MOBILE SECURITY
SURVIVAL GUIDE FOR JOURNALISTS

KATRIN VERCLAS
MELISSA LOUDON
ALIX DUNN

SAFER MOBILE
https://safermobile.org

The **Mobile Security Survival Guide for Journalists** helps you better understand the risks inherent in the use of mobile technology. It also discusses some tactics you can use to protect yourself. The guide covers both local journalists and those on assignment in another country. It is important for any journalists or person engaged in sensitive work to understand that mobile communications are inherently insecure and expose you to risks that are not easy to detect or overcome. This guide is designed to help you navigate these challenges.

We outline the risks and offer tips to help mitigate them. Our primary goal is to help you make better decisions about using your mobile phone while on assignment for both your professional and personal communication.

It should be noted that this guide does not guarantee your safety. Rather, it is a foundational resource for you to understand and minimize risks of mobile communication in the field.

The Mobile Security Survival Guide is written with the workflow of a journalist in mind:

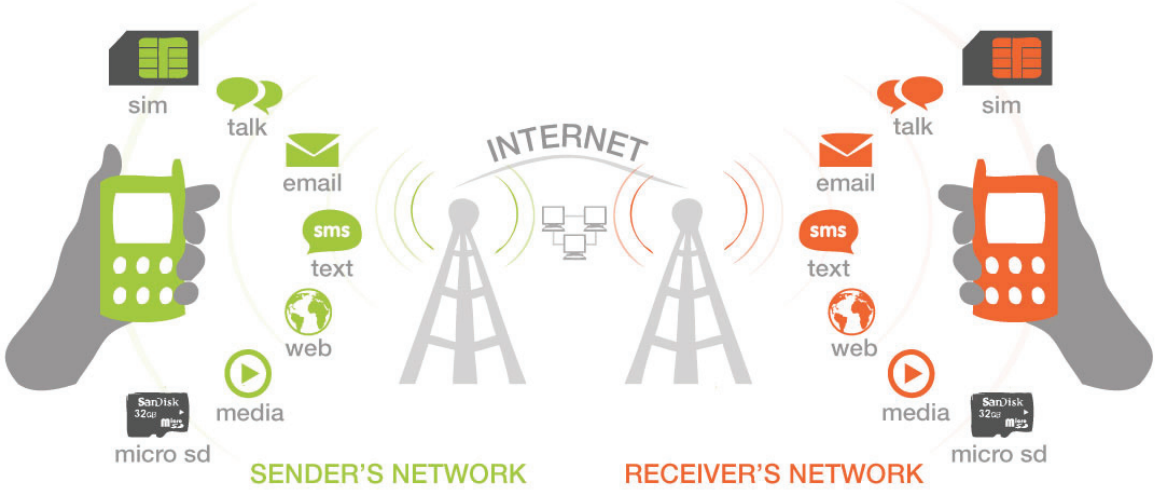
The Mobile Security Survival Guide is written with the workflow of a journalist in mind:

1. **Mobile Network Awareness: The Basics** –
   What does your mobile use say about you?
2. **Preparing for Assignment** –
   Assess your digital risks and prepare your phone.
3. **Reporting/In the Field** – Talking to sources and conducting interviews;
   checking in with your newsroom, your phone in emergency situations.
4. **Filing the Story** – Sending updates, news bursts, or multimedia content from the field.
5. **BONUS section! Social Media** –
   Safer use of social media to follow news, connect with sources,
   share breaking stories and promote your work.

1 MOBILE NETWORK AWARENESS: the basics

Mobile phones are pervasive, discreet, and increasingly sophisticated devices. They are extremely useful for reporters. However, phones may also reveal to third parties lots of information about you and your work in the field. There is much more on how to assess your specific risks in the Mobile Risk Primer. Check out the Risk Assessment Guide.

Your mobile network operator logs data about you, your communication activities and your device. This graphic shows a schematic overview of the layers of mobile networks, to give you a sense of the different elements that make up communications between two phones.



Data stored on network logs.

