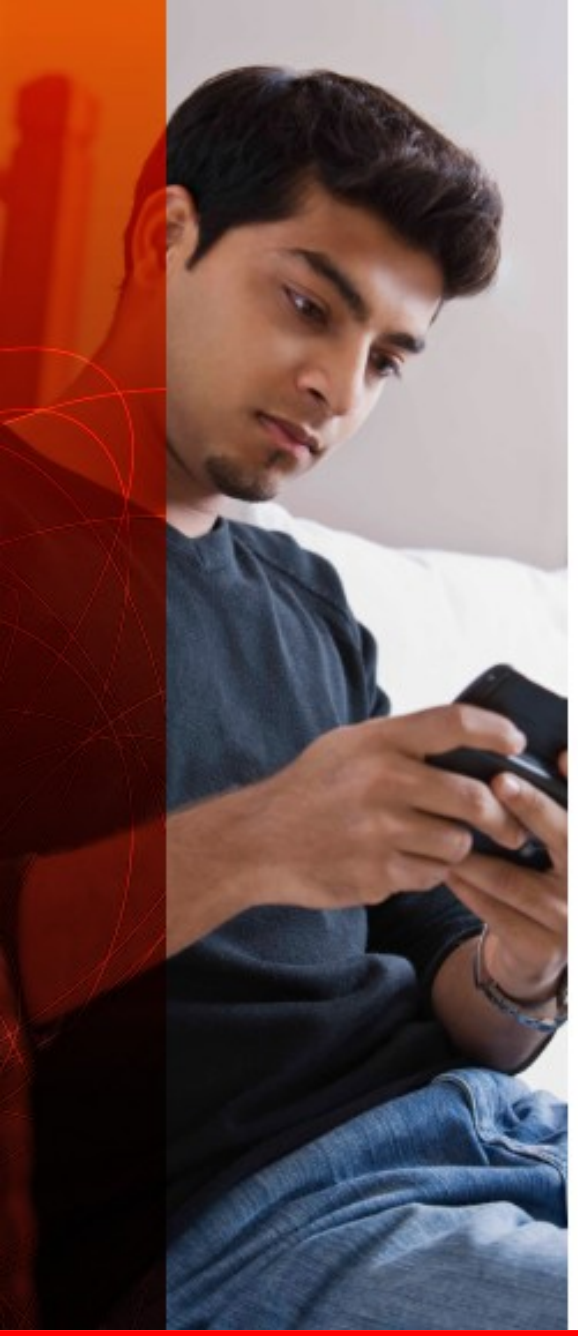
Mobile Security Awareness

MOBILE THREATS AND CONSEQUENCES

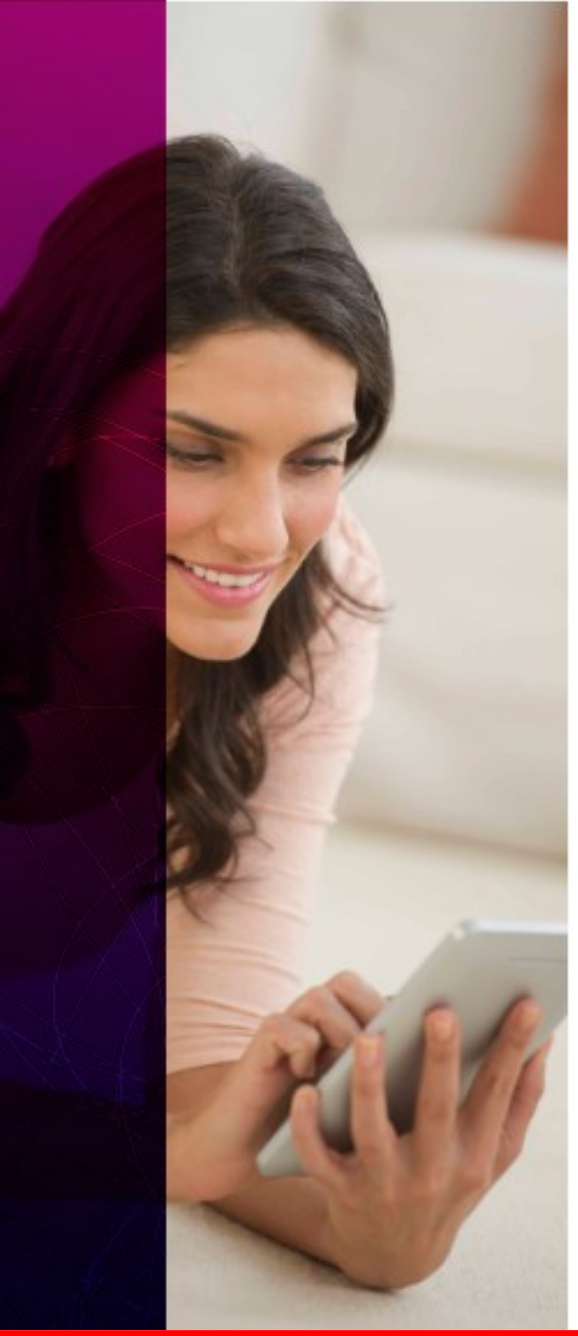
THREATS	DANGERS
Device loss or theft	• Loss of sensitive personal and employer information such as contacts, calendars and photos • Breach of your privacy, and in a worst-case scenario, you could become a victim of identity theft • Compromised online accounts • Payment to replace the device, and/or possible 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 • Unauthorized withdrawals made from your bank account
Malware and spyware	• Compromised personal information—you could even become a victim of identity theft • Unauthorized 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



