CONSUMER PRIVACY & IDENTITY QUARTERLY

VOL N°1 ISSUE N°3

DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:

SAFEGUARD YOUR SMARTPHONE WHEN TRAVELING ABROAD

Follow along with our step-by-step guide to secure your smartphone while on the road. You will never worry about losing important information if your phone is lost during your travels.

SECURE YOUR HOME WIFI WITH THESE SIMPLE STEPS & TIPS

Would you consider giving a stranger or a nosy neighbor keys to your house? The same concept applies to protecting your home network. Read this article for more information in securing your Wi-Fi.

ALSO INSIDE:

IMPLICIT DENY: WHAT TO LOOK OUT FOR IN MOBILE APP PERMISSIONS

SAFEGUARD: REMOVING EXIF DATA FROM YOUR MOBILE DEVICE'S PHOTOS

HOW TO SAFEGUARD YOUR SMARTPHONE WHEN TRAVELING ABROAD

Traveling with your smartphone opens many helpful possibilities—instant access to maps in unfamiliar terrains or a way to prep for unexpected inclement weather. However, traveling exposes your smart devices to added risks for loss or even worse, theft. Follow along with our step-by-step guide to secure your smartphone while on the road. You will never worry about losing important information if your phone is lost during your travels.

Your flight is booked and your luggage is packed. All items on the "before you travel" list are checked and you are ready to embark on the road, but your smartphone probably is not.

If you are like one-third of Americans, you do not have any security measures in place to safeguard your phone and all the valuable data it holds. And if you are like the other two-thirds, the steps you have taken to protect your phone may not be enough.

That can be an expensive oversight for the estimated 1 to 3 million Americans whose smartphones are stolen each year. Smartphones have become an indispensable part of our daily routine; we use them to store our favorite destinations, contact our friends and family, do work, and even sometimes pay for our groceries. Traveling with a smartphone means you are carrying passwords to your personal accounts, proprietary company documents, and sensitive banking information inside a small, easily pilfered device, which is itself worth hundreds of dollars. Even with "kill switches" that can disable a stolen or lost device, smartphones are still a top target for thieves. When traveling internationally, it is important that you take steps to guard your smartphone and stay a step ahead of the potential crooks.

Smartphones should be configured for traveling before you begin your trip. The best and most secure method would be to leave your personal smartphone at home and dedicate a loaner or backup device for traveling. Choose a smartphone with a removable battery and load it up with only the contacts and non-sensitive data and apps you need, for instance to look up nearby restaurants or search for directions. Do not root or jailbreak your smartphone as doing this can significantly reduce its security.

Whether you are using your personal or dedicated travel smartphone, equip your phone with a PIN code that is 6 digits or longer (and please, avoid using your birthdate or phone number), an alphanumeric password, or a complicated swipe pattern. Current smartphones may allow you to unlock via a fingerprint scan or facial recognition. In addition to these methods, make sure you set the phone to automatically lock after the shortest active usage time allowed. Lastly, do not save your passcode or swipe sequence as a reminder on the phone itself. This means anyone with access to your unlocked device can uncover your passcode.

A Subscriber Identity Module (SIM) card lock is an easy security tool to implement under any smartphone OS. This feature requires a PIN code that needs to be entered before a phone can connect to a network, keeping thieves from using your SIM card with another smartphone.

Continued on page 5...

Before you travel, delete any sensitive information that is unnecessary for travel needs. In a foreign country, your smartphone, much like a passport or ID card, may be subject to a forensic search, meaning you would have to provide authorities unfettered access to your personal device.

If you need to access documents that you would prefer foreign customs not access, store them in a cloud service, such as Google Drive, and access them as needed when connected to a Wi-Fi network. Log out and delete local copies on the phone when you are done.

In the latest versions of smartphone operating systems, Apple and Google both implemented whole-disk encryption, making stored data impossible to read without a passcode. If encryption is not enabled by default, turn it on.
Note: some foreign countries do not allow the use of encryption, so check applicable laws.