Activity on your phone creates a data trail that is logged on the mobile network, rom placing or receiving a call, to sending a message, browsing the web, or just being connected and ready to receive communication. Identifying information logged on the network about you and the persons you contact include your IMEI number (the unique handset identifier), the IMSI (the unique SIM card identifier), the time and duration of voice calls, SMS, and the photos or video you take while reporting. Your data use and websites that you visit are not only stored on your device but also create meta data logged by your mobile network. This is not necessarily nefarious but simply a function of the network so it can bill you for your activities.

SAFER MOBILE
https://safermobile.org

Your location is being stored.

When your phone is switched on, the network "knows" your location. It triangulates using the cell towers nearby or your phone's GPS if it is turned on. If you make or receive a call, or send or receive a text message, your location is stored in network records. Note that this is a basic function of the mobile network, not any nefarious surveillance. All networks triangulate your signal, to make it possible to direct communications accurately from one phone to another. In urban areas your location may be accurate to a few meters.

The problem here is that network records can be vulnerable, and can be used if you are identified as a person of interest and are placed under surveillance by someone who can access them. Your network records can also be retrieved through a legal mechanism, an informal intelligence or government request, or through a corrupt employee of the network operator.

Disable location services when they are not in use.

On advanced phones that run social media and other applications you should disable location services when they are not in use. Some phones warn the user when an application requests location information, and the phone's settings have an option to disable location services. Individual applications also may have settings options that allow the user to disable location services. See this SaferMobile guide for more on disabling geolocation services.

Turn off your phone strategically.

When turning off your phone, be sure to remove the battery – simply powering off your phone is not enough. Think about where you turn your phone on and off. If you are travelling to an in-person interview, you can turn the phone off and remove the battery before you leave, then return the battery and turn it on after you arrive to obfuscate your path. Leave sensitive locations before putting the battery in and turning on your phone, and then turn the phone on later in a different location.

WARNING: Trying to be too clever may show draw attention to yourself by showing irregular activity on the network. If you are a person of interest or under any surveillance, these tactics may make you look more suspicious. In that case, consider not taking your phone with you at all to sensitive meetings and leave it at home.

Use geolocation to your advantage, especially in emergencies.

Geolocation may be used to your advantage. It can be a record of where you were and where you were not at any given time. If a person goes missing, the network operator will have a record of where their phone was last. Advanced phones can use applications that send their location periodically to a website, where friends can track the phone's location. There are also applications that allow you to quickly send a short message with geolocation data if you are in danger.

TIP CHART

Turning off GPS
can save your battery during long reporting trips. Because satellites are much further away than cell towers, the satellite signal is comparatively weak. While cellular phones often function indoors, GPS usually will not work without an unobstructed view of the sky. Even though the phone does not transmit when listening for GPS radio signals, the process can use up your battery.

Avoid identifying information.
As much as possible, avoid linking your identity to your phone number. Buy prepaid SIM cards and, if possible in your country, avoid registering the SIM with personally identifying information. Buy a number of cheap, low-tech phones that you don't mind throwing away, if necessary.

Have an alternative to deal with disruption.
Always try to have an alternative in case you are unable to access one or more services. Carry SIM cards for other mobile network operators, and if possible, carry more than one phone. In some cases, only an out-of-country operator may have roaming service. Have a backup plan agreed upon in advance with sources and colleagues if you suspect that your specific line or the entire mobile service may be disrupted.

SAFER MOBILE
https://safermobile.org

2 PREPARING TO GO ON ASSIGNMENT

You have been given your assignment. You may be travelling to cover a story or you may reside in a given country. Either way, when it comes to your mobile communications, you should take some precautions and plan ahead as you prepare.

The International Federation of Journalists offers a Survival Guide for Journalists; the International News Safety Institute lists practical information on safety and security; and the Committee to Protect Journalists has a brandnew Journalist Security Guide. This section of the Mobile Digital Survival Guide will focus specifically on mobile-related security issues.

