, all the time, your phone will be connecting to any available network to keep location-based services working, constantly syncing your email, and supporting other services you may not even want or need at that time.

It's safest to set your phone to automatically connect only to your trusted networks, and to ask you before connecting to any other network it finds. The general rule is to limit your phone's automatic connection capabilities to just the networks that you know, trust and use most often – like your office, home and gym.

It's been a while since I've been to that gym. I check my email at the neighborhood donut shop most mornings. Yum.



If your phone has **Bluetooth support**, it's also best to select this feature manually as well. Nearby attackers could potentially exploit Bluetooth to access data on your phone. Bluetooth settings work like Wi-Fi on most phones – it can be either on or off, so we recommend making your smartphone discoverable to other Bluetooth only when necessary.

www.dbooks.org

Tip 3

Control Application Access & Permissions

Apps are wonderful things, but many of them store sensitive data that must be protected. Android users can take advantage of their mobile phones' multitasking capability by employing a special access control app. Most will start up when your smartphone boots and run in the background. These apps further restrict a thief or hacker's access to your device.





More important than controlling app access is policing app permissions. Most of today's apps require a network connection to operate. They may store data in the cloud, constantly track your location, or push updates to your smartphone. Get to know the permission settings of each app or service and what data or systems they access. You may be permitting services to access your phone without prior approval, or your apps may be pushing alerts and updates when you aren't specifically requesting them. You can restrict all notifications at once by looking under your device's settings.





On many devices you can turn off location based services entirely as well, so your phone isn't constantly broadcasting your GPS location, no matter which apps request it.



Keep Your OS & Firmware Current

Here's another tip that's a no-brainer. The threats to mobile security are only growing in number and sophistication. Your device has an operating system that runs all of its apps and services, as well as firmware which runs the device hardware itself. It's definitely important that you routinely accept the major updates from Apple, Google, or whoever the manufacturer is.

Criminals are innovating their attacks at an alarming rate, with growing sophistication. Connect often and download security patches and other minor updates that are released expressly to block the latest hacker scheme or exploit. Most of these updates will be free of charge. No manufacturer wants a major attack to cripple its users, so they have a vested interest in helping you stay up-to-date.



Equipment does "age out", rendering older devices unable to run the latest OS version. Unfortunately, there is a huge population of Android users currently using outdated firmware and OS versions that can't be updated due to hardware incompatibility. Take advantage of the chance to upgrade your device every couple years, if and when promotions are offered by your carrier.

www.dbooks.org



Back Up Your Data

It's amazing that this far into the personal computing age, most users still don't copy their critical info to ease data recovery in case of theft or loss.

Tsk, tsk, tsk…I've been backing up my stuff since floppy disks were cool.



Start to think of your phone like you do your PC or laptop. Maybe you back up your computer data locally, or use a company approved cloud-based backup service? That's great. Why wouldn't you want to protect your phone as well? Take the time to sync all of your apps and data – not just your email and calendar – just in case your phone becomes lost, stolen or corrupted.



Good idea.
Plus I'd be heartbroken if I lost all the funny videos of my cat, Mr. Peepers.



Depending on how much you use your phone, you may want to take a data backup daily or weekly, but certainly once a month. There are commercial backup services for mobile devices as well, but most users find that the standard data sync functions cover their basic needs.

Tip 6

Wipe Data Automatically if Lost or Stolen

It's a good idea to enroll your smartphone in a **"find my phone" service** that will help you locate your device should it be lost or stolen. These services typically have the ability to wipe your phone, which means remotely erase all data and completely disable the device should it fall into the wrong hands. If you are using a company smartphone, your IT group probably offers these services.



It's going to turn my phone back into a brick phone from the 80s?

Well, just about as functional, yes.



On some devices you can add extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts – a good idea as most PINs can eventually be brute forced. Finally, this may be apparent, but many people don't even think about removing sensitive data before selling their smartphone or sending it in for repairs.

I'm here to help. Now you see why data backup is so important?



www.dbooks.org



Never Store Personal Financial Data on Your Device

As a behavior that all mobile users should adopt, this one is pretty straightforward. Never store personally identifiable information such as such as Social Security Numbers, credit card numbers, or checking account numbers on your smartphone, especially in text messages.

If you currently use any online banking or online payments software, it shouldn't require this information to authenticate your identity. The best way to protect your organization's business data is to remove it from the device completely. The best rule of thumb is to access sensitive and confidential data directly on the server, and only ever from an approved and authorized mobile device.





Beware of Free Apps

Maybe this advice sounds a bit harsh, but we got your attention, right? Listen, there are lots of great free apps out there, many are well reviewed and are being enjoyed securely by millions of mobile users right now.

Yeah, like those furious fowl who love to demolish swine!



The problem is, more and more free and innocent apps are trying to make money from their offerings, so sometimes they track your personal information with limited disclosure or authorization, then sell your profile to advertising companies. The app developers in question may not even be aware of their privacy violations – leaking your location, gender, age and other personal data to embedded mobile ad networks while in the pursuit of revenue.



Why is that fun-looking game asking to be able to place calls? Maybe to add hundreds of dollars to your bill ringing premium rate numbers!

Caution is key. Be sure to read the reviews and download only from reputable publishers. As we've pointed out, look closely at the permissions that the app is requesting. More and more free apps are just wrappers for malware, unfortunately. When you log into mobile banking that innocent app might capture your credentials then call the criminals up to pass them the data.

Sometimes free simply means too good to be true.

www.dbooks.org



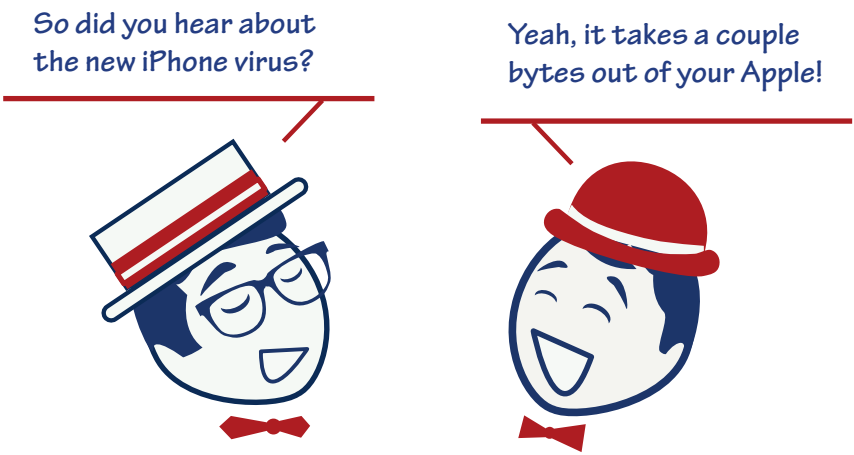
Try Mobile Antivirus Software or Scanning Tools

Without active virus scanning and updated malware definitions on your mobile device, it could already be infected with spyware and you may not even know it. Good news is the well-known PC antivirus vendors are now offering similar services to mobile users that scan and protect your smartphone just as they did your desktop. They can point out problems in your settings and instruct you how to correct them. Some even offer additional mobile security services such as download protection, SMS/call-screening services, parental controls, and anti-phishing features.

The publisher of this booklet, application security company Veracode, offers a free scanning tool named **Addressbook Detector for iOS (aka AdiOS)**
It will quickly and easily find all the apps on your iPhone or iPad that have the potential to violate your privacy by accessing your entire address book.

Download AdiOs here

Today's antivirus packages do require quite a bit of memory to run, and its best to plug them in during the lengthy scanning process. But they are definitely worth a look, especially if you are engaging in high-risk activities like mobile banking or mobile payment services. Stick to the best-known commercial vendors and you'll minimize your risk.



Just remember that when it comes to the level of security built in to your favorite app – that is how it handles sensitive data and its immunity to hacks and attacks – you shouldn't blindly trust your favorite app store. The security and privacy levels of the apps they sell are not tested prior to acceptance; this is left up to each app developer to certify.

www.dbooks.org

Tip 10

Use MDM Software, if Recommended by IT

Mobile Device Management, or MDM is being increasingly employed by IT departments to secure, manage and support all mobile devices that are authorized to access enterprise networks. These services control and protect sensitive and confidential business data by distributing mobile application or configuration settings to company-owned equipment as well as employee-owned.

Whoa, you lost me after "MDM is…"



Here's the bottom line: Enroll your mobile device in a managed environment, if your organization offers one. This will only help you as an authorized user to configure and maintain the right mobile security and privacy settings. The goal of MDM is to optimize the functionality and security of your mobile computing experience, not to impede the way you like to work.



So if you enroll your iPad into our MDM program, JW, you can bring it to the office with you!

If your organization doesn't offer MDM, there are other options provided natively on many devices that accomplish similar ends. SIM card locks and credential storage functions protect the phone by requiring a passcode to use network-dependent services, and operate similar to screen/key access PINs.

SIM locks prevent anyone from making unauthorized calls with your smartphone, or from removing your SIM and using it in another phone. Secure credential storage protects authentication certificates such as the one required to access your organization's Virtual Private Network (VPN), keeping login info out of sight of prying eyes.



www.dbooks.org

One last thing, Joe.

It's still up to IT professionals to make mobile security as invisible to enterprise users as possible. The more you can do to harden the organization's sanctioned mobile devices before distributing them, the better. You have to security test your mobile apps before folks like JW download or install them. It's also good to provide a whitelist of applications that are safe and approved for use. IT pros must proactively implement mobile security best practices on behalf of our new power users!

This was actually kinda fun for me, in a power user sort of way. Now that I've got all these recommendations completed, am I free to roam?

Hang on now, ROAMING is a whole different subject. In fact we need to review your last expense report…

There you go again, Joe! Just when I thought we understood each other…

Who told you it was cool to bring your iPad with you to Mumbai? You need to…



Sigh. We may never get Joe and JW to see eye-to-eye on everything, but when it comes to mobile security, it pays to remember that we're in this together. It doesn't matter if you prefer an iPhone, Android, BlackBerry, iPad or Windows Mobile device. Anyone can be a mobile power user, and all it takes is **10 easy steps**. Now go forth and assert your mobile security dominance!

www.dbooks.org

References

[1] Study by Software Advice, Inc.

[2] IDC Research, Worldwide Mobile Phone Tracker, Q1 2012

[3] Comscore, 2012 Mobile Future in Focus, February 2012

[4] IDC Research, Worldwide Mobile Phone Tracker, Q1 2012

[5]The Brookings Institute, 10 Facts about Mobile Broadband, 8 December 2011

[6] Ponemon Institute, Global Study on Mobility Risks, February 2012

[7] Verizon, 2012 Data Breach Investigations Report

[8] Ponemon; 2011 Cost of a Data Breach

[9] BusinessWeek: Global Payments Trades Halt on Breach Probe, 30 March 2012

[10] Data Loss Database

[11] Juniper Networks: Mobile Security Report 2011, February 2012

[12] Veracode, State of Software Security Report vol. 4

VERACODE

Want to Have Us Present the Top 10 Mobile Security Tips to your Employees?

We can make that happen - at no cost to you!

If you can get 250 employees together we'll come to your site for a 90 minute mobile security seminar. Your employees will leave the seminar with a clear understanding of today's mobile computing threats and be able to take action to protect your company against those threats.

If getting 250 staffers together in one place at one time is tough, we're happy to present at an online webinar – that way everyone can dial in from their desks.

To let us know you'd like to host an onsite seminar or an online webinar visit info.veracode.com/mobile-security-ebook-coupon and we'll get it on the calendar.

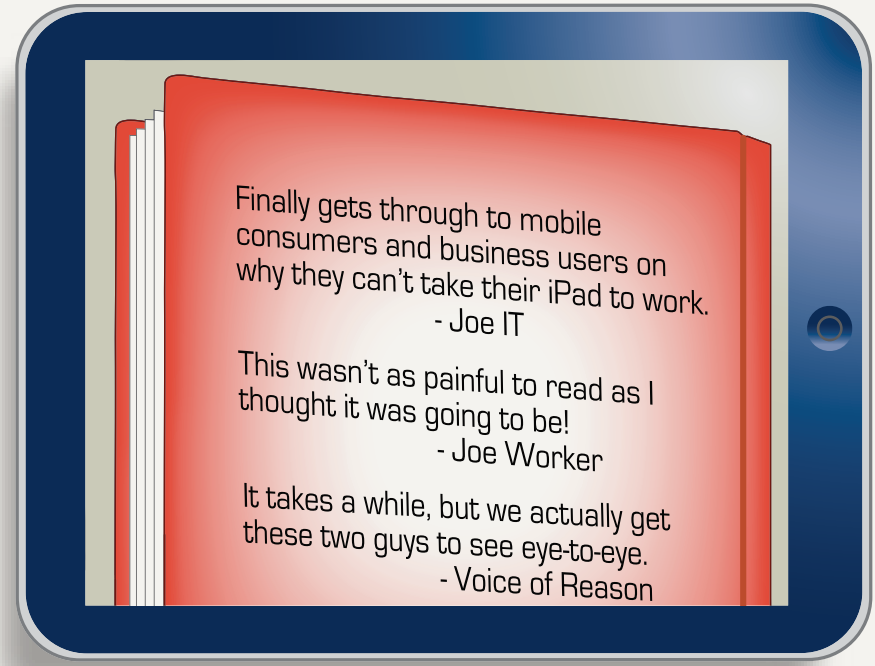
Bonus Offer!

Get one **FREE** Android mobile application security scan when your organization hosts an onsite seminar or online webinar

About Veracode

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. Veracode is the only application security company that supports iOS, Android, BlackBerry and Windows Mobile.

www.dbooks.org



Brought to you by:

VERACODE

Securing the Software That Runs the World

Share this:

Contact us: 1-888-937-0329
info@veracode.com