Some Android devices allow you to add removable storage, such as a secure digital (SD) card. Only use SD cards if they can be encrypted, as unencrypted SD card means your data can be even more easily removed and accessed by intruders.

You can keep any passwords you need in a password manager, such as Lastpass. Make sure your password app is accessible over the Internet. Password managers can store encrypted copies of your passwords and other information, such as passport and credit card numbers.

All major smartphone operating systems provide tracking software with the phone. You just need to set up or activate it before you begin your travels. For iPhone, use Find My iPhone. For Android, you can use Android Device Manager or third-party programs like Cerberus. They can remotely track, lock, or erase all data on the phone.

For greater protection, install an anti-virus app, such as AVG, and scan your device regularly during the trip. For Android users, go into phone settings and be sure the "Allow untrusted applications" box is not checked so that only apps registered on the official Google Play store can be downloaded and installed on your phone.

Your phone's lockscreen can reveal sensitive data and personal correspondences. Lock screens are often configured by default to display calls, texts, emails and even portions of messages without requiring you to enter the passcode. Turn "lock display" options off under notification settings. Also, block voice-assistant programs like Siri from operating when your phone is locked.

Another important tip is to keep a copy of your phone's unique International Mobile Station Equipment Identity (IMEI) number. You can obtain the code from behind your phone's battery, under your phone's settings, or by dialing *#06# into most phones. You can use the code to trace a stolen phone and prove ownership to legal authorities or phone retailers.

Finally, an obvious but important step before you head to the airport: do not store your phone in checked bags. Keep it in your pocket or in your carry-on luggage at all times.

You will be prepared for most scenarios by following these steps before you hop on the plane. However, you can take additional steps while traveling for extra assurance and security. As you use your phone during the trip, routinely clear its cache, call history, texts and emails. We recommend messaging apps that encrypt communications, such as WhatsApp, for both personal and professional correspondences.

Only install trusted applications while on the road, preferably ones you have vetted by using them back home, and be mindful of permissions that apps request. Do not grant apps (except trusted security apps) administrator privileges. Watch for odd behaviors in the phone's software, as they could indicate a virus or malware infection.

Never click on links in text messages or emails, particularly from senders whom you do not recognize. They are often spam messages and could contain malware.

Turn off Wi-Fi and Bluetooth when not in use—they make your phone vulnerable to malware and hacking—and be sure your phone is not set to automatically connect to open Wi-Fi networks. Do not use Wi-Fi networks unless a password is required and be extra cautious when using public Wi-Fi network by avoiding banking or social media apps that are full of your personal data.

Do not allow your phone's web browser to save passwords. Also, consider using programs that can mask your identity and web traffic. For Android users, Orbot is an application that funnels your traffic through the anonymous Tor network. Orweb is a privacy-enhanced browser that can use proxies to mask your traffic. For iPhone users, use the default Safari browser in Private mode.

The more complex but secure solution is to connect your phone through a virtual private network when accessing contents online. A VPN encrypts your traffic, allowing for secure online communications.

Concludes on page 6...

Now, here are some practical tips for common phone uses while traveling. First of all, do not connect your phone to computers or use SD cards unless you are certain they are free of malware. Running low on juice? Forget about plugging your phone into public charging stations found by public squares or bus stations. A thief could hide a small computer inside the charging stand and steal your personal data. Charging stations in airports, however, are typically secure and safe to use.

More useful tips: keep an eye on your phone in public places and do not let strangers access your device, not even to take your picture or make a call. That is a quick way to get hacked or robbed. When in public, enter your PIN discreetly, shielding your screen if necessary. Finally, to reduce the risk of theft, carry your phone as little as possible and store it in the hotel safe when not needed.

Be aware of your surroundings at all times and hold your phone with a tight grip during use. If possible, keep your phone hidden by using a wireless headset for calls and wearing a smartwatch to receive time-sensitive notifications.