Availability of services

If you travel to your assignment, do your best to understand the availability and reliability of phone services in the location where you are headed. Can you use your mobile device in all the locations where you will be working? Is service generally reliable or often disrupted, intentionally or unintentionally? What is the likelihood of getting your phone confiscated? Are there instances of surveillance of journalists or activists' mobile communications? What is the degree of freedom of expression? If working in a location with political repression, how closely is the government associated with the mobile network operators?

Assess your operational environment to help you decide what precautions are necessary. What are the policies regulating whether governments and other entities can intercept your communications and access your phone records? Are the tactics and tools you are using considered legal where you are working? For instance, a number of countries prohibit the use of encryption over telecommunication networks. If they are illegal, your risks may increases considerably.

TIP CHART

Know your phone.
It may sound obvious, but be sure to know how to work your phone. For example,become familiar with how your camera works and how to control its options. The flash of your camera or the sound when you click Capture may draw unwanted attention to you. Take the time to pre-set functions to avoid getting noticed by others.

Practice on your mobile keypad.
Learn how to operate your phone without looking at it. You may need to know how to type a text message (SMS) without looking at your mobile keypad or perhaps while it is hidden in your pocket.

Plan your shortcuts. You can save time and effort by setting and knowing your shortcuts. Many phones allow you to set up shortcuts to access applications, such as the camera. Know and practice those shortcuts without looking at the phone.

SAFER MOBILE
https://safermobile.org

Sensitive content on your phone –Take a look at the content on your phone.
Think about your most sensitive information, data that may put you, your sources, or your newsroom at risk if seen by an adversary. This may include:

- The names, numbers, photos, emails, contact information, and Twitter handles of your contacts.
- Call logs and saved SMS messages
- The username and password for your personal or professional social media or email accounts.
- Mobile photos and videos documenting certain events

Conduct your personal mobile security risk assessment.

Security assessment and risk mitigation are resource-intensive processes. The aim of this SaferMobile risk assessment guide is to help you formulate a realistic plan that you can manage yourself.

Remember that mobile tech is only one part of your reporting toolkit. For an excellent guide on assessing and addressing additional security needs, see this publication by Frontline Defenders.

Back up your mobile content/wipe your phone.
Back up all content off your mobile phone to a secure computer. Be sure to include contacts, messages, logs, media, and any other content that you believe is important. If you are working in sensitive areas, you can re-format or wipe your phone later, deleting all content and records and only keeping essential information. WARNING! Know that even a reformat of your phone does not forensically-sound delete all data. With forensic extraction equipment, some data may be restored off your phone if it is confiscated.

TIP CHART

- **Have a list of important or emergency numbers handy apart from the phone.** Depending on your level of risk, you may want to code this information in a way that is (quickly and easily) decipherable only to you.
- **If possible, have a second phone readily available** to be able to communicate in case you lose one. If you are able to use a basic or feature phone (a non-smartphone) for your reporting, it might be a good option, particularly if you face serious risks. A non-smart phone is easier to replace and generally contains less information that might compromise you. Generally, consider your phone disposable and keep as little data as possible stored on it.
- **Make sure you have enough credit if you use a pre-paid plan**. You don't know how many phone calls you will make or how much data you will need while reporting in the field.
- **Apps: Pick and download security apps** after you have been given an assignment, researched your operational environment, and thought about your specific mobile security risks assessment. Test all apps. Always test any mobile apps, understand how they work and when to use them. For some apps, especially for those using end-to-end encryption, both the sender and the recipient have to have the same app on their phones. Plan for this in advance.
- **Carry a spare phone, SIM, and battery.** If you believe that you are a person of interest in an insecure environment, and that your number may be targeted for disruption, carry an extra phone and SIM card. Always keep at least one extra battery and your charger on hand. Practice how to change your mobile batteries quickly and in the dark.

SAFER MOBILE
https://safermobile.org

There are guides on anonymous and encrypted browsing, encrypted mobile email, and tools for encrypted chat and encrypted SMS. Note that there are many apps for a specific operating system only.

You may draw unwanted attention to yourself if you use specific security applications.

Consider crossing borders without obvious security apps on your phone if you are concerned about surveillance, or if specific technology (especially encryption tools) is illegal where you are working. Encrypted communications are very obvious on the mobile network if there is data surveillance, and encryption may make your communications stand out. Consider whether specific security applications may incriminate you, and whether more secure communications are worth the risk of being identified as someone who is trying to conceal something.

3 REPORTING:

You have arrived on location and are ready for work. And you likely know well the adage of the Committee to Protect Journalists, "Staying in touch means staying alive." Remember, if you have an alternative story as to why you are there (i.e., I'm not a journalist), make sure your communications are in line with this story. For instance, if your cover story is that you are in a given place to do academic research, let your phone data and communication patterns reflect that story.

Have a plan of action ready such as who to contact in case of detainment. If you do not have this information memorized, use coded language — that is easy for you to decipher — to more safely store specific emergency contacts or procedures on your mobile phone.

SMS

Texting is an easy way to communicate, but it is also one of the least secure forms of mobile communication. Text messages are sent entirely in clear text, and meta-data (location, time sent, and who it was sent to) is routinely logged by the network operator. SMS filtering and data mining has been reported during periods of unrest. If you chose to check in with your newsroom or others via SMS, and you are working in a highly insecure environment, take precautions.

TIP CHART

Use codes for SMS if needed. If necessary, use pre-arranged codes to communicate sensitive information to your contacts.
Change your codes regularly, and make sure your system incorporates a way to let others know when you think the code may have been broken. To practice, try the code-making exercise in the SaferMobile training guide. Avoid words that could be considered "high profile" or inflammatory if you suspect keyword filtering of SMS is taking place. However, remember that information about the recipient of text messages (i.e. that person's number and other information) is still logged by the network operator. Take care not to put any sensitive sources at risk with your communications.

Use security apps for safer SMS messages.
If you will be checking in or communicating via text message, explore, test, and install encrypted SMS apps. See this list of suggested apps. Remember that for some apps and alternative forms of communication, both the sender and the recipient need to install the app on their phone. And consider whether a more secure form of communications is worth the risk of being identified as someone who is using encryption.

Remember to avoid having your location tracked by keeping your phone off and the battery out when traveling or meeting in sensitive locations. For more information on location tracking, see this Primer on Geolocation.

SAFER MOBILE
https://safermobile.org

VOICE CALLS

If you plan on using your mobile phone to make phone calls, take a look at SaferMobile's guide on evaluating your mobile voice call risk. Voice calls are easily intercepted and should not be considered secure if you are working in an insecure environment.

Create and use codes on calls, too.

If you are worried about your calls being intercepted or recorded, but still need to use the mobile network to make some voice calls, consider using a pre-arranged codes to communicate sensitive information. The SaferMobile training guide has a code-making exercise to help you and your contacts practice creating and using codes. Remember, your code is only useful if it's easy to remember and use, and if the recipient understands its meaning. You shouldn't need to write it down. Your code should include a way to let others know when something goes wrong.

Explore Voice over IP (VoIP).

Voice over IP (VoIP) apps and services may offer an alternative to voice calls. But understand that VoIP calls are not secure either. Read this SaferMobile guide on VoIP, which also lists suggested apps based on your operating system.

TIP CHART

- **If you use voicemail while on assignment, use a good PIN and password.** Voicemail hacking is a reality. If you do choose to use a voicemail service, make sure you use a good PIN and password, and change them periodically, particularly if you suspect they have been guessed. A good PIN should be something that is difficult for an attacker to guess, even if they have some of your personal information.

- **Try secure chat instead of voice or VoIP.** If you need the immediacy of voice but don't want to use VoIP, you might consider switching to secure chat as an alternative. Encrypted email can also be used to substitute for voice calls. Gibberbot, for instance, is an off-the-record messaging app on Android for secure instant messaging. Also, check out the SaferMobile guide to securing your mobile email.

EMAIL

This guide from SaferMobile suggests tactics for improving the security of your mobile email. Here are some takeaways, but consult the guide for more.

Practice basic email security precautions. Choose a strong, unique password for your email account, and change it often. Log out of your mail service after use, and avoid storing your email password on your phone.

Consider that even a deleted message may be stored in your phone's memory and could to be restored with the right software or equipment. Don't open emails (or SMS) from people you don't know to avoid malware on your phone. If necessary, get hold of the sender through other channels and verify that they indeed sent the message.

Enable TLS/SSL for all email.

Most email clients and many email services support encrypting your email between your email client and the server. But be aware that even if you are using TLS/SSL, it does not mean that your messages are reliably encrypted.

If you can use TLS/SSL to send and receive mail, you always should. This is how you set up Gmail to use TLS/SSL in the Android mail app and the equivalent guide for the iPhone and for Blackberry email. For email providers other than Gmail, you should be able to set things up the same way – just use the incoming and outgoing mail server settings of your provider. More information is here.

Encrypt your email and use a web-based encrypted email provider.
For more on what this means (and instructions on how to encrypt your email communications) consult this SaferMobile guide.

SAFER MOBILE
https://safermobile.org

USING YOUR PHONE FOR NOTES

There are many mobile media tools to help you use your phone for better journalism. Examples include Evernote, a tool for creating, sharing, and tagging notes, or Dragon Dictation, a tool for transcribing interviews.

Make sure all your mobile media tools are worth the trouble.

Are they trustworthy? Do they make your work easier or more cumbersome? In all cases, download and experiment with the app before you head out on assignment, and be sure your apps come from reputable software developers. Read this SaferMobile guide and ask yourself these 6 questions before you download any apps to your phone.

Satellite phones are not as secure as many people think they are.

Satellite telephones are an alternative to mobile telephones. Satphones send signals from the mobile device directly to satellites, bypassing local wired and mobile infrastructure. Because they do not rely on the local infrastructure of telephone lines or cellular towers, they are useful wherever local infrastructure is unavailable or untrustworthy. But because satellite phones operate differently than mobile telephones, they raise unique privacy and security concerns. Before you consider using a satellite phone, read this SaferMobile guide on Satellite (in)Security.

CAPTURING AND UPLOADING MEDIA

Your mobile phone is a great tool for capturing photo, audio, and video elements for your story. Attaching location information to this multimedia can add value to your stories: It provides more context and can be used to verify or corroborate events. It helps journalists and publishers find an interested audience and lends itself to aggregation – content with location information can be situated on maps and other visualizations. There is much more producing media on your phone at the Mobile Media Toolkit, a site dedicated to 'making media mobile.'

If it adds value (and is safe), add location information to your mobile images.
You can tag content with location by using a physical address. You can also let software on your mobile phone automatically find your location. Doing this requires a phone that has GPS hardware, or that can run software that can access your network settings. For details, read this MobileActive.org article on how to add location information.

Location information can expose you and your sources, and it should be used with caution. Most phones store the time the media was taken and may also include location information such as GPS coordinates, and the make and model of the phone in the meta data of photos and videos.

Be Aware that **meta-information** is captured and stored with my mobile content. Check your mobile content to see what meta information (often referred to as EXIF data) is being captured and stored with your photos or videos. On smartphones, you can check this via the photo gallery. This SaferMobile guide on removing location information shows you other ways to check for meta data on your mobile content.

Remove location data from your mobile content.

The safest way to remove EXIF data is to upload your photo to a computer and remove the data using software. You can downloaded a tool for Mac called PhotoLinker. For Windows, EXIF Cleaner is another option, and you can remove files in a batch. For details on how to do this on your computer, see this SaferMobile guide on removing location information. If you work primarily on your mobile while on assignment, you can remove location information from content on your phone. There are some apps available on iPhone and Android that offer EXIF manipulation, such as EXIF Wizard and others.

SAFER MOBILE
https://safermobile.org

TIP CHART

Check your defaults on photo sharing sites. Another way to remove location data is to have your photo sharing site scrub the location information for you. Two popular sites, Facebook and Flickr, both do this. At the time of this writing this was the default policy on each service, but check this before your assignment. For instructions on how to change the default to not import EXIF location data, see this SaferMobile guide.