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

This is how you can prevent unauthorized 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.

Google Play

Microsoft® Store

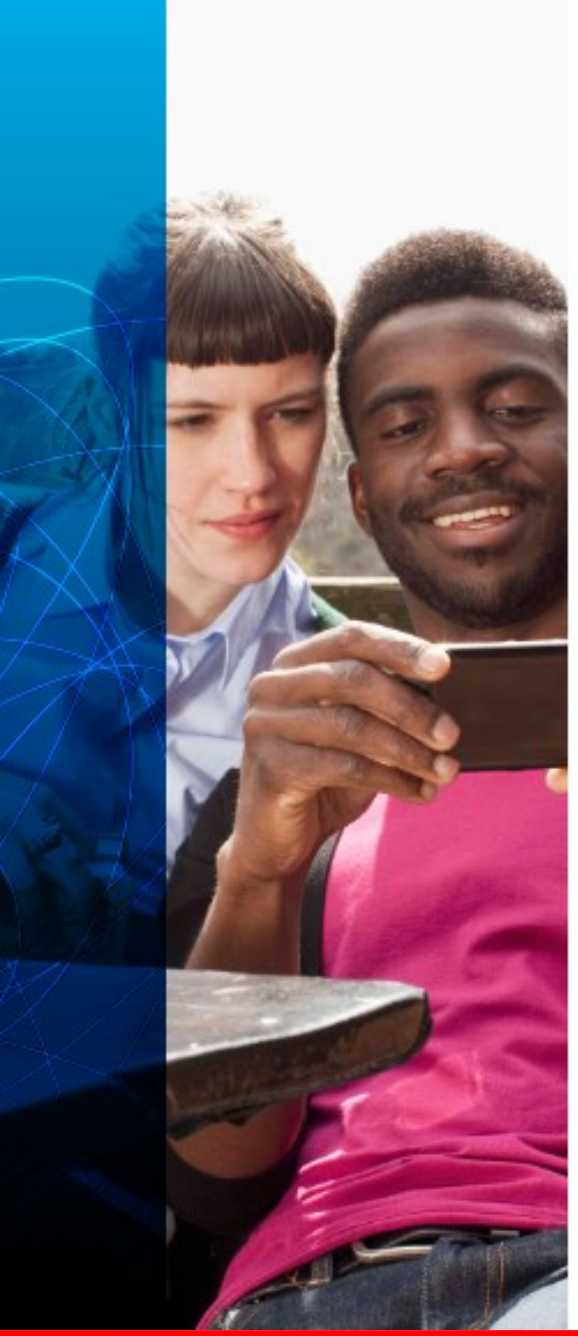
3 BACK UP YOUR DATA

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 ensure that your device is always performing at an optimal level.