Even after following these recommendations, your phone is not 100 percent safe from loss or theft. In the worst case scenario that your phone is stolen, alert the police and your carrier immediately. They can assist in tracking the phone and shutting off its service. Next, find a computer and use your phone's tracking software to locate, disable, lock, or erase it. If you locate your phone, do not attempt to recover it. Let the police handle it. Most importantly, update passwords for all accounts you've previously linked to the phone as they may been accessed or tampered with by the thief before you are able to activate the kill switch.

Once you've returned home from what is hopefully an enjoyable trip, update and run your anti-virus app to be sure your phone was not infected. Check your phone again for physical evidence of tampering. If you find any, change the passwords for any accounts you accessed from the phone for extra precaution.

Protecting your device and its data definitely takes some work. But if you do, your smartphone will be more secure and you will have one less thing to worry about on your next trip.

Additional Useful Tips for Securing Your Smartphone

PASSWORDS: FIRST LINE OF DEFENSE

Creating a secure password can be a challenge. It has to be sufficiently random so it cannot be easily guessed, but it also has to be something you can always remember on the go. Here are our tips for creating foolproof passwords:

- Use a pass-phrase. Instead of just choosing individual characters, choose words and numbers. An example password could be: "TheNYKnickswillneverwinatitleIn2000years." To foil brute-force dictionary attacks, mix letters and numbers and make the phrase long.
- Combine numbers that are meaningful to you with symbols. For instance, if the address of your first apartment was 209, you graduated high school in 1990 and your parents were married 50 years ago, a potential password could be "209#1990&50."
- Use an anagram. Create a sentence that is meaningful to you, like "I got my driver's license in 1989 and moved to Kansas." Then using the first letters of each of the words (including capitalization) and all of the numbers, your password could be: "Igmdli1989amtK."

PINS: MORE THAN FOUR NUMBERS

Most people use four-digit PINs to secure their phones. But your phone is more secure with a longer PIN or password. Some tips:

- A numeric PIN that is 10 digits or longer is tougher for hackers to crack.
- On Android phones, use a complicated swipe pattern to secure your phone. They are very tough to guess, as long as you remember to wipe oils off your screen which can leave a trail showing where you swiped.
- Create a lengthy alphanumeric password instead of a PIN.
- Some clever apps like Lockdown Pro on Android randomly rearrange the numbers or letters on lockscreen keypads, so people peering over your shoulder can not easily memorize your PIN or password.

TAMPER-PROOFING YOUR SMARTPHONE

A hacker or identity thief can secretly replace components on your smartphone to surreptitiously steal data or install malware. Guard against such attacks with these tips:

- Place small unique marks on your phone's SIM card, removable memory card, battery, and casing so you can more easily detect if any of those items have been replaced. You can use an ultraviolet marker, which is not visible in normal light.
- Use an app like Lookout to immediately record access attempts. Lookout can be configured to secretly take a photo of someone entering an incorrect PIN code and email you the photo along with a map of their location.
- Place tamper-proof labels or tape on the joints of your phone to provide visible evidence of unauthorized access.

SECURING YOUR HOME WI-FI

Would you consider giving a stranger or a nosy neighbor keys to your house? The same concept applies to protecting your home network. Use our steps and refer to your router's manual for model specific information in securing your Wi-Fi.

How does Wi-Fi work?

Have you ever wondered how Wi-Fi technology seamlessly connect multiple devices in every nook and cranny of your home? Simply put, Wi-Fi is a router that connects your computer using radio waves instead of cables. It uses frequencies, like walky talkies and car radios, to transmit information between devices. A central device known as a Wireless Access Point (WAP) inside the router distributes Internet connections by physically connecting phone or cable live and converting signals into radio waves. Once this central connection between the router and phone line is established, the WAP produces an electric field or hotspot that ties all of your computer peripherals together like an online virtual hub. The size of the hotspot may vary from home to home, but the Wi-Fi network works best within a 66-foot range.

How do I secure the Wi-Fi network in my home?

