**Communications Security**

**MOBILE PHONES**

*BASIC*

**1. The Problem with Mobile Phones**

Mobile phones are basically insecure:

1. Information sent from a mobile phone is vulnerable
2. Information stored on a mobile phone is vulnerable
3. Mobile phones give out information about their location
4. Mobile phones can be used to eavesdrop

Not only can the company that runs your mobile phone network intercept your calls and text messages (if unencrypted), and monitor your location – many companies also choose, or are required, to share this information with governments if asked.

Here, we'll describe some of vulnerabilities you need to be aware of when using mobile phones of any type, and recommend ways you can stay a bit safer.

**2. Information sent**

1. **Information sent from a mobile phone is vulnerable**

Each mobile phone provider has full access to all text and voice messages sent via its network. Other people who are close to the mobile phone can also tap calls and text messages using inexpensive equipment.The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording.

See the Making a Call and Sending a Message Lessons to learn how to text and talk more securely. The situation can be different when you are using secure communications apps to communicate (whether by voice or text), because these apps can apply end-to-end encryption to protect your communications.

If you absolutely have to communicate sensitive information using regular phone or SMS, try to use an inconspicuous code for sensitive words that you and your contact have agreed on before hand.

**3. Information stored**

1. **Information stored on a mobile phone is vulnerable**

Mobile phones can store all sorts of data: call history, text messages sent and received, address books, photos, video clips, text files. These may reveal your network of contacts, and personal information about you and your colleagues.

Some phones have encryption options available which should be applied. If you have an Android phone this can be done in *Settings -> Personal -> Security -> Encryption*.

Do not store confidential files and photos on your mobile phone. Move them, as soon as you can, to a safe location, as outlined in the Backing Up lesson. Frequently erase your phone call records, messages, address book entries, photos, etc. Learn more about safe deleting in the Deleting lesson.

Protect your SIM card and additional memory card (if your phone has one), as they may contain sensitive information. For example, make sure that you don’t leave them at the repair shop when your phone is being serviced. Use only trusted phone dealers and repair shops if possible. When selling, handing on or disposing of your phone make sure all information is deleted. Never hand on or sell SIM cards or memory cards – you should physically destroy them.

When capturing pictures or video it is important to be careful of privacy and safety of those pictured. For example, if you take photos or record video of a sensitive event, it might be dangerous to you or to those who appear in the recordings if your phone fell into the wrong hands. [**Guardian Project**](https://guardianproject.info/)has created an open-source app called **ObscuraCam** to detect/select faces on photos and blur them. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

Metadata such as phone identity and location are also captured on photos and videos. In some instances, such information is really important to have to prove the credibility of images and video so that they could be used as evidence in courts of law. At other times metadata can put you or others at risk. The GuardianProject has made a plugin tool for ObscuraCam called [InformaCam](https://guardianproject.info/2012/01/20/introducing-informacam/%5D" \t "_blank) that allows you to store a version of the image/video with metadata while also creating a redacted version without any sensitive data that can safely be shared on social media.

**4. Location**

1. **Phones give out information about their location**

The greatest privacy threat from mobile phones is the way that they announce your location all day and all night through the signals they broadcast. Every mobile phone automatically and regularly informs the phone service provider where it is at that moment. Only if a phone is switched off or without signal will it be prevented to send out such signals.

If you have a smartphone your location can also be tracked from apps, WI-FI or Bluetooth. Many apps use your GPS location to help them provide services, or just to collect data for their own use. You should only turn on your location when you need it and make sure that you only give location permissions to apps that you trust and that have a good reason to know where you are.

In each case, location tracking is not only about finding where someone is right now. It can also be about answering questions about people's historical activities and also about their beliefs, participation in events, and personal relationships. For example, location tracking could be used to try to find out whether certain people are in a romantic relationship, to find out who attended a particular meeting or who was at a particular protest, or to try and identify a journalist's confidential source.

**5. Eavesdropping**

1. **Phones can be used to eavesdrop on the owner**

If a phone is infected with the right malware it is possible for its microphone or camera to be turned on remotely allowing somebody to hear or see whatever is happening in the same room as the phone. This may happen even when the phone appears to be switched off.

As a result, people having a sensitive meeting or conversation are sometimes told to turn off their phones off and take out the battery. While this will make sure your phone can’t be used to listen in on you, it does have its own disadvantage: if many people at one location all switch off their phones at the same time, it's a sign to the mobile carriers that they all thought something was worth them turning their phones off, such as a sensitive meeting.

An alternative that might give less information away is to leave phones in another room where the phones' microphones wouldn't be able to overhear the conversations. If you know this wouldn’t be possible, try to take the battery out of your phone before you travel to the meeting.

Don’t forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

**6. General Precautions**

As is the case with other devices, the first line of defence for the safety of the information on your mobile phone is to physically protect the phone and its SIM card from being taken or tampered with.

* Keep your phone with you at all times and avoid leaving it out in public.
* Always use your phone's security lock codes or Personal Identification Numbers (PINs) and keep them secret. Always change these from the default factory settings.
* Draw or make a mark on the SIM card, additional memory card, battery and phone with something unique and not immediately noticeable to a stranger. Place printed tamper-proof security tape over the joints of the phone if it is easily opened. (Tamper-proof security tape can be bought cheaply and easily over the internet) This will help you easily to identify whether any of these items have been tampered with or replaced.
* If your phone is locked, ask someone you trust about unlocking it. A locked phone poses higher risk as it means all your data is controlled by one operator.
* The 15-digit serial or IMEI (International Mobile Equipment Identity) number helps to identify your phone and can be accessed by keying \*#06# into most phones, by looking behind the battery of your phone or by checking in the phone's settings. Make a note of this number and keep it separate from your phone, as this number could help to trace and prove ownership quickly if it is stolen.
* Consider the advantages and disadvantages of registering your phone with the service provider. If you report your phone stolen, the service provider should then be able to stop further use of your phone. However, registering it means your phone usage is tied to your identity.

**7. Protection from malware**

There are also a number of steps you can take that will help avoid your phone being easily infected with malware. This does *not* prevent your phone being infected, it just makes it more difficult to infect.

* Keep your software updated to keep your phone secure. There are two types of updates that need to be checked:
  + The phone operating system: For Androids go to: *settings -> About phone -> updates -> check for updates*
  + Apps you have installed: In Androids, open the Play store app, from the *side menu* select My Apps.
* Do not accept or install any unknown programmes on your phone, such as ring tones, wallpaper, apps or any others that come from an unexpected source. They may contain malware.
* Connect your phone to a computer only if you are sure it is malware free. Learn about how to check in the Malware lesson.
* If you don't know or use any of the features and applications on your phone, disable or uninstall them if you can.
* Try to avoid connecting to WiFi access points that don't provide passwords.
* Make sure communication channels like Infrared (IrDA), Bluetooth and Wireless Internet (WiFi) on your phone are switched off and disabled if you are not using them. Use them only in trusted situations and locations. Consider not using Bluetooth, as it is relatively easy to eavesdrop on this form of communication. Instead, transfer data using a cable.
* When setting up your phone, there are a number of settings you can select and apps you can download that will help make your phone more secure. Instructions for set up can be found in the tools section: Basic Security Setup for Android.

**8. Burner phones**

Phones that are used temporarily and then discarded are often referred to as burner phones. People who are trying to avoid surveillance sometimes try to change phones and numbers frequently to make it more difficult to recognise their communications. They will need to use prepaid phones (not associated with a personal credit card or bank account) and ensure that the phones and SIM cards were not registered with their identity; in some countries these steps are straightforward, while in others there may be legal or practical obstacles to obtaining anonymous mobile phone service.