iOS 11.0.3
Apple Inc.
276.6 MB

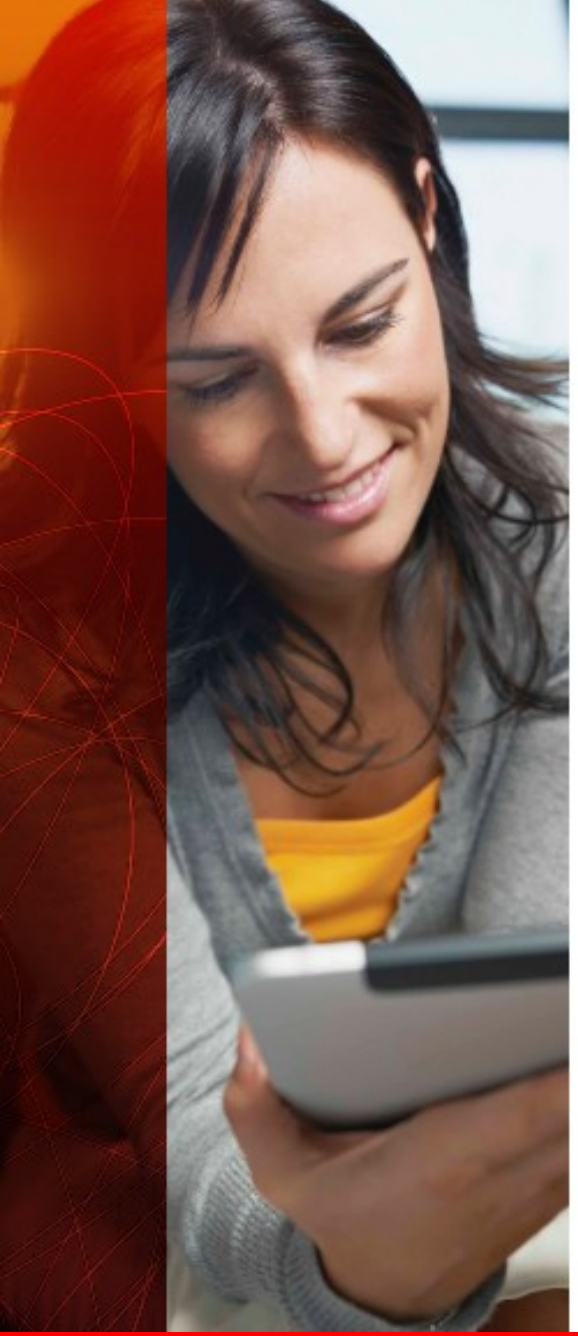


5 DON'T HACK YOUR DEVICE

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.

10

Jailbreak



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 realize 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.

Bluetooth®

AirDrop

8 AVOID TEXTING OR EMAILING PERSONAL INFORMATION

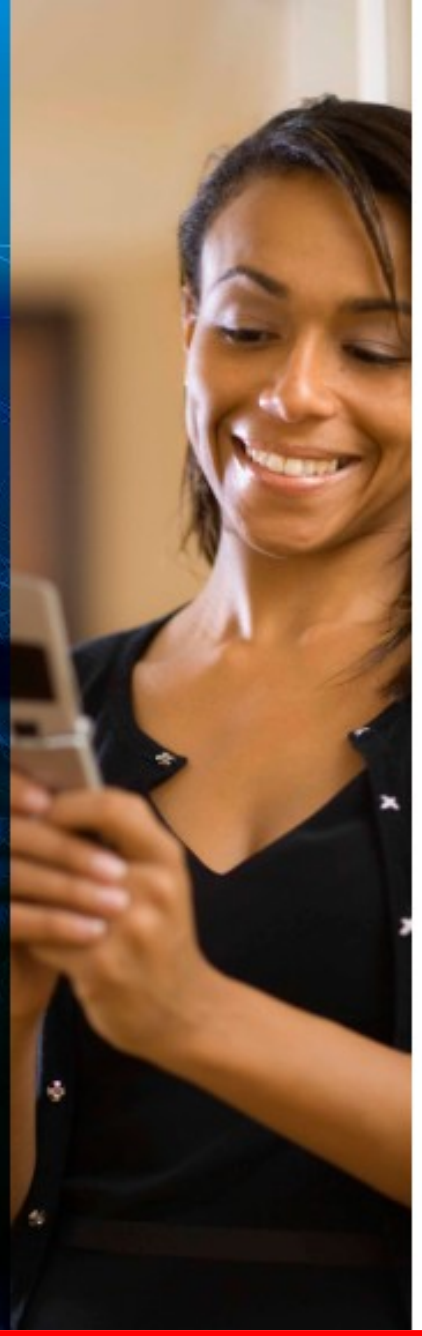
Even if you receive a text that appears to be from your bank or another legitimate business, never respond with personal information. Instead, contact the business directly to confirm their request.

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.

Sunilyadav

(CEO & Founder of Techspreading)

THANK YOU!