All routers across a make and model share the same internal IP address, username, and password. For this reason, it is crucial to re-configure the router's settings prior to enabling your Wi-Fi network at home. The first step in the process is to establish a physical connection between your PC and your router using a USB or Ethernet cable. Next, enter the router's internal IP address (found on the back of the router usually) into your web browser (e.g., http://192.168.0.1/) and press Enter. The login screen that appears will request the router's default username and password which may found within the manufacturer's manual.

Note: If you no longer have the applicable documentation, check the manufacturer's website to obtain the router's internal IP address, username and password.

How should I configure my router and what criteria should I follow?

- Username and Password: To thwart hackers, you should change the router's default username and password to include uppercase letters, lowercase letters, numbers, and symbols. Refer to our guide about passwords on p. 6.
- Service Set Identifier (SSID): The default SSID, sometimes labeled Network Name, often identifies the brand name of your router. This gives potential attackers information they may use to break into your network. It is important to choose a name that neither relates to your device nor to you personally.
- SSID Broadcast: This feature helps anyone within range discover your network. This option should be disabled because announcing the existence of your network diminishes its security.
- Router Firewall: The firewall should be enabled because it will block outsiders from connecting to devices within your network. Furthermore, it will not interfere with system firewalls already in place.
- Remote Access: This preference allows you to access your network from anywhere in the world. Such capacity should be disabled because it will likely benefit hackers more than you.
- Wireless MAC filtering: This option should be activated so you may limit network access to specific devices based on their unique MAC addresses.
- Encryption: To maximize security, you should select WPA2-PSK and AES, which are modern encryption standards deployed in all Wi-Fi routers. Further, the PSK password should be long and complex but different from the router access password.

What additional measures should I follow?

- Stationary computers should directly access the internet through a cable.
- Turn your network off during extended periods of non-use.
- If you have enabled guest access on your computer, make certain it is password protected.
- Position the router away from windows and close to the center of your home to limit the reach of the signal.

Can I recover my password?

If you forget your password or your router is compromised, you can restore the factory settings by pressing the reset button located on the back of the router.

IMPLICIT DENY: WHAT TO LOOK OUT FOR IN MOBILE APP PERMISSIONS

Mobile applications provide a wide array of services and benefits at the cost of you granting permission to access certain features on your phone or tablet. This article will help you ensure that you don't give unnecessary permissions to any given app.

What is the purpose of mobile application permission requests?

To work as intended, mobile apps often require access to certain features on your phone. For example, an app that allows the mobile device to function as a flashlight would require sustained access to the camera's flash feature. Therefore, any user requiring this functionality must accept this permission request. The problem arises when some apps require permissions that have nothing to do with the app's functions. For example, is a game app like Candy Crush asking to know your location at all times? App developers are motivated to request for more permissions than less as this data is used to sell advertisements or derive user insights for (sometimes) nefarious purposes.

If I download an app, can I selectively accept/decline requests?

Android users who choose to download a mobile app must accept all permissions requested. iOS users are not subject to this all or nothing proposition, they have the option to accept some and decline others. Permission requests for Windows phone users depend on the specific app itself, some require acceptance of all requests while others do not.

Which requests should be accepted and which should be declined?

Permission requests are neither inherently "good" nor "bad." The appropriateness of any request depends on the purpose of the mobile app. For example, an app that provides driving directions would necessitate access to the device's GPS tracking feature. A flashlight app would have no such need. Therefore, permission requests should be aligned with the functionality of the app. User acceptance of any permission request should only be granted when the app's purpose is logically tied to it.

Why would an app request unwarranted permissions?

Collecting user data is crucial to gaining insights about smartphone users' needs and wants. Therefore, app developers are motivated to collect as much information on their users as they can to improve their current app or develop brand new ones. Additionally, user data is a source of profit for app developers as it can easily exploited and sold to advertisers; for instance, location data can be sold to advertisers to allow geographically targeted ads.

Permission requests can be difficult to understand. How can I know if their presence is justified?

As previously mentioned, the permission requests should align with the app's core functionality. We will examine the most frequently misused requests and clarify the type of apps for which they are required with the following table.