There are a number of limitations to burners hiding your identity.

* First, just swapping SIM cards offers minimal protection, because the network operator knows the history of which SIM cards have been used in which devices, and can track either individually or both together.
* Second, governments have been developing mobile location analysis techniques where location tracking can be used to generate leads or hypotheses about whether multiple devices actually belong to the same person. There are many ways this can be done. For example, an analyst could check whether two devices tended to move together, or whether, even if they were in use at different times, they tended to be carried in the same physical locations.
* A third problem for the successful anonymous use of telephone services is that people's calling patterns tend to be extremely distinctive. For example, you might habitually call your family members and your work colleagues. Even though each of these people receives calls from a wide range of people, you're likely the only person in the world who commonly calls both of them from the same number. So even if you suddenly changed your number, if you then resumed the same patterns in the calls you made or received, it would be straightforward to determine which new number was yours. Remember that this inference isn't made based only on the fact that you called one particular number, but rather on the uniqueness of the combination of all the numbers that you called.

Together, these facts mean that effective use of burner phones to hide from government surveillance requires, at a minimum:

* Not reusing either SIM cards or devices;
* Not carrying different devices together;
* Not creating a physical association between the places where different devices are used;
* And not calling or being called by the same people when using different devices.
* (This isn’t necessarily a complete list; for example, we haven’t considered the risk of physical surveillance of the place where the phone was sold, or the places where it's used, or the possibility of software to recognize a particular person's voice as an automated method for determining who is speaking through a particular phone.)

**9. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Expert lesson for advice on how to root and encrypt your phone.**

*RELATED LESSONS/TOOLS*

* *Making a Call Lesson*
* *Sending a Message Lesson*
* *Backing Up Lesson*
* *Safe Deleting Lesson*
* *Malware Lesson*
* *ObscuraCam Tool guide*
* *Basic Security Setup for Android guide*

*FURTHER READING*

* [*Security in a Box – Chapter 10, Use mobile phones as securely as possible*](https://securityinabox.org/en/guide/mobile-phones)
* [*Security in a Box – Chapter 11, Use smart phones as securely as possible*](https://securityinabox.org/en/guide/smartphones)
* [*EFF - The problem with mobile phones*](https://ssd.eff.org/en/module/problem-mobile-phones)

***Mobile Phone Basic Checklist***

* ***Do not use regular phone for sensitive calls***
* ***Do not use regular phone for sensitive SMS messages***
* ***Use a code if necessary***
* ***Encrypt your phone***
* ***Don’t store sensitive information on phone***
* ***Regularly erase call records, messages, photos etc.***
* ***Back up your phone***
* ***Don’t leave your SIM card at the repair shop with your phone***
* ***Only use trusted repair shops/ dealers***
* ***Delete data from phone before handing on***
* ***Don’t hand on SIM card or memory card***
* ***Use ObscuraCam for sensitive photos***
* ***Leave phones in different room when having sensitive meetings***
* ***Don’t have sensitive phone calls in public place***
* ***Always keep your phone with you***
* ***Keep your phone locked***
* ***Always change codes from default settings***
* ***Mark your phone, battery and SIM card***
* ***Use tamper-proof security tape***
* ***Get your phone unlocked***
* ***Write down your IMEI number***
* ***Think carefully whether or not you should register your phone***
* ***Regularly update software***
* ***Never accept unexpected programmes***
* ***Only connect phone to malware-free computer***
* ***Only give location permissions to apps you trust***
* ***Disable or uninstall applications you don’t use***
* ***Avoid WIFI that is not password protected***
* ***Keep WIFI, Bluetooth and Infrared off when not in use***
* ***Only use WIFI, Bluetooth and Infrared in trusted locations***

***For burner phones*** *(NO CHECKBOX FOR THIS ONE)*

* ***Use unregistered pre-paid phone, paid for with cash***
* ***Use unregistered pre-paid SIM, paid for with cash***
* ***Do not reuse phone or SIM card for different contacts***
* ***Do not turn on when with your regular phone***
* ***Do not turn on in location associated with you***

*EXPERT*

**1. Get full access to your smartphone**

Firmware is the permanent software that a manufacturer programmes into a device’s read-only memory. They run in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc. Most functionalities are 'locked in' so the user is not capable of controlling or altering these functions. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to alter the programs running the smartphone. The process of overcoming these manufacturer imposed limits on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Successful rooting or jailbreaking will enable you to install additional applications, make modifications, and give you total control over data storage and memory of the smartphone in order to make it more secure.

*WARNING*: Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

* There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
* The manufacturer or mobile carrier warranty may be voided.
* In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

Rooting or jailbreaking is a complex process and different for every device. Search the internet for instructions on the best way to root your own device.

**2. Alternative Firmware**

Rooting your phone will allow you to install alternative firmware.

An example of an alternative firmware for some Android phones is [**Cyanogenmod**](http://www.cyanogenmod.com/) which allows you to uninstall applications from the system level of your phone. By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge. This sort of alternative firmware includes features such as the automatic concealment of your location when online by using a Virtual Private Network as default, and automatic incognito browsing meaning history of your communication is not recorded on your smartphone.

**3. Encryption of volumes**

Rooting your phone will also allow you to encrypt its entire data storage or create a volume on the smartphone to protect certain information.

[**Luks Manager**](https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=en) allows easy, on-the-fly strong encryption of volumes with a user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the Luks Manager provides to store all your data.

The Android Privacy Guard (APG) allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well as when emailing.

You can learn how to install and use it in the K9 & APG Guide in the tool kit.

[**Cryptonite**](https://play.google.com/store/apps/details?id=csh.cryptonite&hl=en_GB)is another open source files encryption tool with more advanced features on it, and specially prepared for rooted Android phones with a custom firmware.

**4. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on the dangers of using mobile phones.**

*RELATED LESSONS/TOOLS*

* *K9 & APG tool guide*

*FURTHER READING*

* [*Security in a Box – Chapter 11, Use smart phones as securely as possible*](https://securityinabox.org/en/guide/smartphones)

***Mobile Phone Expert Checklist***

* ***Check if rooting your phone is right for you***
* ***Install alternative firmware***
* ***Encrypt volumes with Luks Manager***
* ***Encrypt files and emails with APG***

**MAKING A CALL**

*BASIC*

**1. Regular phone calls**

When you make a call from a landline or a mobile phone, your call is not end-to-end encrypted. If you're using a mobile phone, your call may be weakly encrypted between your handset and the cell phone towers. However as your conversation travels through the phone network, it's vulnerable to interception by your phone company and, by extension, any governments or organizations that have power over your phone company. There are also inexpensive techniques which other people can use to listen to your calls if they are close to your phone.

*Regular phone calls to or from your mobile phone are not secure.*

**2. VoIP Calls**

The easiest way to ensure you have good encryption on voice conversations is to use VoIP instead of regular calls. VoIP (Voice over Internet Protocol) refers to calls made using the internet. Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. Good call encryption software is currently only supported on a few models of smart phones.

In order to have end-to-end encrypted VoIP conversations, both parties must be using the same (or compatible) software. Conversations between providers such as Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place.

**3. Making secure calls on your phone**

**Signal**

[Signal](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) is a free, simple open-source tool for having end-to-end encrypted phone calls and also for sending secure messages. It works for both Androids and iPhones and replaces the previous android app called Redphone. (Users with RedPhone installed will be prompted to install Signal instead. If you already have Signal installed, you can just uninstall RedPhone. It will no longer be maintained as an independent app.)

Signal now also incorporates secure messaging app, Textsecure – meaning there is one simple app you can use for both secure calling and messaging, whether on Android or iPhone, as long as the person you are communicating with has Signal too.

Signal uses your existing phone number and address book. There are no separate logins, usernames, passwords, or PINs to manage or lose. It uses your mobile number as your identificator (like a user name) – this makes it easier for the user, though it also makes it easier to analyze the traffic it produces and trace it back to you. Signal uses a central server, which is a point of centralization and thus puts it in the powerful position of having control over some of this data. However they cannot hear your conversations or see your messages, so no one else can either.

**Ostel**

Another notable tool for having end-to-end encrypted phone calls is OStel.It works on every smartphone (Blackberry, iPhone, Nokia, Android) and every desktop (Mac, PC, Linux, etc). It is one of the most secure means to communicate via voice and comes with many easy set-up wizards for different VoIP services, available [here](https://ostel.co/). (The accompanying app for Android phones is CSipSimple.) Both you and the person you want to talk to will need an ostel account. It securely encrypts all your speech and makes it very difficult to trace your data and find out who you are talking to. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use.

**4. Making secure calls on your computer**

**JitsiMeet**

When using voice communication to exchange sensitive information it is important to choose a tool that encrypts the call all the way from your computer to the recipient's computer. We would recommend that you use the free and open-source tool, *JitsiMeet* as your choice for VoIP. It provides a free, easy to use, open source, more secure alternative to Skype and can be used for video and voice and for group video chat. There is no requirement for you or the person you’re communicating with to sign-up. You just visit <https://meet.jit.si> enter a meeting name, (make sure it has no spaces and is difficult to guess), and share the link with whoever you want to speak with. Simple as that.

**Skype**

Beware! Most popular VoIP providers, such as Skype and Google Hangouts, offer transport encryption so that eavesdroppers cannot listen in, but *the providers themselves are still potentially able to listen in*. Depending on your threat model, this may or may not be a problem, but we would recommend that you avoid Skype if you discuss sensitive information. It is important to keep in mind that Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies access to all your communications history.

While we can't recommend Skype as a secure communication tool, it is very important to take some precautions if you still decide to use Skype as a tool for sensitive communication:

* Download and install Skype only from its official website [www.skype.com](http://www.skype.com/) to avoid a Skype program infected with spyware.
* Change your Skype password regularly.
* Set the privacy settings on Skype so that it does not keep a history of chats.
* Disable the Skype setting which automatically accepts incoming files, as this has occasionally been used to introduce malware/spyware onto computers.
* Always independently verify the identity of the person with whom you are communicating. It is easier to do this when voice chatting, especially if you know the person you want to talk to.
* Decide if your Skype username should identify your or have any relationship to your real name, or the name of you organisation.
* Be careful of what you say - develop a code system to discuss sensitive topics without using specific terminology.

**4. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Mobile Phones Lesson*
* *Signal Tool Guide*
* *Jitsi Tool guide*

*FURTHER READING*

* [*EFF - Communicating with others*](https://ssd.eff.org/en/module/communicating-others)
* [*Security in a Box - Secure communication guide*](https://securityinabox.org/en/guide/secure-communication)

***Making a Call Basic Checklist***

* ***Avoid regular phone calls for sensitive conversations***
* ***Use Ostel or Redphone for calls on your phone***
* ***Use Jitsi instead of Skype on your computer***

***If you must use Skype*** *(NO CHECKBOX FOR THIS ONE)*

* ***Download from official website***
* ***Change password regularly***
* ***Adjust settings so you don’t keep chat history***
* ***Verify who you’re speaking to***
* ***Consider using anonymous username***
* ***Use codes for sensitive topics***

**SENDING A MESSAGE**

*BASIC*

**1. Regular SMS Text messages**

SMS messages are not well encrypted so you should not rely on them to transmit sensitive information securely. Sent SMS messages can be intercepted and kept by your service operator or by third parties with inexpensive equipment. Those messages will carry the phone numbers of the sender and recipient as well as the content of the message. What's more, SMS messages can easily be altered or forged by third parties.

If you do need to use SMS for something, consider establishing a code system between you and your recipients. Codes may make your communication more secure and may provide an additional way of confirming the identity of the person you're communicating with. Code systems need to be secure and change frequently.

Saved messages on your phone can easily be accessed by anybody who gets hold of your phone so consider deleting all received and sent messages straightaway.

*Regular SMS text messages to or from your mobile phone are not secure.*

**2. Sending secure SMS on your phone**

**SMSSecure**

SMSSecure is a free, open-source tool for sending and receiving secure SMS text messages on Android phones. It works both for encrypted and non-encrypted SMS, so you can use it as your default SMS application. It automatically imports all your contacts and existing SMS, so only takes a few seconds to set up. No internet connection is required to send or receive SMS. To exchange *encrypted* SMS this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. SMSSecure also encrypts all SMS locally, so if your phone is lost or stolen, your messages are protected.

Many people who previously used TextSecure for secure SMS now use SMSSecure.

You can find SMSSecure on [google play](https://play.google.com/store/apps/details?id=org.smssecure.smssecure) and installation takes only a few clicks.

**2. Sending secure online messages on your phone**

**Signal**

[Signal](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) is a free, simple open-source tool for sending end-to-end encrypted messages and also for having secure calls. It works for both Androids and iPhones and replaces the previous android app called TextSecure. (Users with TextSecure or the old Signal will have already received the update, or can do it manually be visiting the Playstore/Appstore and pressing Update) If you don’t have data or internet access, Signal also operates as a regular *unsecured* SMS messaging service – you just need to hold down on the send button to select the preferred function.

Signal now also incorporates secure voice calling app, Redphone – meaning there is one simple app you can use for both secure calling and messaging, whether on Android or iPhone, as long as the person you are communicating with has Signal too.

Signal uses your existing phone number and address book. There are no separate logins, usernames, passwords, or PINs to manage or lose. It uses your mobile number as your identificator (like a user name) – this makes it easier for the user, though it also makes it easier to analyze the traffic it produces and trace it back to you. Signal uses a central server, which is a point of centralization and thus puts it in the powerful position of having control over some of this data. However they cannot hear your conversations or see your messages, so no one else can either.

**Telegram**

A note on Telegram: While Telegram does use end-to-end encryption in some modes, there have been serious concerns with the quality of their encryption and the amount of information it gathers on users, including their full contact lists. Users must also remember to start a new “Secret Chat”, before encryption is activated. Given these concerns we cannot recommend Telegram as a secure method of communicating.

**ChatSecure**

ChatSecure as a secure text chat application that works for both iPhones and Androids and across a number of platforms. Not only does ChatSecure encrypt your phone to phone messages, it can also operate across a number of platforms, and offers more functions than Signal. ChatSecure offers easy and strong encryption for your chats that provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

See how to set it up in the ChatSecure tool guide.

**3. WhatsApp**

WhatsApp is the most popular mobile communication tool in the world, offering free messaging to individuals and groups and operating on all phone types. Until November 2014, using WhatsApp was considered highly insecure and was not recommend for anyone who required any level of security in their communications. It now offers strong encryption for *some* messages on *some* phones.

Since November 2014, WhatsApp has integrated the secure code of a well-respected privacy and technology company (Open Whisper Systems) into its product. This means that its messages now have a very strong level of verifiable security, and WhatsApp can no longer easily view or be forced to handover messages to authorities.

However it is very important to note:

* This only currently applies to users using WhatsApp on *Android* phones (users on Apple iOS, Windows Phone, Blackberry and Nokia will be only get the same protection at some point in the future.)
* Only for messages from one individual to another individual (ie: not for group chats)
* Does not encrypt any pictures sent once they arrive on the phone
* While WhatsApp or others cannot view the content of your messages, they can still know that you are communication with someone (e.g metadata). In some cases, this may still have negative security consequences.

For these reasons we still recommend that you use [Signal](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) for secure messaging and calls.

**4. Secure online messaging on your computer**

**Pidgin**

Instead of using Skype, Google Talk or MSN Messenger to send messages on your computer we recommend you use the secure, free, open-source tool, Pidgin, instead.

Pidgin is a chat program which lets you log in to accounts on multiple chat networks simultaneously. This means that you can be chatting with friends on MSN, talking to a friend on Google Talk, and sitting in a Yahoo chat room all at the same time. Pidgin runs on Windows, Linux, and other UNIX operating systems.

See how to set it up in the Pidgin tool guide.

**Adium**

Adium is good alternative to Pidgin that works with OS X on Macs. See how to set it up in the Adium tool guide.

**4. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *TextSecure tool guide*
* *ChatSecure tool guide*
* *Pidgin tool guide*
* *Adium tool guide*

*FURTHER READING*

* [*EFF - Communicating with others*](https://ssd.eff.org/en/module/communicating-others)
* [*Security in a Box - Secure communication guide*](https://securityinabox.org/en/guide/secure-communication)

***Sending a Message Basic Checklist***

* ***Avoid regular SMS messages for sensitive texts***
* ***Use TextSecure or ChatSecure for messages on your phone***
* ***Use WhatsApp only if individual Android to Android chat***
* ***Use Pidgin or Adium instead of Skype to instant message on your computer***

**EMAIL**

*BASIC*

**1. Keeping your webmail private – HTTPS**

There are a few important steps that you can take in order to increase the security of your email communication. The first is to make sure that only the person to whom you send a given message is able to read it.

HTTPS, (also referred to as SSL or TLS), encrypts your communications so that it cannot be read by other people on your network. This can include the other people using the same Wi-Fi in an airport or at a café, the other people at your office or school, the administrators at your ISP, malicious hackers, governments, or law enforcement officials. Communications sent over your web browser, including the web pages that you visit and the content of your emails, using HTTP rather than HTTPS are very easy for an attacker to intercept and read.

Most email providers give you a way of accessing your email using a web browser, such as Firefox or Chrome. Of these providers, most of them provide support for HTTPS. You should always make sure that your connection is secure before logging in, reading your email, or sending a message. You can tell that your email provider supports HTTPS if you log in to your webmail and the URL at the top of your browser begins with the letters **HTTPS** instead of **HTTP** (for example: https://mail.google.com).

If your email provider supports HTTPS, but does not do so by default, try replacing HTTP with HTTPS in the URL and refresh the page. If you’d like to make sure that you are always using HTTPS on sites where it is available, download the [HTTPS Everywhere](https://www.eff.org/https-everywhere" \t "_blank) browser add-on for Firefox or Chrome.

Webmail providers that use HTTPS by default include Gmail, RiseUp and Yahoo.

Some webmail providers give you the option of choosing to use HTTPS by default by selecting it in your settings, such as Hotmail.

HTTPS is the most basic level of encryption for your web browsing that we recommend for everybody. It is as basic as putting on your seat belt when you drive.

**2. Switching to a more secure email account**

While using HTTPS protects your communications from other people on your network, there are some things that it does not do. When you send email using HTTPS, your email provider still gets an unencrypted copy of your communication. Governments and law enforcement may be able to access this data with a warrant.

Yahoo and Hotmail, for instance, provide a secure connection *only* while you log in, to protect your password, but your messages themselves are sent and received insecurely. They also insert the IP address of the computer you are using into all of the messages you send. We do not recommend that you use them for secure communications.

**Gmail**

Gmail accounts, on the other hand, use a secure connection during log-in and all the way until you log out and, unlike Yahoo or Hotmail, Gmail avoids revealing your IP address to email recipients. One way to make Gmail (or Yahoo) even more secure is to turn on 2-step-verification. This is one of the safest and simplest computer-security measures. To break into an account with 2-Step Verification, intruders would not only have to know your username and password, they'd also have to get a hold of your phone, or codes you hold with you. Setting it up is simple: [see here](https://support.google.com/accounts/answer/185839?hl=en).

However, it is not recommend that you rely on Google for the total confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom.

**RiseUp**

If possible, you should create a new RiseUp email account by visiting https://mail.riseup.net. RiseUp offers free email to activists around the world and takes great care to protect the information stored on their servers. Unlike Google, they have very strict policies regarding their users' privacy and no commercial interests that might some day conflict with those policies. In order to create a new RiseUp account, however, you may need two 'invite codes.' These codes can be given out by anyone who already has a RiseUp account. Otherwise, you will need to tell RiseUp about yourself and they may give you access.

**3. Recipient security**

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. You yourself are only part of the picture.

* Even if you access your email account securely, consider what precautions your contacts may or may not take when sending, reading and replying to messages.
* Try to learn where your contacts' email providers are located, as well. Naturally, some countries are more aggressive than others when it comes to email surveillance. To ensure private communication, you and your contacts should all use secure email services hosted in relatively safe countries.
* And, if you want to be certain that messages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. RiseUp is one good choice.

**4. Tips on improving your email security**

* Always be careful when opening email attachments that you are not expecting, that come from someone you do not know or that contain suspicious subject lines. When opening emails like this, you should ensure that your anti-virus software is up-to-date and pay close attention to any warnings displayed by your browser or email program. See more about this in the Malware lesson.
* Using anonymity software like Tor, which is described in the Internet lesson, can help you hide your chosen email service from anyone who might be monitoring your Internet connection.
* When creating an account that you intend to use while remaining anonymous from your own email recipients, or from public forums to which you might post messages by email, you must be careful to avoid using Hotmail, Yahoo, or any other webmail provider that includes your IP address in the messages you send.
* You may consider using several different, anonymous email accounts for communicating with different groups of people to protect of your contact network. You may also use different email accounts for signing up to Internet services which require email accounts.
* After all above precautions it is still very important to beware of what you write in the messages and what impact would it have if it fell into the wrong hands. One way of increasing the security of information exchange is to develop a code system for sensitive information exchange, so you would not use real names of the people, real addresses of places, etc.
* Remember that secure email will not do you any good if everything you type is recorded by spyware and periodically sent over the Internet to a third party. The Malware lesson and offers some advice on how to prevent this sort of thing, and the Passwords lesson will help you protect your accounts.

**5. Email on Smartphones**

In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

* Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
* If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands. See the Advanced section of this lesson for details on how to do so.

**6. Signs your email has been hacked**

If you suspect your email account has been hacked or compromised, you can take steps to reduce the damage done. While it is difficult to be certain, there may be clues such as:

* You notice any changes to your email account content or settings that you didn't make;
* Your email contacts notify you that they have received an email that you didn't send;
* You cannot login to your email account, though you are sure your password and other settings are correct;
* You are regularly not receiving some email messages from your colleagues that they insist that they sent to you;
* Some private information that was sent or received exclusively by email was made known to a third party, though neither you nor your correspondent shared it with anyone else;
* If on your account activity log (if your email provider offers one) you see that your account was accessed at time that you do not remember or from a place (or IP address) that you did not go to.

**7. What to do if your email is hacked**

In such situations you may want to take some cautionary action:

* **Stop using this email account for sensitive information exchange**, at least until you understand the situation better.
* **Change your password** for this and all other accounts with a similar password as soon as possible.
* **Change your security question answers** (if you use them) for all accounts, so they are impossible to guess, or find the answer through researching information about you.
* **If you are not able to log in** to your account to change the passwords, consider getting in contact with your email provider to try to reclaim your account.
* **Mitigate information loss and impact** to your community. Determine what kinds of sensitive information and contacts you had in your account and decide whom you should alert. Determine what services (web, financial, etc.) you need to revisit or cancel. It is important that you **check the folders of your account** to research on what could have been sent from your account and to act accordingly.
* **Review your account settings** to see possible changes that has been made. Check accounts signature option for links and malware, forwarding options that would allow to copy emails that you receive to third account, away message, display name, etc.
* **Research how your account was compromised.** Was it because of having a weak password, or due to malware infection, etc. The more you will establish about this, the better you will be able to respond to the situation and better you will be able to protect your contacts.
* **Review security of all of your devices** that access emails from this account, and devices on which you stored the password to this email account. Scan your computer: learn how in the Malware lesson. Consider switching to more secure programs like Firefox, Thunderbird, LibreOffice and other Free and Open Source Programs. After making the above improvements to the security of your devices, change your account passwords again to new, stronger ones.
* **Consider reporting hacking** of your account to your email provider.
* **Consider using a more secure account**, e.g. one that notifies you of and prevent access from unusual places or devices. Consider using account that is hosted outside of your country. Consider using email encryption, such as PGP, outlines in the Advanced email lesson.
* **Consider avoiding storing read emails**.

It is important that you act quickly and precisely in the situation like this. Having a prepared and rehearsed plan may help you.

**8. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on how to send encrypted emails for sensitive information.**

*RELATED LESSONS/TOOLS*

* *Malware lesson*
* *Internet lesson*
* *Passwords lesson*

*FURTHER READING*

* [*Security in a Box - Secure communication guide*](https://securityinabox.org/en/guide/secure-communication)

***Email Basic Checklist***

* ***Make sure it says HTTPS in browser before you log in***
* ***Download the HTTPS Everywhere browser add-on***
* ***If using Gmail, set up 2-Step Verification***
* ***Create a RiseUp account if possible***
* ***Use secure email services hosted in safe countries***
* ***Use same email provider as sensitive contacts***
* ***Be careful opening email attachments***
* ***If needed, use different email accounts for different groups***
* ***If needed, use a code for sensitive information***
* ***Use strong passwords***
* ***Protect your computer from malware***
* ***Do not use phone as primary means for email***

**If your email has been hacked** (no check box)

* ***Don’t send any sensitive information***
* ***Change your password***
* ***Change your security questions***
* ***Reclaim your account***
* ***Determine who to alert/what to cancel***
* ***Find out how you were compromised***
* ***Review security on all devices***
* ***Consider reporting it***
* ***Consider moving to more secure account***
* ***Avoid storing read emails***

*ADVANCED*

**1. What is PGP?**

If your threat model includes a government or law enforcement, or you have some other reason for wanting to make sure that your email provider is not able to turn over the contents of your email communications to a third party, you may want to consider using end-to-end encryption for your email communications. End-to-End Encryption is uninterrupted protection of data traveling between two communicating parties.

PGP is the standard for end-to-end encryption of your email. PGP stands for Pretty Good Privacy. It's actually very good privacy. If used correctly, it can protect the contents of your messages, text, and even files from being understood even by well-funded government surveillance programs.

**2. Public Key Encryption**

PGP is built upon the concept of Public Key Encryption. This is a cryptographic system that uses two keys -- a public key known to everyone and a private key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

* So public key encryption lets you encrypt and send messages safely to anyone whose public key you know.
* If others know your public key, they can send you messages, which only you can decode.
* And if people know your public key, you can sign messages so that those people will know they could only have come from you.
* And if you know someone else's public key, you can decode a message signed by them, and know that it only came from them.

You should keep your private key stored somewhere safe, and protected with a long password. (If someone else gets a copy of your private key, they can pretend to be you, and sign messages claiming that they were written by you.) You can give your public key to anyone you want to communicate with you, or who wants to learn whether a message truly came from you.

**3. Using PGP**

Unfortunately, PGP has a reputation for being difficult to understand, or use. The good news is that there are many programs available now which can hide the ancient design of PGP and make it somewhat easier to use, especially when it comes to encrypting and authenticating email—the main use of PGP.

For detailed instructions on how to install and use PGP encryption for your email, see:

* [How to: Use PGP for Mac OS X](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x" \t "_blank)
* [How to: Use PGP for Windows](https://ssd.eff.org/en/module/how-use-pgp-windows-pc" \t "_blank)
* [How to: Use PGP for Linux](https://ssd.eff.org/en/module/how-use-pgp-linux" \t "_blank)

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Learn how to install and use encryption for email on your smartphone in the [*K9 and APG Guide*](https://securityinabox.org/en/K9_APG_main).

**4. What PGP Can’t Do: Metadata**

PGP is all about making sure the *contents* of a message are secret, genuine, and untampered with. But that's not the only privacy concern you might have. PGP does not protect your metadata—which is everything else, including the subject line of your email, or who you are communicating with and when. Metadata can provide extremely revealing information about you even when the content of your communication remains secret.

If you're exchanging PGP messages with a known dissident in your country, you may be in danger for simply communicating with them, even without those messages being decoded. Indeed, in some countries you can face imprisonment simply for refusing to decode encrypted messages.

Protecting your metadata will require you to use other tools, such as Tor, at the same time as end-to-end encryption. You can learn how to do this in the Internet lesson.

**5. Sharing your public PGP key**

The tool guides for PGP will explain in detail about how to create your public PGP key and how you might want to share it. In general, it’s good to keep in mind that if you are working in a dangerous environment and if would use a pseudonym generally, use that pseudonym (and alternative email) when labelling your key.

Disguising that you are communicating with a particular person is more difficult. One way to do this is for both of you to use anonymous email accounts, and access them using Tor. If you do this, PGP will still be useful, both for keeping your email messages private from others, and proving to each other that the messages have not been tampered with.

**6. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to improve basic email security and know if my email has been hacked.**

*RELATED LESSONS/TOOLS*

* *Internet lesson*
* *PGP for Mac O SX tool guide*
* *PGP for Windows tool guide*
* *PGP for Linux tool guide*
* *K9 & APG tool guide*

*FURTHER READING*

* [*EFF - Public key cryptography and PGP*](https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp)

***Email Advanced Checklist***

* ***Install and use PGP***
* ***If you need to protect your metadata, use Tor***
* ***Consider using pseudonym with your public key***
* ***To disguise contact completely, both parties use anonymous email accounts, Tor and PGP***

**THE INTERNET**

*BASIC*

**1. How To Circumvent Online Censorship**

Many governments, companies, schools, and public access points use software to prevent Internet users from accessing certain websites and Internet services. This is called Internet filtering or blocking and is a form of censorship. Content filtering comes in different forms. Sometimes entire websites are blocked and sometimes content is blocked based on keywords contained in it. One country might block Facebook entirely, or only block particular Facebook group pages—or it might block any page or web search with certain words in it.

Regardless of how content is filtered or blocked, you can almost always get the information you need by using a circumvention tool. Circumvention tools usually work by diverting your web or other traffic through another computer, so that it bypasses the machines conducting the censorship.

There are different ways of circumventing Internet censorship, some of which provide additional layers of security that you may need. The tool that is most appropriate for you depends on your threat model. If you’re not sure what your threat model is, you should work it out using the Managing Information lesson. Users with a high threat model who need to ensure total anonymity online should use tools outlined in the Advanced lesson.

**2. HTTPS**

HTTPS is the secure version of the HTTP protocol used to access websites. Sometimes a censor will block the insecure version of a site only, allowing you to access that site simply by entering the version of the domain that starts with HTTPS. This is particularly useful if the filtering you're experiencing is based on keywords or only blocks individual web pages. HTTPS stops censors from reading your web traffic, so they cannot tell what keywords are being sent, or which individual web page you are visiting (*censors can still see the domain names of all websites you visit*).

If you suspect this type of simple blocking, try entering https:// before the domain in place of http://.

Try EFF’s [HTTPS Everywhere](https://www.eff.org/https-everywhere" \t "_blank) plug-in to automatically turn on HTTPS for those sites that support it.

**3. Website variations**

Another way that you may be able to circumvent basic censorship techniques is by trying an alternate domain name or URL. For example, instead of visiting http://twitter.com, you might visit http://m.twitter.com, the mobile version of the site. Censors that block websites or web pages usually work from a blacklist of banned websites, so anything that is not on that blacklist will get through. They might not know of all the variations of a particular website's domain name—especially if the site knows it is blocked and registers more than one name.

**4. Web-based proxies**

A web-based proxy (such as <https://proxy.org/>) is one of the simplest ways of circumventing censorship. It is a website that lets its users access other, blocked or censored websites. In order to use a web-based proxy, all you need to do is enter the filtered address that you wish to use into the box in the proxy webpage; the proxy will then display the requested content inside its own webpage.

Web-based proxies are a good way to quickly access blocked websites, but they have certain disadvantages, as well.

* They often don’t provide any security and will be a poor choice if your threat model includes someone monitoring your internet connection.
* They do not always display pages correctly, and many web-based proxies will fail to load complex websites, including those that feature streaming audio and video content.
* And, of course, web-based proxies only work for webpages. You cannot, for example, use an instant messaging program or an email client to access blocked services through a web-based proxy.
* Finally, web-based proxies themselves pose a privacy risk for many users, depending on their threat model, since the proxy will have a complete record of everything you do online.

There are numerous proxy tools that use encryption, providing an additional layer of security, as well as the ability to bypass filtering. Although the connection is encrypted, the tool provider may have your personal data, meaning that these tools do not provide anonymity. They are, however, more secure than a plain web-based proxy. The simplest form of an encrypted web proxy is one that starts with “https”—this will use the encryption usually provided by secure websites.

**5. Virtual Private Networks**

A Virtual Private Network (VPN) encrypts and sends all Internet data between your computer and another computer. This computer could belong to a commercial or non-profit VPN service, your company, or a trusted contact. A proxy server is mainly for web traffic only, but a VPN encrypts and protects all traffic. The main difference is that a VPN server encrypts your data, but a proxy server does not. A VPN also lets you use more than just the Internet – you can use it to access webpages, e-mail, instant messaging, VoIP and any other Internet service.

**Psiphon3**

Psiphon3 is a secure, public circumvention tool that combines VPN, SSH and HTTP Proxy technology to provide you with uncensored access to Internet content. It is available free online for Windows and Android. You can learn how to use it in the Psiphon3 tool guide.

Because Psiphon 3 is VPN-based, it is able to proxy all of your Internet traffic, not just websites. It should be noted that although Psiphon is does not allow individual user’s IP addresses to be associated with any individual website visited, Psiphon is intended primarily as a censorship evasion tool, rather than one that guarantees anonymity.

For information about other VPN services and to figure out which one might be right for you, click [here](http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/" \t "_blank). Do not use a VPN that you do not trust.

While a VPN protects your traffic from being intercepted locally, your VPN provider can still keep logs of what websites you access or even provide a third party with the ability to snoop directly on your web browsing. Depending on your threat model, the possibility of a government listening in on your VPN connection or obtaining the logs may be a significant risk and, for some users, could outweigh the short-term benefits of using a VPN. These users, or anyone who requires total anonymity online, should use Tor, as described in the Advanced lesson.

**6. Circumventing censorship from your smartphone**

Using your smartphone to go online is often risker than using a computer. You can reduce your risks through the use of these tools.

Using a VPN on your mobile will give you uncensored access to Internet content while encrypting what you do. We recommend using the Psiphon3 tool, outlined above, which works on Androids as well as Windows.

Users with a high threat model who need to ensure total anonymity online should use tools outlined in the Advanced lesson of this lesson.

**7. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on how to ensure you stay anonymous online.**

*RELATED LESSONS/TOOLS*

* *Managing Information lesson*
* *Psiphon3 tool guide*
* *Proxy Mobile tool guide*

*FURTHER READING*

* [*EFF - How to circumvent online censorship*](https://ssd.eff.org/en/module/how-circumvent-online-censorship)
* [*EFF - Choosing the VPN that's right you*](https://ssd.eff.org/en/module/choosing-vpn-thats-right-you)
* [*Floss manuals - Bypassing censorship*](http://en.flossmanuals.net/bypassing-censorship/)
* [*OpenNet - Outlining internet restrictions*](https://opennet.net)

***The Internet Basic Checklist***

* ***Assess your threat model***
* ***Download HTTPS everywhere***
* ***Use domain name variations***
* ***Use a web-based proxy***
* ***Check which VPN is right for you***
* ***Download and use Psiphon3***

***For smartphones*** (no checkbox)

* ***Download and use Psiphon3***

*ADVANCED*

**1. Anonymity Online**

Accessing information on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. You can reduce your risks through the use of anonymising tools such as Tor.

**Remember, these tools can only protect your anonymity if you do not log in to sites or post something online that could identify you!**

**2. Tor**

Tor is free and open-source software that provides anonymity as well as allowing you to circumvent censorship. When you use Tor, the information you transmit is safer because your traffic is bounced around a distributed network of servers. This can provide anonymity, since the computer with which you’re communicating will never see your IP address, but instead will see the IP address of the last Tor router through which your traffic travelled.

One of Tor's strengths is that it does not just work with a browser but can be used with various types of Internet software. Email programs, including Mozilla Thunderbird, and instant messaging programs, including Pidgin, can operate through Tor, either to access filtered services or to hide your use of those services.

Tor is the gold standard for secure censorship circumvention. It can be slow and tricky to use. However, it also provides a reliable, secure and public means of circumvention that saves you from having to worry about whether or not you trust the individuals who operate your proxies and the websites you visit. Tor is open source and can be downloaded free online for Windows, Mac, Linux, and Android.

To learn how to install and use Tor, see the Tor for Mac tool guide or Tor for Windows tool guide.

**3. Anonymity online on your mobile**

**Orbot and Orweb**

Orbot is a free proxy app that enables other apps to use the internet more securely. It uses Tor to encrypt your Internet traffic and then hides it by bouncing through a series of computers around the world. This process takes a little longer, but the strongest privacy and identity protection available is worth the wait.

To learn how to install and use Orbot, see the Orbot tool guide.

Orweb is the safest browser on Android. Orbot and Orweb together circumvent web filters and firewalls, and offer a truly private internet connection. Both apps are available for Android and iPhone.

To learn how to install and use Orweb, see the Orweb tool guide.

**Remember, these tools can only protect your anonymity if you do not log in to sites or post something online that could identify you!**

**4. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to circumvent censorship.**

*RELATED LESSONS/TOOLS*

* *Tor for Mac tool guide*
* *Tor for Windows tool guide*
* *Orbot tool guide*
* *Orweb tool guide*

*FURTHER READING*

* [*Security in a Box - Anonymity and circumvention*](https://securityinabox.org/en/guide/anonymity-and-circumvention)

***The Internet Advanced Checklist***

* ***Install and use Tor***
* ***On mobile install and use Orbot and Orweb***

**SOCIAL MEDIA**

*BASIC*

**1. Protecting Yourself on Social Networks**

Social networking sites are some of the most popular websites and tools we use on the Internet. Facebook, Google+, and Twitter have hundreds of millions of users each. With social networking platforms come many benefits, such as the unprecedented opportunity to communicate, publish, coordinate, and persuade. Many people use it for their professional as well personal lives. But, this also means that we're sharing a lot about ourselves online, usually more than we realise. In some cases, this can put our operations, our contacts, or us at risk.

When using social networks it is important to consider:

* How can I interact while protecting myself, my identity, my privacy and my contacts?
* What information do I want keep private and who do I want to keep it private from?

Depending on your circumstances, you may need to protect yourself against the social media site itself, against other users of the site, or both.

**2. Take care registering**

* Consider whether you want to use your real name or not. Might you want to share things that could be dangerous if they were linked to you?
* When you register, don't provide more information than is necessary. Do you really need to include your birthday/contact number/employment details?
* If you are concerned with hiding your identity, *use a separate email address*. Be aware that your IP address may be logged at registration, so for full, guaranteed anonymity you may want to use a VPN or even Tor.
* Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities.
* Choose a strong password, change it regularly and, if possible, enable two-factor authentication.
* Beware of password recovery/security questions whose answers can be mined from your social media details. For example: “What city were you born in?” or “What is the name of your pet?” You may want to choose password recovery answers that are false. One good way to remember the answers to password recovery questions, should you choose to use false answers for added security, is to note your chosen answers in a password safe. See the Password lesson for more information on how to choose and remember strong passwords.
* Only connect to people you know personally and trust.

**3. Check the Site's Privacy Policy**

Remember that information you post on most social media sites does not belong you – it is subject to the sites own policies and they can use it or share it with others. We know that reading privacy policies is a near-impossible task, but you may want to take a look at sections on how your data is used, when it is shared with other parties, and how the service responds to law enforcement requests.

Social networking sites often collect sensitive information beyond what you actually post—where you are, what interests and advertisements you react to, what other sites you've visited (e.g. through "Like" buttons). Be aware of what you like and repost if they may put you at risk. It can be helpful to block third-party cookies and use tracker-blocking browser extensions to make sure such information isn't being passively transmitted to third parties.

Some social networking sites, like Facebook and Twitter, have business relationships with data brokers in order to target advertisements more effectively. You can see guides that walk you through how to opt-out of these tracking schemes here:

* How to opt-out of Facebook's data broker relationships
* How to opt-out of Twitter's data broker relationships

**4. Change Your Privacy Settings**

Specifically, change the default settings. For example:

* Do you want to share your posts with the public, or only with a specific group of people?
* Should people be able to find you using your email address or phone number?
* Do you want your location shared automatically?
* See here for: How to change your Facebook privacy settings

Remember, privacy settings are subject to change. Be sure to pay attention to these changes closely to see if any information that was once private will be shared, or if any additional settings will allow you to take more control of your privacy.

**5. Think about what you share**

Always ask the questions:

* + Who can access the information I am putting online?
  + Who controls and owns the information I put into a social networking site?
  + What information about me are my contacts passing on to other people?
  + Will my contacts mind if I share information about them with other people?
  + Do I trust everyone with whom I'm connected?

Be careful about putting too much information into your status updates – even if you trust the people in your networks. It is easy for someone to copy your information or unintentionally share something.

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have?

**6. Sharing videos/photos**

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first. As a good rule of thumb, don't post information, images, or updates about people you know if *they* aren't posting about themselves.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

[Guardian Project](https://guardianproject.info/) has created an open-source app called **ObscuraCam** to detect/select faces on photos and blur them. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

**7. Check what your friends share about you**

Remember that you’re not the only person who can give away potentially sensitive data about yourself**.**Your friends can tag you in photos, report your location, and make their connections to you public in a variety of ways. You may have the option of untagging yourself from these posts, but privacy does not work retroactively. You may want to talk to your friends about what you do and do not feel comfortable having them share about you in public.

**8. Think about what you join**

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

**9. Don’t rely social media sites**

**Don’t use social media sites for instant chats**

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most *insecure* ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

*Never* engage in chats with people you don’t know, especially those who want to send you documents or pictures. This is a method commonly used by authorities to put malware in activists’ computers.

You should use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the Sending a Message lesson or Pidgin tool guide to find out how.

**Don’t rely on social media for storage**

Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable.

**10. Access sites securely**

Access social networking sites using **https://**to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.

Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine.

**11. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Password lesson*
* *How to opt-out of Facebook's data broker relationships*
* *How to opt-out of Twitter's data broker relationships*
* *How to change your Facebook privacy settings*
* *ObscuraCam tool guide*
* *Sending a Message lesson*
* *Pidgin tool guide*

*FURTHER READING*

* [*EFF - Protecting yourself on social networks*](https://ssd.eff.org/en/module/protecting-yourself-social-networks)
* [*Security in a Box - Social networking tools*](https://securityinabox.org/social_networking_tools)

***Social Media Basic Checklist***

* ***Consider using a pseudonym***
* ***Don’t provide more registration information than necessary***
* ***Consider registering anonymously***
* ***Consider separate accounts for campaigns***
* ***Choose a strong password***
* ***Use two-factor-authentication***
* ***Use false answers to security questions***
* ***Only connect to people you know***
* ***Be aware of the privacy policy***
* ***Opt out of data broker relationships***
* ***Change default privacy settings***
* ***Be careful about what you share***
* ***Don’t post about people without their consent***
* ***Use ObscuraCam for sensitive photos***
* ***Agree with friends what they shouldn’t post about you***
* ***Be careful about joining groups***
* ***Don’t use social media for instant chats***
* ***Never engage with people you don’t know***
* ***Don’t rely on social media for storage***
* ***Use https://***
* ***Delete browsing history when using public computers***

**RADIOS & SATELLITE PHONES**

*BASIC*

**1. Why Radio**

Radios are an insecure method of communication and should not be used for senstive communication if at all possible. If possible, use alternative options as outlined in the Making a Call lesson. However many in the humanitarian field still need to use them sometimes. If necessary, develop a system of code words between those communicating so that your message will not be so easily understood.

**2. VHF radios**

Very High Frequency (VHF) radios operate in the 30 to 300 MHz range. Usually handheld, they can communicate over short ranges, approximately 10 kilometers, in most cases. They are often referred to as “line of sight,” though in many circumstances they can effectively reach beyond that. Thick trees and buildings can obstruct VHF signals. Elevating the VHF antenna may improve the radio’s transmission range. Also, installing a repeater, which automatically receives and re-transmits radio signals, can further extend the range. Repeater systems are reliable and require little maintenance. Before using a VHF radio or repeater, it may be necessary to obtain authorisation from the host government.

The advantages of VHF radios are:

• Fairly inexpensive;

• User-friendly;

• Sturdily built: can be dropped, withstands rain, etc.;

• Well-positioned repeaters can increase area coverage; and

• 24-hour contact if users are monitoring the VHF.

Disadvantages are:

• Not secure – anybody can listen in;

• Limited battery life (need for spare batteries/ongoing recharge);

• Badly placed repeaters greatly limit the utility of the network;

• Hand-held units are frequently lost or stolen;

• Repeaters are very vulnerable to intentional damage; and

• Highly dependent on the topography of the area (handset-to-handset, 2–

5km; handset to base, mobile or repeater, 7–15km. Obstacles in between, such as high buildings or hills, will interfere with the signal; positioning on a high point can increase range).

The most commonly used brand is Motorola.

**3. High Frequency radios**

HF (High Frequency) radios, in the 3 to 30 MHz frequency range, allow voice communications over medium and long range (conceivably around the world). Less affected by obstacles, HF signals can “bend” around hills and buildings and do not require repeaters to function over long ranges. However, the transmission range of HF signals may be influenced by time of day, weather conditions, electrical interference, and poor system configuration. It takes skill to achieve reliable HF connectivity over long distances. HF radios are often installed in vehicles or at base stations. HF systems are generally more expensive than VHF and require more maintenance.

The advantages of HF radios are:

• Short- to extremely long-range communication without a relay station;

• Less affected by topographical variation;

• High degree of independence;

• Easy to network, with multiple stations sharing the frequency;

• Messages can be sent simultaneously to multiple destinations;

• Monitoring is simple;

• Well-adapted for use in vehicles;

• Adaptable to changing operational conditions;

• Relatively cheap to purchase; no call charges;

• Relatively easy to diversify functions of the network (voice, fax, GPS tracking, SITOR or PACTOR data transmission);

• Possible to integrate with other networks (phone/email); and

• Requires limited maintenance.

The disadvantages are:

• Not secure – anybody can listen in;

• Requires registration and licensing in most countries;

• Transmission strength varies during the day depending on solar activity;

• ‘skip zone’: no reception between maximum extent of direct wave (ground wave) and longer radius starting with the closest reflections from the ionosphere;

• Staff have to be trained in order to take full advantage of the network; and

• Technical expertise needed for installation, and HF can interfere with other electronic equipment if not installed correctly.

**4. Capabilities**

A radio set should have the following capabilities.

• Remote diagnostics: one unit can interrogate another to get details on operational factors such as power output, signal strength and battery voltage. This allows for diagnosis of potential impediments by a technician who does not have to be physically present at the unit.

• Emergency call: distress signals are automatically sent out to a number of pre-programmed stations, prioritising the urgency of the call for the receiver.

• A GPS connected to a personal computer with tracking software installed can interrogate a GPS connected to a mobile unit without the occupants of the vehicle being aware that this is happening. Vehicle movements can thus be monitored. Carefully consider the risks of others monitoring such tracking software before applying it.

The most commonly used brands of HF radios are Codan and Barrett.

**5. Radio procedures**

The benefits of radio equipment can be maximized by following simple standard radio procedures.

* Equipment is maintained in optimum condition.
* Staff and visitors are trained in the use of radios.
* All authorized frequencies and selective calling lists are posted at base stations and in mobile units.
* Radios are monitored 24 hours a day in moderate, high, or severe risk alert countries.
* Each communication has clarity, brevity and security. To ensure effective communication, use the following procedures:
  + Ensure no one else is transmitting at the same time. Wait for ongoing discussions to finish and the users to sign off before beginning transmission.
  + Make message brief but precise.
  + Use common procedure words.
  + Use call signs instead of personal names. Do not identify organizations or personnel by name over the radio.
  + Break the message into sensible passages with clear pauses between.
  + Maintain clear speech with normal rhythm and moderate volume.
  + Hold the microphone approximately five centimeters from mouth.
  + Avoid excessive calling. Use radios for work-related purposes only.
  + Never transmit specific security-related information or travel plans or discuss transfer of cash or goods.
* Use of duress code words is encouraged for all risk levels. Duress code words are generally innocuous words or phrases selected for use over the radio or telephone to indicate that the speaker is in a threatening situation but not free to communicate.

**6. What now?**

**Swipe right for this lesson’s checklist**

Go to the Advanced lesson for advice on using a satellite phone securely.

*RELATED LESSONS/TOOLS*

* *Making a Call*

*FURTHER READING*

* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)

***Radio & Satellite phones Basic Checklist***

* ***Avoid radios for sensitive communications***
* ***Ensure proper training in radio usage***
* ***Use code words if necessary***
* ***Pre-program distress signals***
* ***Carefully consider use of GPS tracking software***
* ***Do not identify organisations or individuals over radio***
* ***Never transmit security-related information or travel plans***
* ***Set duress code words***

*ADVANCED*

**1. Why Satellite Phones**

Satellite phones, which provide high-quality, direct-dial voice, fax, and e-mail, are often used to supplement a radio network, especially in moderate- to high-risk areas. Today’s satellite terminals are rugged, portable, and may be cheaper to operate than cellular phones in some areas. Modern satellite phone networks encrypt voice traffic to prevent eavesdropping and so are usually thought of as safer than radios. However, anyone with cheap computer equipment and radio could eavesdrop on calls by breaking this encryption quite easily.

**2. Dangers of Tracking**

Satellite phones can be tracked with ease. Detecting radio frequency emissions is relatively simple for a trained technician with many commercially available tracking devices. Satellite phones can also be tracked through their own built-in GPS devices. GPS location data may be transmitted by a sat phone in the clear.

**3. Recommended Protocols**

Experts recommend strict protocols when using satellite phones in a hostile environment:

* Avoid using a satellite phone (or any radio frequency-based device) from the same location more than once.
* Avoid using a satellite phone or similar device from a location that cannot be easily evacuated in case of attack.
* Keep the maximum length of any transmission to 10 minutes. (Some experts warn that even this could be too long, as instantaneous tracking is at least possible.)
* Turn off the machine and remove its battery as soon as the transmission is over and before traveling.
* Avoid having multiple parties transmit from the same location.

**4. Dangers of Breaking Encryption**

Satellite transmissions, while encrypted, are not entirely secure either. Many governments are now capable of defeating encryption.

* You should use code words in highly sensitive transmissions, or avoid satellite phones entirely for such communications.

If your satellite phone is confiscated, authorities or hostile actors can access critical information from its call log, phone book, and sent folder.

* You should routinely delete call logs and sent folders to protect your sources, and that you keep the sim card separate from the phone when not transmitting.

**5. What now?**

**Swipe right for this lesson’s checklist**

**Go the Beginner lesson for advice on using radios.**

*RELATED LESSONS/TOOLS*

* *Making a Call*

*FURTHER READING*

* [Committee to Protect Journalists](https://cpj.org/reports/2012/04/armed-conflict.php#6)
* [Small World News](http://smallworldnews.tv/Guide/Guide_SatPhone_English.pdf)

***Radio & Satellite phone Advanced Checklist***

* ***Avoid using from the same location more than once***
* ***Avoid using from a location that cannot be easily evacuated in case of attack***
* ***Keep transmission under 10 minutes***
* ***Turn off and remove battery as soon as the transmission is over and before traveling***
* ***Avoid having multiple parties transmit from the same location***
* ***Use code words in highly sensitive transmissions, or avoid satellite phones entirely***
* ***Routinely delete call logs and sent folders***
* ***Keep the sim card separate from the phone when not transmitting***