Upload and delete. Uploading content right away when you have sufficient internet access can help avoid losing the content if you lose your mobile. You can upload using http://m.twitpic.com/upload or http://m.flickr.com/#/upload, for instance.

WARNING: Keep in mind that if you upload large amounts of media from your phone directly, the amount of data uploaded, your location while you are uploading it, and other data about the communications is logged on the mobile operator's network. Consider this if you are in sensitive areas (such as a protest area or a meeting place with a source) before uploading media.

Need WiFi but lack Internet in the field? If you tether your phone and use it as a portable WiFi hotspot, keep in mind these security implications. Take a look also at this guide on how to use your Android phone as a hotspot without rooting your phone.

Keep the memory card in your phone as empty as possible. This way, you can store all pictures and videos you take while at an event. If possible, bring multiple memory cards to use when needed. Practice changing memory cards in your mobile quickly (ideally without looking) and store full memory cards in a safe place in case your phone gets taken from you.

Be prepared for an emergency. While you are in the field, be prepared for an emergency. Remember, careful planning and strategic considerations are required for journalists to be as safe as possible in insecure environments (particularly in contexts where media harassment or worse is common).

Have remote-lock set up on your mobile phone.

Some mobiles provide a security level usually known as remote-lock. It enables you to lock your mobile by sending an SMS with a particular keyword you previously set to your mobile if you lose it. For more, see this SaferMobile guide to covering protests and peaceful assemblies.

Prepare content in advance.

If you will be posting content online, write important links in an SMS and save it as a draft. You can just copy and paste the links if your mobile supports this feature. If you expect to send a particular message to someone, prepare it in your drafts. That will save you time, and you can just click "send" when you want to send it.

Be prepared to use emergency mobile applications.

Consider installing a remote wipe and emergency notification app on your phone. There are numerous apps available and not all work perform as well as others. Here is one review with a handy chart of remote wipe apps. Remember that remote wipes and even a factory wipe of your phone may not remove data in a forensically sound manner. If you work in an environment with a technically sophisticated adversary who may use data extraction tools, even data that was 'wiped' may be able to be extracted and restored. To minimize your exposure if your phone is taken, keep as little data as possible on it, and no sensitive data at all.

SAFER MOBILE
https://safermobile.org

4
FILING THE STORY

While you may not be filing an entire story on your mobile phone, you can use it to send updates, news bursts, or multimedia content from the field. Unless you are using HTTPS, an attacker on the network can use a packet sniffing tool to see what content you are uploading, including any photos or videos you are submitting online or to your newsroom.

Disable MMS if not needed.

Unless you really need MMS functionality on your phone, check the settings to see if it can be disabled. MMS, like SMS, can be intercepted and viewed by the network operator. Delivery rates for MMS tend to be lower as well, making this a more unreliable form of communications as well as a more insecure one. MMR can be an attack vector in another way: There have been cases where MMS has been used to sneak mobile viruses and malicious mobile software into unsuspecting phones.

Keep your personal and physical safety in mind when deciding to file on the scene. Are you increasing your odds of having your phone taken if you file on location? Depending on the specific threats you face, you may want to use a (more) secure application such as Wuala, a cloud-storage system for Android or iOS that encrypts files locally on your phone before they are uploaded. You may also consider TextSecure, a secure messaging application for Android that stores sent and received text messages in an encrypted database on your phone.

If you use the Blackberry Enterprise Server (which routes messages through RIM's servers), messages are encrypted as they travel from one Blackberry handset to another. Blackberry has often been considered 'more secure' and is in wide use by many journalists. Chris Parson on his blog notes, that: "BBM, for example, is encrypted. However, it is encrypted using a global key. RIM has written that,

The BlackBerry device scrambles PIN messages using the PIN encryption key. By default, each BlackBerry device uses a global PIN encryption key, which allows the BlackBerry device to decrypt every PIN message that the BlackBerry device receives.

This means that RIM can decrypt consumer messages that are encrypted using the global key. Consumer devices include all RIM services that are not integrated with a BlackBerry Enterprise Server (BES). The BES lets administrators change the encryption key, which prevents RIM from using the global decryption key to get at the plain text of BES-secured communication. Many countries want access to consumer-level encrypted BBM communications and have demanded access to decrypted BBM messages." There is much more on BB security in his excellent post.

5 BONUS SECTION: SOCIAL MEDIA

Chances are you already use social media sites like Facebook, Twitter, and YouTube to:

- Stay on top of stories and follow breaking news.
- Find other reporters or citizen journalists reporting on specific issues or regions.
- Reach out to particular sources or experts.
- Break your own news and help cover a story as it unfolds.
- Promote your own published story and engage with your audience.

If you are reporting from the field or traveling for your assignment, chances are, again, that you do these things from your mobile phone. Here, we offer some tips and actions to take to better protect yourself while on your handset.

Set a strong password and keep it safe. Keep your account details safe. Check out this guide from SaferMobile for more on setting a strong password.

While a strong password won't always protect you, it adds an important extra layer of security. Despite the risks involved, Twitter and other social media platforms are very powerful tools that can help report news from the field, especially when events are unfolding quickly, or you have limited options or decreased capacity and staff.

Use Twitter from your mobile to share publicly as you report.

As you know, your Tweets should only contain information you want to share widely and publicly. This should be information that can be freely distributed by you, your organization, and your supporters, without adding any additional risk to yourself, other individuals, or organizational operations.

You likely use Twitter or other social media to get to know the experts, activists, and sources on a given topic. You may need to contact these individuals or organizations to ask questions, verify facts, or set up interviews. Keep privacy and security in mind when doing this from your mobile phone, as it can reveal information about your sources. A record of any correspondence may be kept on your mobile device, which can easily be lost, stolen, or accessed without your consent.

Be Careful! Reaching Out to Sources.

Whether on mobile or not, if someone is not publicly and actively posting on social media sites, Do NOT contact them via a public social message to ask questions, verify facts, or set up an interview concerning a sensitive topic or while reporting from an area of conflict. This can put both you and your source in danger.

Understand the risks you face depending on how you access a social media platform.

For example, many Facebook mobile apps send data in plain text rather than over a secure connection. Unless you are sure that the app you are using communicates over HTTPS, it is better to use your mobile browser to access Facebook's secure mobile site.

Avoid older browsers and browse securely.

Your phone's web browser needs to support HTTPS. Avoid older browsers, particularly Opera Mini Basic 3 and below. All your communication with Facebook, YouTube, and Twitter should display a lock icon to indicate secure mobile browsing, and a web address starting with https:// rather than http://

Set up HTTPS, and check this often on your mobile.

With Facebook, set "Always Use HTTPS" in your account settings but be aware that this setting is not applied when browsing from a phone! You may also notice that some applications warn you that you cannot access them using HTTPS. If you use such applications, be aware that they may turn the Always Use HTTPS setting off, and you will need to go back into your account settings and turn it back on every time.

Even if you mitigate risk as best you can when in the field, understand that your activity on social media sites is recorded and stored.

Be aware of your video footprint.

Mobile video can prove that you or others were at certain events. Be aware of the risks involved in putting your face or voice on film, as well as those of others whose face, presence in a particular place, or identity might be revealed.Unless your newsroom requires you to use a specified channel or account, create an anonymous YouTube account for posting videos from your mobile device.

Sign up to YouTube anonymously and use this account on your mobile.

While anyone can view YouTube videos online, it's necessary to have a YouTube account in order to upload or share video content. If you already have a Gmail account, you can sign in with that. However, if you are trying to remain anonymous, it's recommended that you do not link your YouTube account to identifying email addresses. There is much more in these SaferMobile guides: SaferFacebook, SaferTwitter, or SaferYouTube.

For more information and many more resources on mobile security, check out SaferMobile.org / @safermobile on Twitter / facebook.com/safermobile

SAFER MOBILE

https://safermobile.org