Permission Request	Purpose	Apps that need this permission
Location	Track user's position	Maps, running apps, and location-based social media (e.g. Foursquare)
View Network State	Checks for network connectivity	Email, social media, maps, and search
Full Internet Access	Connects to the Internet	Browser, gaming, and messenger apps
Modify SD Card	Write to external storage	Camera, audio and video editing apps, and document apps
SMS	Send text messages	Social media and communication apps
Identity	Link to existing accounts	Social media and communication apps

Do I have other means of determining if permission requests are being used for deceitful purposes?

There are many things you can do with respect to permission request concerns. One method is to utilize organizations such as PrivacyGrade to obtain information regarding privacy-related behaviors of any given app. Further, Android users can download an app called "Pocket Permissions" which provides detailed information concerning the legitimacy of permission requests as they relate to any given app. Lastly, running a Google search on the mobile app prior to download will reveal common complaints with which it is associated.

SAFEGUARD: REMOVING EXIF DATA FROM YOUR MOBILE DEVICE'S PHOTOS

Cyber criminals can take advantage of the metadata from your camera to track your location or presume your identity. Learn how and when to remove EXIF data from your mobile photos.

What is EXIF data?

EXIF stands for Exchangeable Image File Format, which fortunately is the extent of the technical jargon required to understand this subject. In layman's terms, EXIF data is the detailed information that resides within the pictures you take with your mobile phone or digital camera. A great deal of mundane information, such as camera's shutter speed and flash settings, is captured. However, additional data such as the time, date, and location of your picture may also be revealed. It is important to note that EXIF data is collected and maintained by your Photos app and online photo sharing services, and its removal requires extra effort on your part as the user.

How can I see the EXIF data embedded in images?

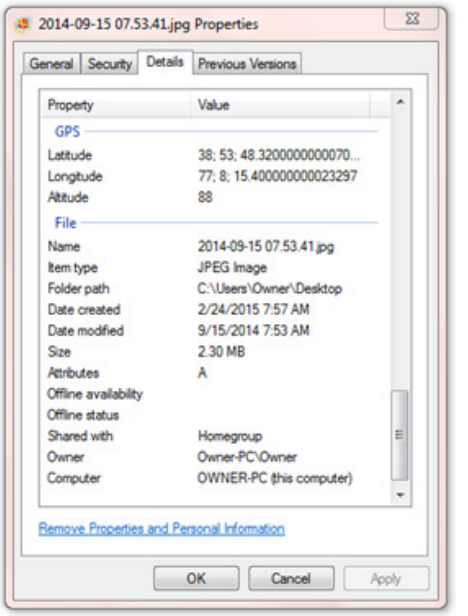
Begin by downloading the photo to your computer. If you are running Windows, right-click the file and go to Properties. If you have a Mac, you will need third-party software such as ImageOptim to view EXIF data associated with your photos.

Does EXIF data pose risks?

The primary concern with EXIF data is geotagging, or its capacity to show precisely where you were when any given picture was taken. This can cause privacy concerns, particularly to parents who wish to prevent the casual online observer from knowing the location and travel habits of their children.

I've taken many pictures with my mobile phone and posted them online. Is the EXIF data accessible?

The two largest social media sites, Facebook and Twitter, strip EXIF data automatically. Instagram does too, unless you add the picture to your Photo Map. Lastly, Flickr allows you to decide during the upload process. One notable exception, however, is Google Photos which maintains all EXIF data associated with your images.



EXIF data example

Would anyone knowingly post pictures to a site that does not remove EXIF data?

Many people want their photos to contain time, date, location, and descriptive captions as a means of providing context for friends, family, or followers. Others plan vacations and sightseeing destinations based on the EXIF data embedded within pictures taken by world travelers.

How can I strip EXIF data myself?

Any reputable site that says it strips EXIF data is likely doing so. However, you may avoid the risk altogether by removing the data yourself prior to upload. To do so requires following the same process used to view EXIF data (described above). From there, those of you using Windows may click Remove Properties and Personal Information at the bottom of the Details tab. If you have a Mac, you may follow the steps provided within the ImageOptim software.

