McAfee®
An Intel Company

10 QUICK TIPS TO MOBILE SECURITY

10 Quick Tips to Mobile Security

CONTENTS

INTRODUCTION

32% OF PEOPLE BELIEVE THAT THEY DON'T NEED SECURITY SOFTWARE FOR THEIR MOBILE DEVICES

There's no doubt about it—mobile devices have become man's new best friend. If you don't believe it, consider that there are currently more than 4 billion[1] mobile phones in use worldwide among 7 billion people, not to mention millions of tablets. We use our devices to stay in touch, take pictures, shop, bank, listen to music, and socialise. We store personal and professional information on them, and because we use them for almost everything, they have both a high financial and emotional value.

Losing your smartphone or tablet, or the information on it, can be a hassle. If you lose your mobile device, you not only have to replace it, but you could also lose the sensitive information you had stored on it, including account numbers and confidential work information. So, why do so many of us leave our mobile devices unprotected and not use mobile security?

Most of us now understand that we need to protect our computers from the myriad of threats that we see each day. But many of us don't realise that we face the same threats, as well as a host of new ones with our mobile devices. In fact, 32% of people believe that they don't need security software for their mobile devices.[2]

[1] http://mashable.com/2011/03/23/mobile-by-the-numbers-infographic/
[2] McAfee Digital Assets Survey, 2011

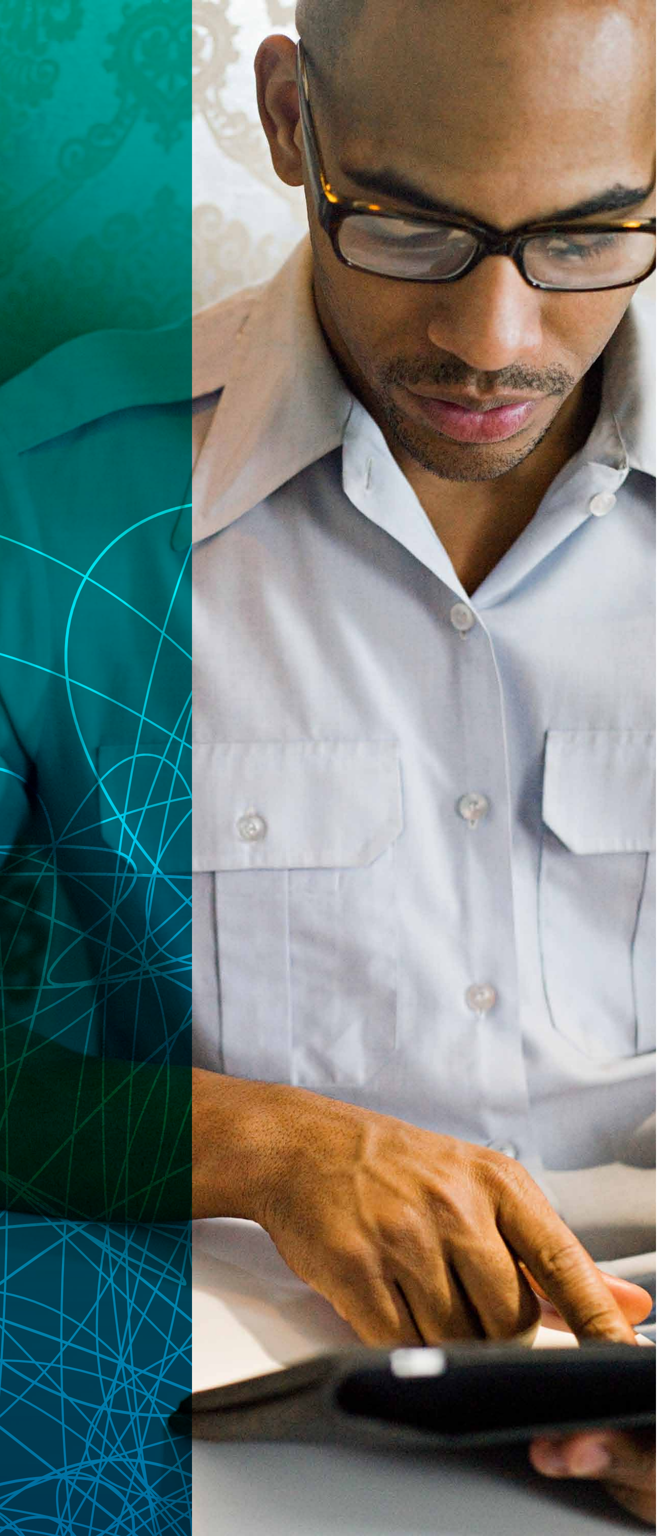
MOBILE MALWARE TARGETED AT ANDROID DEVICES HAS INCREASED BY NEARLY 37% OVER THE PAST SEVERAL MONTHS

For one thing, the growing popularity of mobile devices has led cybercriminals to see them as a new avenue for attack. Mobile malware targeted at Android devices has increased by nearly 37% over the past several months.[3]

Even though we think of mobile devices as our phones or tablets, they are really mini-computers that can be more vulnerable than the ones sitting on our desks.

So, as a mobile user, keep in mind that you need to learn how to protect yourself from a variety of threats. Here are just a few to consider:

[3] McAfee Threats Report: Third Quarter 2011



MOBILE THREATS AND CONSEQUENCES

THREATS	DANGERS
Device loss or theft	• Loss of sensitive personal and employer information such as contacts, calendars and photos • Breach of your privacy, and in a worst-case scenario, you could become a victim of identity theft • Compromised online accounts • Payment to replace the device, and/or possible calls or texts charged to your account
Phishing scams (often delivered via emails, texts and social networking sites)	• Sensitive information revealed such as account numbers and login credentials • Unauthorised withdrawals made from your bank account
Malware and spyware	• Compromised personal information—you could even become a victim of identity theft • Unauthorised charges could appear on your mobile bill • Others may listen in on your phone calls and retrieve your voicemails
Quick Response (QR) codes	• You could accidentally download a malicious application • Your personal information could be compromised, or your device could cease to function properly
Wi-Fi networks	• You could connect to an unsecured network, and the data you send, including sensitive information such as passwords and account numbers, could potentially be intercepted

IMPORTANT MOBILE STATISTICS

50% OF SMARTPHONE USERS DO NOT USE ANY PASSWORD PROTECTION

If you're still not convinced that your phone needs protection, consider these statistics:

- People are 15 times more likely to lose a mobile phone than a laptop, making loss the biggest threat to mobile users.[4]
- Consumers on average store "digital assets" they value to be worth £24,875[5] in their devices, including digital media, professional information, personal correspondence and photos—yet more than a third lack protection across all of those devices.
- By 2014, mobile Internet use is expected to take over desktop Internet use,[6] which could make mobile devices even more attractive to scammers and cybercriminals.
- 44% of adults are afraid to use their phone as a mobile wallet due to the lack of security software,[7] making it critical that consumers know how to shop safely from their mobile devices.
- By 2015 there are expected to be 500 million mobile banking users worldwide,[8] making mobile banking safety a top concern.
- Mobile malware aimed at the Android platform alone grew 400% in the six months between June 2010 and January 2011,[9] and no platform is immune.
- 40% of consumers say losing their mobile devices would be worse than losing their wallets,[10] yet they often leave them unsupervised or unprotected.
- More than 50% of smartphone users do not use any password protection to prevent unauthorised access to their device.[11]

[4] http://www.mcafee.com/us/about/news/2011/q1/20110216-03.aspx

[5] McAfee Digital Assets Survey, 2011

[6] http://mashable.com/2011/03/23/mobile-by-the-numbers-infogrpahic/

[7] http://www.bgr.com/2011/10/18/just-17-of-u-k-consumers-would-use-their-phone-as-a-mobile-wallet-study-reveals/

[8] Yankee Group, June 2011

[9] Juniper Networks

[10] "The Rise of Smartphones and Related Security Issues", April 2011

[11] *The Wall Street Journal,* "Google Mail Hack Blamed on China", June 2011

TOP 10 MOBILE SAFETY TIPS

Considering how much we rely on our mobile devices, and how much opportunity the cybercriminals have to launch attacks against them, you'll want to make sure you are protected. Follow these simple tips:

1 LOCK YOUR DEVICE WITH A PERSONAL IDENTIFICATION NUMBER (PIN) OR PASSWORD

This is how you can prevent unauthorised access. Also, configure your device to automatically lock after a certain period of time.

Even after your device is password-protected, never leave it unattended in public—lost and stolen devices continue to be the number-one threat to mobile users.

2 ONLY INSTALL APPLICATIONS (APPS) FROM TRUSTED SOURCES

- Shop at reputable app stores—Before downloading an app, research the app and its publishers. If you are an Android user, avoid installing non-market applications by de-selecting the "unknown sources" option in your device's Applications Settings menu.
- Check other users' reviews and ratings to see if an application is safe.
- Read the app's privacy policy—Check to see how much of your data the app accesses and if it will share your information with third parties, if there is a privacy policy. For example, if a game application requests access to your address book, you should ask yourself why it would need that access. If you are at all suspicious or uncomfortable, don't download the app.

3 BACK UP YOUR DATA

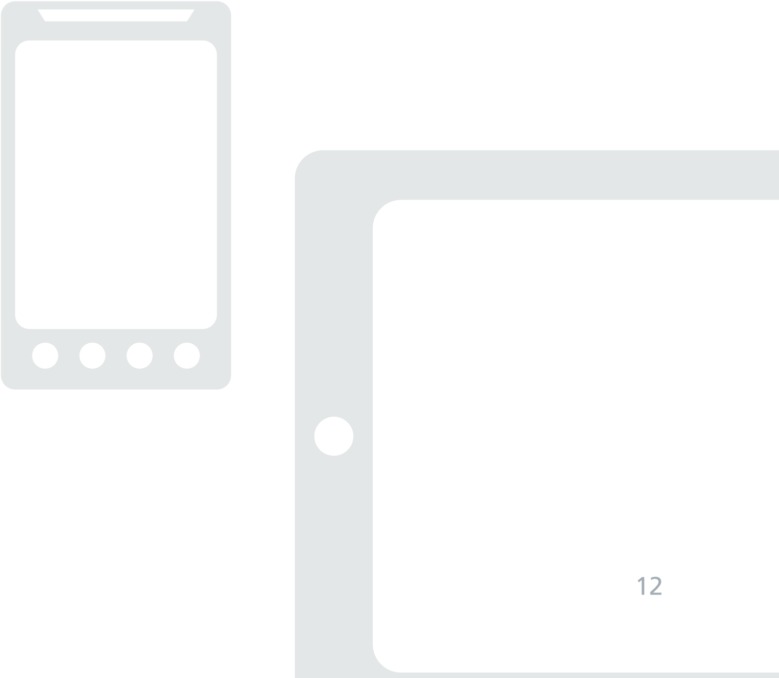
It is relatively easy to do, and many smartphones and tablets have the capability to backup data wirelessly, so you can quickly restore the information on your phone if the data is lost or accidentally deleted. And, if you lose your device, you will still be able to retrieve your information.

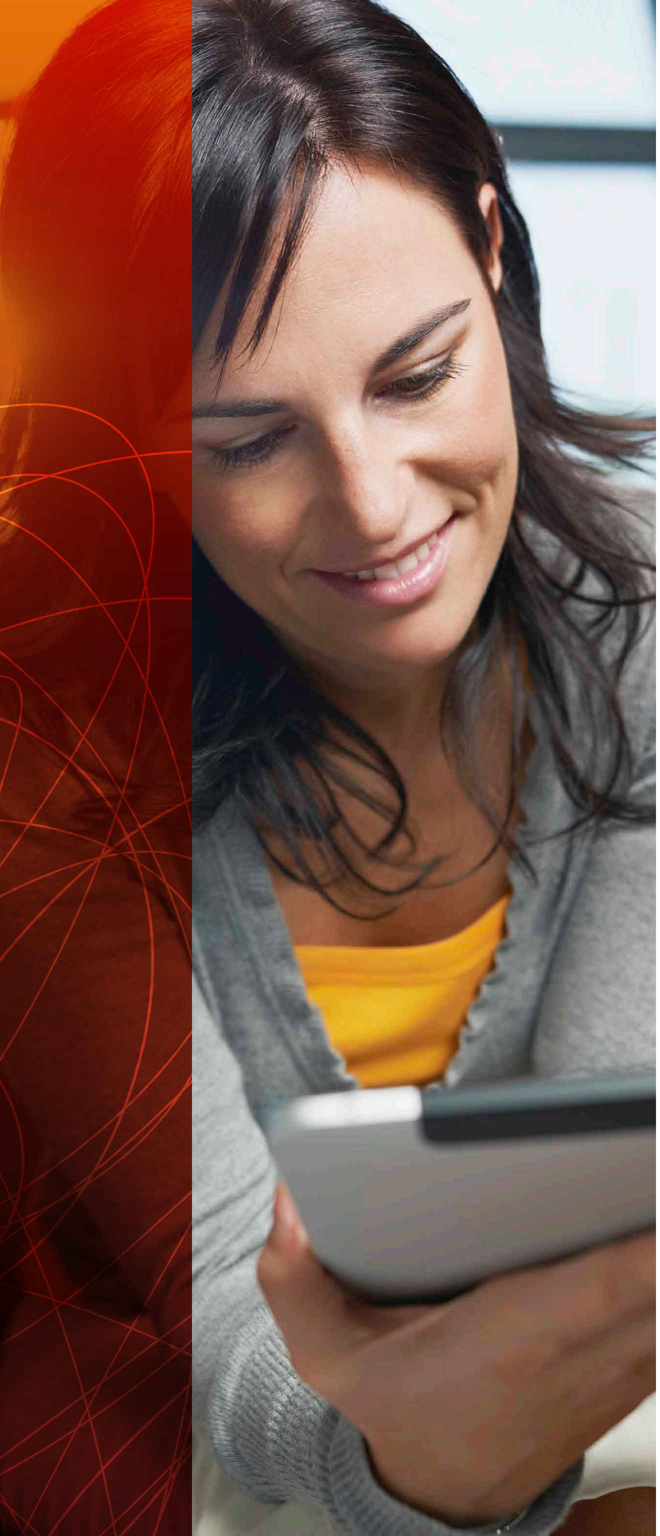
4 KEEP YOUR SYSTEM UPDATED

Download software updates for your mobile device’s operating system when prompted. This way, you’ll always have the latest security updates and you'll ensure that your device is always performing at an optimal level.

5 DON’T HACK YOUR DEVICE

Hacking, or tampering with your own device to free it from the limitations set by a provider, can significantly weaken the security of your device. By hacking your device, you can potentially open security holes that may have not been readily apparent, or undermine the device’s built-in security measures.





6 ALWAYS LOG OUT OF BANKING AND SHOPPING SITES

- Log out of sites instead of closing the browser—If your phone or tablet is lost or stolen, a thief can potentially log in to your accounts. Also, never save usernames and passwords in your mobile browser or apps, just in case your device falls into the wrong hands.
- Don't bank or shop online from public Wi-Fi connections—It's best to save your sensitive transactions, such as online banking for when you're on a network that has security measures in place.
- Double-check the site URL—Make sure that the web address is correct before logging in or sending any sensitive information. You may want to download your bank's official app so that you know you're going to the right website every time.

7 TURN OFF WI-FI, LOCATION SERVICES, AND BLUETOOTH WHEN THEY ARE NOT IN USE

- Turn off Wi-Fi if you’re not using it—Cybercriminals and identity thieves can easily access your information without your knowledge if the connection is not secure. One way to stay safe is to limit your use of hotspots. When you’re away from your home or work network, use a 3G or 4G data connection instead since most mobile phone providers encrypt the traffic between cell towers and your device.
- Turn off apps that use location services—You may not realise it, but some mobile service providers store this information and it could be shared, leaked, or used to push ads to you.[12]

[12] http://www.itstactical.com/digicom/privacy/data-leaks-location-based-services-and-why-you-should-be-concerned/

- Bluetooth should be turned off when you don't need it—Many devices are preset to use default settings that allow other users to connect to your device, sometimes without your knowledge. This means malicious users can potentially access your device and copy files, or gain access to another device attached to your Bluetooth device.

8 AVOID TEXTING OR EMAILING PERSONAL INFORMATION

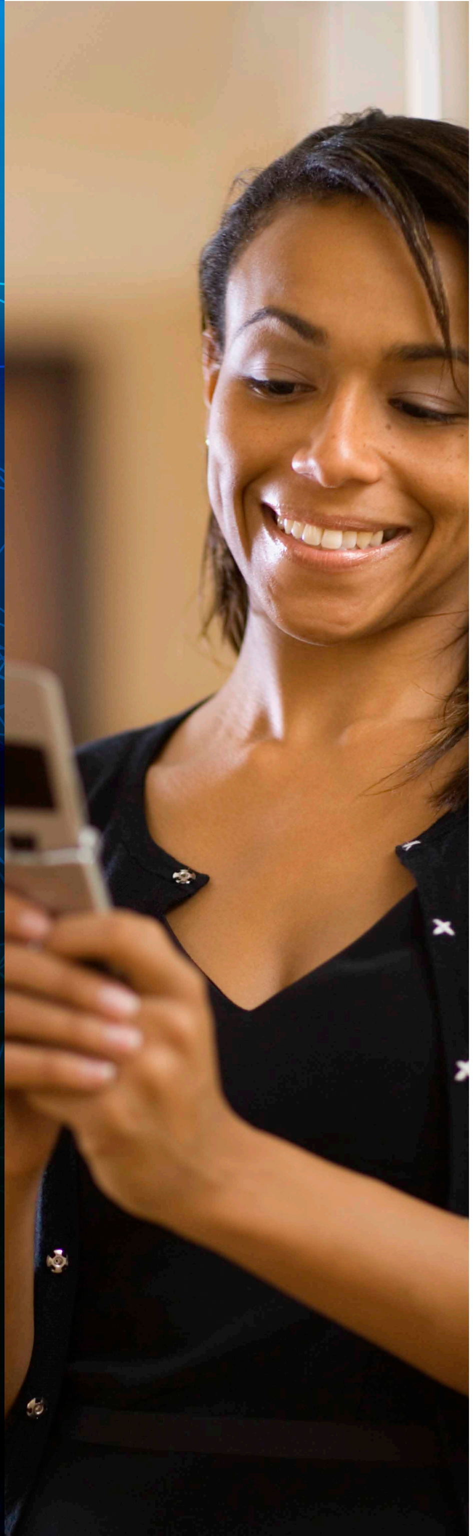
Even if you receive a text that appears to be from your bank or another legitimate business, never respond with personal information. Instead, contact the business directly to confirm their request.

And even though it may be tempting to store important information on your phone, remember that your device can easily be lost or stolen and your personal information, including passwords and banking information, could fall into the hands of the bad guys.

9 DON'T CLICK ON LINKS OR ATTACHMENTS IN UNSOLICITED EMAILS OR TEXT MESSAGES

Remember to use your Internet best practices, and be wary of links in unsolicited email or text messages (both SMS and MMS). Our best advice is to delete unsolicited messages as soon as you receive them.

Also, be wary of shortened URLs and QR codes—they could lead you to dangerous websites. Use a URL preview site, such as LongURL, to check to see if the web address looks legitimate before visiting it. If you plan to scan QR codes, select a QR reader that offers a preview of the code's embedded web address, and use mobile security software that warns you of risky links in QR codes.

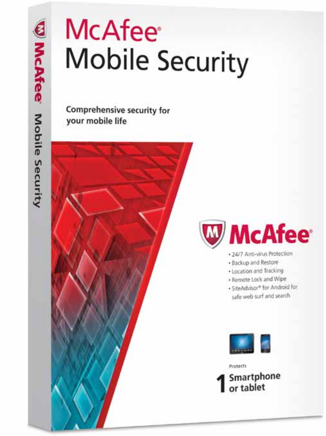


10 INSTALL A MOBILE SECURITY APP

Make sure that you have mobile antivirus protection that can catch existing and emerging mobile threats, and keep your software updated. This way, no matter what the bad guys have up their sleeves, you can keep your information and device safe.

RESOURCES

MOBILE SECURITY



Available for Android smartphones and tablets as well as BlackBerry and Symbian smartphones.

When it comes to the complex world of mobile threats, your best defence is security software that offers several layers of protection, such as McAfee Mobile Security.™

McAfee Mobile Security offers:

- **Complete antivirus, antispyware, and antiphishing**—Scan and clean malicious code from inbound or outbound emails, text messages, attachments, and files.
- **Safe searching and shopping**—Protection from risky links within texts, email, and social networking sites, as well as browser exploits and malicious QR codes.
- **App protection with App Alert**—Review a report on your app's access to your personal data so you can make informed decisions about each app.
- **Device lock**—Protect against misuse of your phone and personal data by remotely locking all data, including the data on your memory (SIM) card.
- **Remotely wipe data**—Protect your privacy by remotely deleting the data on your phone and removable memory card.
- **Backup and restore data**—Preserve irreplaceable personal information on demand, on a schedule, or before you wipe your missing smartphone; then restore your information to your new device.
- **Locate and track**—Recover your smartphone if it is lost or stolen. View its location on a map, send a text to prompt its return, and use a remote alarm to make it "scream."
- **Call and text filtering**—Easily filter out spam, incorrect names, and unwanted texts.
- **Uninstall protection**—Keep a thief or another user from bypassing your McAfee mobile protection.

Try McAfee Mobile Security for free.

OTHER RESOURCES

Mobile Security Advice
http://home.mcafee.com/AdviceCenter/Default.aspx?id=ad_ms

Safety Tips for BlackBerry Devices
http://us.blackberry.com/business/topics/security/

Tips to Protect Your Android Phone
http://www.cio.com/article/675129/Android_Security_Six_Tips_to_Protect_Your_Google_Phone

Google Good to Know
http://www.google.com/goodtoknow/online-safety/mobile-security/

National Center for Missing and Exploited Children
http://www.netsmartz.org/CellPhones

Consumer Action Mobile Transaction Tips
http://www.consumer-action.org/english/articles/your_digital_dollars-safety_and_privacy_in_online_and_mobile_transactions/

IN SUMMARY

The explosion of Internet-enabled mobile devices has delivered productivity and flexibility gains that we have never realised before. However, they have also given hackers and scammers unprecedented opportunities to target your personal data. Protect yourself by following the safety tips listed in this guide, and stay educated about emerging threats. By investing a little bit of time and effort, you can enjoy all the fun and convenience that mobile devices offer while safeguarding your privacy, identity, and bank account.

For more information and advice about mobile security, please visit the McAfee Security Advice Center.

About McAfee

McAfee, A wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security company. Since our founding in 1987, we have had just one mission: to help our customers stay safe. We achieve this by creating proactive security solutions for securing your digital world.

Through our vigilance, we allow consumers and companies to work, play and shop online more securely, no matter where they are or how they connect. McAfee is relentlessly focused on finding new ways to keep our customers safe.

http://www.mcafee.com

McAfee®
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
1.866.622.3911
home.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.