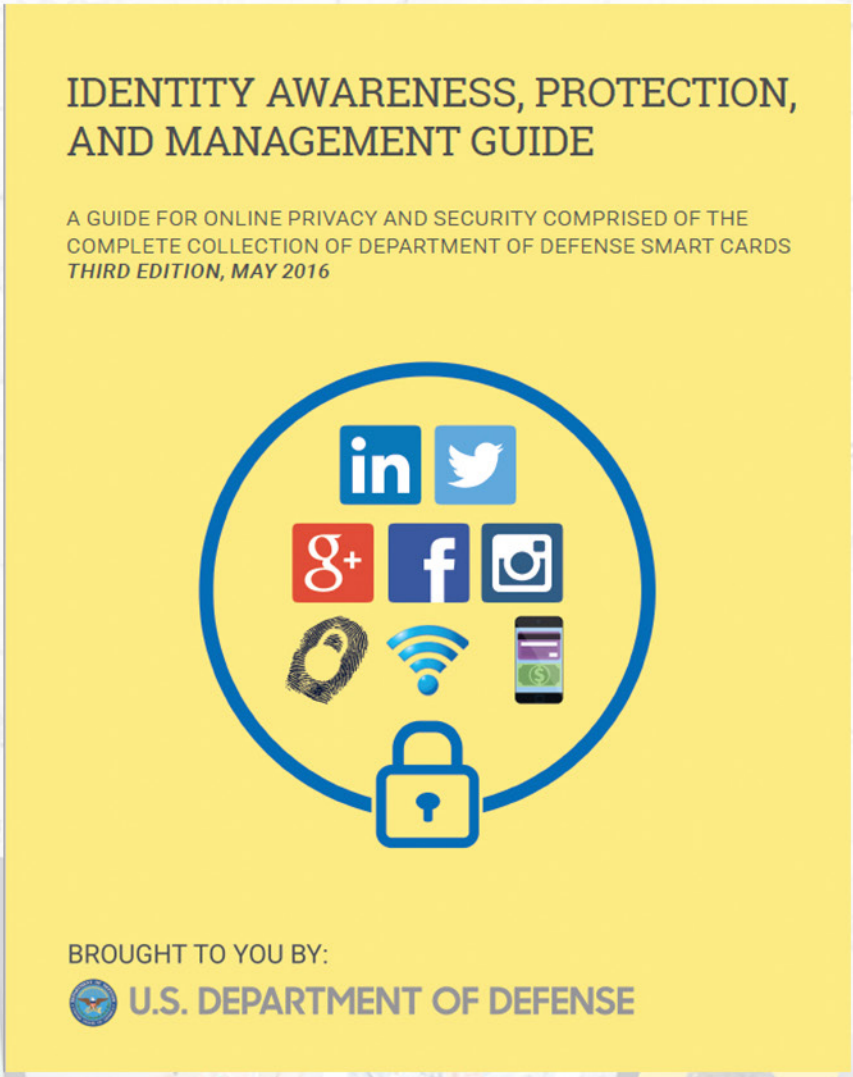
We've talked about social media sites, is there any other way my EXIF data might be shared?

Unless you have specifically stripped EXIF data from your photos, the information will be shared each time you send an image to anyone via text message, e-mail, or file transfer. You may be especially vulnerable within this scenario because you trust your friends and family to avoid misuse of your data. However, if they forward your image to other friends, soon the EXIF data and how it is shared is outside your control.

My main concern is public knowledge of my work location, where my family lives, and where my children attend school. Is there a simple way to prevent geotagging from occurring in the first place?

Fortunately, this is possible. If you have an iPhone, go to Settings then to Privacy and turn off Location Services. Those of you with Android phones may also follow Settings to Location and turn off Location Services.

This issue covered the threats your devices and networks pose, and how to mitigate them. For more detailed information please check out the Identity Awareness, Protection and Management Guide.



Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL