Phones

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

Dealing with Harassing Calls, Texts, and Messages

Legal Options

Depending on the method and extent of the harassment, legal remedies may be available. Legal options can be started by you (such as a Peace Bond requested by you and granted by a judge that can "keep the peace" and restrict the abusive person from doing certain things, such as coming near you or calling you. Note that if a Peace Bond is violated, the behaviour can be charged as a crime). Other legal options involve a criminal investigation conducted by the police that may result in a criminal charge and prosecution of the abusive person. You would need to talk to police or get legal advice if you want to explore these options.

Report to the Police

If you report the harassment to the police, they will investigate to determine whether the abusive person has committed a crime, such as criminal harassment, stalking or, based on other things that the abusive person is doing, whether another crime has been committed. When the police investigate, they will collect and assess the evidence they can obtain to determine if a criminal charge is supported.

You may be able to help the police by providing documentation of the harassment. Keep in mind that this documentation is a piece of evidence that may show that a crime has occurred. The police will need to do their own investigation as well.

Document the Harassment

Whether you seek a peace bond or report it to the police, having some documentation (collecting screenshots or recording date/time/notes for the abuse) of the abuse could be helpful. You may want to document the harassment because sometimes you may be the only person to have access to it. Depending on how the harassment occurs or the technology platform on which it took place, the messages may be deleted and not retrievable later on.

Talk to the police, a lawyer, or anti-violence worker in your community to learn about what type of evidence would be most useful for the legal options you want to pursue. These professionals will have a more thorough understanding of local laws, local police, and court procedures.

For some people, documenting and keeping a record of the harassment they are experiencing may feel validating; but for others, it may feel traumatic or triggering. Do what feels best for you. Speaking with an anti-violence worker or legal advocate may be helpful to consider your next steps.

For more information, see our handout on documentation tips and log template. If you are not ready to talk to someone, check out our Preserving Digital Evidence Toolkit for more information and suggestions about how to document evidence and what to include.

Report Harassment to the Technology Company

You may also want to report the harassment to the tech company. Most technology companies have policies that do not allow users to misuse their platform to harass another person. If they confirm that someone is violating their policy by harassing another person through their platform, they may remove the offending message(s), tell the person to stop, and, in rare cases, ban the person from the platform.

Telephone Company

If the harassment is occurring via phone calls or text messages through a telephone provider, consider reporting it to your wireless company.

Reporting to the phone company may be an option if the harassment isn't at the point where the police can investigate. Keep in mind that through this process, the person making the harassing calls **may** be informed of who made the complaint – you. If you do not want the abusive person to know who made the complaint, this might not be the best option.

Social Media

If the harassing message is made through a social media or a messaging app (such as Snapchat or Facebook messenger), you can report the harassment to the social media company. How the company responds to harassment will depend on its terms of use or community guidelines; in some cases, these guidelines may be narrowly defined and the harassment may not fall under their prohibited content. If the harassment is prohibited, the company may remove the offensive content and encourage you to block the harassing person. In rare cases, the company may suspend the harassing person's account.

Tip: Always document the message and the profile information of the person sending or posting the messages before you report the message and the company removes it. Once the social media company deletes it, it is gone forever.

Strategies to Manage Harassing Messages and Calls

Experiencing harassing calls and messages can be very difficult emotionally. It may feel as though the person is always there, you can't get away, and the only solution is to disengage from all technology so they can't contact you. While you can't make the other person stop harassing you, there may be some things you can do to alleviate the constant bombardment of harassment.

Block the Abusive Person from Contacting You

One strategy can be to block the abusive person from contacting you. You can block someone on your smartphone, through the telephone company, or on the social media platform. Blocking works differently depending on the technology platform or smartphone device, so it's important to test it so you know what to expect, become familiar with how it works, and ensure it works most of the time. Test the blocking feature with someone you trust to see how it works.

Keep in mind that there are limitations to blocking. When you block someone, you are blocking their ability to contact you via a particular phone number or social media account. They can still contact you on a different phone number or social media account. It also prevents you from being able to see what they are posting about you.

- **On Smartphones**

Depending on the type of phone you have, you can block the other person in your phone settings to prevent them from contacting you. Generally, once blocked, any calls or text messages from the blocked phone number will not come through. However, blocking is going to be different on each phone; for example, the device may block incoming calls but not text messages or the blocked person may still be able to leave a voicemail but you won't get a notification. If you're not sure how to block on your phone, search "how to block a number" on the make and model of your phone on a platform like Google and, if possible, test blocking to see how it works on your phone.

- **On Social Media**

If the abusive person is harassing you via a messaging or social media app, you can block that person through the social media or messaging app. Each social media has its own blocking feature and processes, so if you are unsure of how to block someone, search "how to block someone" from the specific social media platform on a platform like Google for instructions. Most social media companies have instructions in their help centres.

In general, most social media companies will not inform the other person that they have been blocked. However, the abusive person may realize that they are being blocked when they are unable to see your social media content or message you.

Other Strategies

Not everyone wants to stop all contact with the harassing person. You may want to continue to have contact with the other person because you want to continue to collect evidence of the harassment. Sometimes, knowing what they are saying or doing can help you determine whether their behaviour will escalate. In some cases, you may need to stay in contact to communicate about children, pets or other joint issues.

Use a Specific Ringtone for the Abusive Person

If you still need to stay in contact, but every time the phone rings it upsets you, one option is to use a specific ringtone for the abusive person. This way, when other people are calling, your phone will ring as normal. But when the abusive person calls, the special ringtone will alert you, and you can decide whether to answer it or silence your phone and ignore it.

Let the Call go to Voicemail

One common strategy is to let the calls go to voicemail. This lets you collect evidence of harassment, but you don't have to talk to the other person. Using this strategy along with giving the person their own ringtone will let you know whether to pick up the call or let it go to voicemail.

Get a Second Phone

Another strategy is to get a second phone. You can use one phone for the abusive person to contact you and another phone for everything else. This way, you're not cutting off all contact, but you can have a safer phone that you can use and you're not constantly bombarded with messages from the abusive person.

Forward Calls from a Specific Phone Number

Some phone companies have a feature that lets you forward calls from a specific number to another phone number. You can forward all calls and messages from the abusive person to another number, which means that even if they dial your number, your phone doesn't ring and you don't get the harassing text messages.

Get a New Phone Number or Social Media Account

In some cases, you may decide to just get a new phone number or social media account. This option is best if you want to cut off all ties, want no communication with the abusive person, and don't think the abusive person will learn about the new phone number or social media account. This solution isn't for everyone because it may be a lot of work to change your number or create a new social media account.

Another limitation to this option is that depending on your situation, it may be fairly easy for the abusive person to discover your new number or account – particularly if you have joint friends or family members – or if they have access to your accounts (such as email), offices, or organizations (e.g. health care offices, schools) where you updated your new number.

Make Your Number Private

If you need to call the abusive person but don't want them to know about the new number, consider turning off your caller ID through your phone settings so it doesn't appear on the receiver's caller ID. The receiver will see "Private Number" or "Caller ID Not Available" on their phone when you ring.

If you don't want your number to be masked all the time, another option is to do this on a call-by-call basis. Each telephone company has its own code that you enter before you dial the number you are calling. Because each telephone carrier has its own code, contact your telephone provider for their caller ID blocking code.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from WESNET's Tech Safety project, based on their resource Dealing with Harassing Call, Texts and Messages.

Survivors' Guide to Phones: Increasing Privacy and Responding to Abuse

PART 1: Is Your Phone Being Used Against You?

Unfortunately, conversations and information on phones can be misused to monitor, stalk, control, or harass. **Trust your instincts**. If you suspect that someone is monitoring your phone, here are some questions to consider.

Is There a Pattern?

Does the person seem to know everything – who you've spoken to, the content of conversations you've had either on your phone or near your phone, texts you've written and received, where you go – or just pieces of that information? Narrowing down which of your activities are being tracked will help you determine how you are being monitored, and which safety strategies to consider.

What Does the Person Seem to Know?

If the person knows that you had a conversation, but not specifically what you said, wrote, or shared, then they may be looking at your call log, billing records, or other account information. They also could have talked with the other person you were communicating with.

If the person knows the content of your messages, then they may be using other devices that are linked to your accounts or monitoring your device, or the other person shared or forwarded the messages.

If they know the content of voice or video conversations, but they were not nearby to simply overhear the conversation, and they weren't told of the conversation by the person you were speaking with, then they may be using stalkerware. Caution: anything you do on your phone, including looking up information or looking for the stalkerware could likely be seen. Read more about stalkerware on a safer device.

Has the Person Monitoring You Had Access to Your Phone?

Most monitoring requires physical access to your phone. The person might regularly scroll through your phone to see who called and texted you or may have installed stalkerware on the phone allowing them to view your activity from another phone or computer. With physical access to your phone, they could also download apps or change account and security features to make your phone more vulnerable.

Does the Person Have Access to Your Online or Cloud Account?

Another way someone can monitor your phone use is if they have access to your account with the phone company and/or the cloud account your phone is linked to (e.g. Google or Apple). If their name is on the phone account or they can convince the phone company that they are you or an authorized account holder, they may have the ability to turn on features such as location services, access your billing records online, and see your call logs and other information.

Do They Know Your Location?

Phones and apps can share your location. Check the settings on your phone and in apps to limit location sharing. Most phones also have a feature to help you find a lost phone, which can reveal your location if the other person has access to your phone or account. Learn more about Location Tracking beyond phones.

Part 2: If Your Phone Is Being Monitored

There are steps you can take to secure your phone, apps, and accounts. There isn't one "right" way to respond. What works for someone else may not work or be safe for you.

CAUTION: Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. Making changes could also erase evidence.

1. Reset phone and accounts. Doing a factory reset of the phone may uninstall any stalkerware that was installed without your permission or knowledge. It is important to avoid reconnecting the device with a backup, however, so the stalkerware won't be reinstalled.

You can also uninstall any unfamiliar apps and check for apps and settings that are allowing location sharing. Call your cell phone provider to make sure that no other location-sharing service is enabled.

Reset passwords on phone billing, cloud, and other connected accounts to remove any possible access the person might have.

2. Replace your current phone. If you are able to, and you feel safe, you could replace your phone or set up a second phone. Here are a few options:

- Purchase a new phone, and consider switching carriers and getting a new phone number. Ask if there are additional security features you can set up for your account, such as asking the company to note in your account that you are the only authorized account holder or setting up notifications if changes are made to your account, including adding or removing features.

- Purchase a pay-as-you-go phone with cash.

- A trusted friend or family member might be able to give you an old phone. Be sure to wipe the phone's memory and do a factory reset to remove any of their information from the phone.

Important: Don't connect the new phone to any old accounts, especially cloud accounts like Google or iCloud, and don't use your old number. Don't move data from your old phone to the new phone using a memory card, SIM card, your cloud account, or backups. Doing so could reinstall stalkerware.

3. Strategize about the monitored phone. Some abusive people may escalate their abuse when their access and control are cut off. You may consider keeping the phone on and using it strategically to prevent raising the suspicion of

the abusive person. You may also want to keep the monitored phone for evidence. If you keep the phone, decide how you will store it. You could turn it off or remove the battery. Remember that once you turn the phone back on, your location will be visible if someone is monitoring your location through a cell signal or Wi-Fi. These are all options to consider and to talk through with an anti-violence worker. You can reach out to them for help with safety planning.

4. Talk to friends and family. Family and friends can inadvertently share your location, who you're talking to, or what you're doing through social media posts or with other people. If you have children, teach them how to avoid sharing your location or information about your personal activities.

5. Document what Is happening. You can document what is happening, if it feels safe, by taking screenshots and creating a log of what's happening before you make any changes. You have the option to share this with law enforcement or an attorney, or save it for later. Documenting the abuse can also help you make or update a safety plan. Read more about Documenting Abuse.

Part 3: Ways to Increase Safety And Privacy

1. Put a passcode on your phone. Most phones ask for a 4-digit passcode, but some will allow you to set up a more complex passcode, a pattern, or a biometric lock using your fingerprint or facial recognition. If you're not able to put a passcode on your phone or the abusive person demands that you share your passcode, consider borrowing someone else's phone to look up safety information or to call a crisis line.

2. Secure your phone's online accounts. Phones usually have an online account with the phone company and a cloud account to store personal data (most likely a Google or iCloud account). Review the security settings and consider changing passwords to your phone and cloud accounts to ensure that someone else can't access your information.

3. Use anti-virus and anti-spyware software on your phone. You can research reputable programs online and find them in app stores. Many have free versions and can protect against stalkerware and other malicious apps being downloaded on your device.

4. Turn off location sharing. Phones have built-in GPS that can pinpoint your location, with some phones and apps giving you the option to share that information. You can manage your location sharing within your phone settings, where you can choose which applications can access your location or you can turn off location sharing altogether. Some apps let you manage your location sharing within the app's settings as well.

5. Check your privacy and security settings. Most phones have settings that will help you manage your privacy and security. You can find these controls through the phone settings or app settings. For more information, read our Online Privacy and Safety Tips, and check out our guides on Facebook and Twitter for more information about their privacy and security settings.

6. Log out of apps and accounts. Consider logging out of accounts so that others can't access them if they have access to your phone. You might not be able to log out of some apps without removing them from your phone. It may be more inconvenient to access the account through the browser instead, but make your decision based on your privacy and safety risks.

7. Review downloaded apps. If you find an unfamiliar app on your phone, delete it. Apps are easy to download and easy to forget, and some apps could be gathering your private information. However, be cautious before removing an app if you're worried it may be spyware or stalkerware. Read more about spyware on a safer device.

8. Avoid unlocked or "jailbroken" phones. Removing the manufacturer and phone carrier's restrictions makes these phones more vulnerable to spyware and malware. Knowing if your phone has been unlocked or "jailbroken" can also be a clue as to whether or not someone may have installed a monitoring app on your device.

9. Use virtual phone numbers. Consider using a virtual phone number, which will allow you to screen calls, receive voicemails, and make calls or send texts without sharing your device's phone number. Virtual numbers can be linked to a cloud account (e.g. Google Voice), so be sure that the online account is also secure.

10. Try not to store sensitive information on your phone. The less sensitive information you have on your phone, the less likely someone else can access it. You may want to delete certain text messages or voicemails from your phone and from connected cloud accounts like Google or iCloud.

11. If you're considering a safety app...There are many "personal safety apps" available that offer to increase users' personal safety; some are developed or advertised specifically for survivors of violence. Read more about Safety Apps to figure out if these apps are right for you.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource A Survivors Guide to Phones.

Safely Setting Up and Activating a Phone or Other Devices

This handout has general information for those who want to set up a new phone with a new number. Sometimes perpetrators destroy phones or monitor a woman's "main" phone. Many women may choose to get an extra backup phone to call 9-1-1 or support services privately as they plan what to do next.

There may be unique situations and tech safety needs that are not be covered by this basic advice. Trust your instincts. If you feel you need more information, particularly if your perpetrator knows a lot about technology, please see our other info sheets at www.techsafetycanada.ca.

Common Risks and Benefits of Setting Up and Activating Another Phone

It is important to understand the common risks and benefits of getting a new phone so that you can plan for how to stay safer. These can include:

Potential Risks Include:

- An abuser finds the phone and becomes more abusive.
- Setting up a new mobile phone account may unintentionally link to an abuser's account due to similar or shared data (like address, email, etc.). This can include information from an old phone automatically moving to the new

phone.

- A perpetrator finds out that a survivor has removed herself from his mobile phone account
- Financial abuse, which can affect credit and make it harder to qualify for a phone

Potential Benefits Include:

- Being able to call 9-1-1, support workers, and people you trust on a safe device
- Searching the internet or undertaking other activities on the device without being monitored
- Being able to flee and use location-based services like maps
- Being less isolated

If you decide to get a new phone, here are some things you might think about:

- Creating new, unlinked accounts (like Google, iCloud, or Apple ID)
- How you will keep the battery charged on the phone
- How to keep credit on the phone, and knowing when it may expire
- What you could say and do if a perpetrator or child finds the phone
- Using the phone's data instead of your home Wi-Fi since it can be monitored
- How you will keep the phone from vibrating or ringing

The main thing to remember as you set up and activate a new phone, especially if you plan on still using your "main" phone, is how to keep everything about the new phone and your "main" phone separate. We will cover some basic things you can do. Depending on your situation and how tech-savvy the perpetrator is or their contacts are, it may be safer to review our more in-depth guides about Androids or iPhones before getting a new phone.

Why Keeping Information Separate Is for Safety

Kristin & Joanna's* tech safety stories*

Kristin bought a new sim card and a new phone and set up the new phone with the same provider. After a few days, her partner confronted her and angrily asked why she was setting up a new phone. Kristin had not realised that her husband was the legal account holder of their family account and that he was notified when she added a new phone number in her name. Joanna had a similar experience after providing her email address to the phone company and not remembering that her abusive ex-husband could access her email account and read her incoming emails. He saw an email in her account from the phone company advising her that her new account had been successfully set up.

**names have been changed*

Step-by-Step Simplified Process for Safely Setting Up and Activating A New Phone

1. Create a new email address using a device the perpetrator has not accessed. Whether the new phone you get is an iPhone or Android phone, this email address can be used for the Apple ID, iCloud account, or Google account, etc.

2. Update the privacy and security settings on your new email account. Adjust settings to your comfort level so that your contacts, location, and other personal information is collected only with your knowledge. Stay safer by being selective about the personal information you share during setup.

3. Get a new phone that is not a gift from an abusive person. Keep receipts, if possible.

4. Find a new mobile service provider that your abuser does not or has not used, if possible. Separate your identity by insisting on a new account number and a new phone number for the new phone. Stress to the person activating the phone that the account is in your name and request additional security measures, like a pin or two-step authentication that an abuser could not guess or access.

5. Get a new phone number. This can be hard, and each person's needs may be different. The main risk of keeping an old number and transferring it to a new account is that the perpetrator will still know the number. This may result in harassment or even impersonation to gain control of that number again.

6. Get a new SIM and a new SD card. Do not use the new SIM or SD in the old phone or the old SIM or SD in the new phone. Keep the phones separate. This may require physically entering contacts onto the old phone.

7. Explore your new phone's privacy, security features, and connectivity features that may collect your contact, location, or other information. Make sure to practice using the phone's features so you know how to silence it, charge it, and load credit on it.

8. Use new locks, passcodes, and complex passwords for your new phone. Be cautious about what apps or accounts you access on your new phone as some may notify an account holder of a login from an unknown device. Only download apps under your new Apple ID, iCloud account, Google account, etc.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from WESNET's Tech Safety project, based on their resource Safely Setting Up and Activating A Phone or Other Device.

iPhone Privacy and Security Guide

Please note: This handout is up to date as of December 2022. If you have a newer model or operating system, please check Apple's website for the latest capabilities.

Apple ID

The first time you purchase an iPhone or iPad, you must create an Apple ID. This ID is used for everything that you do with Apple, including shopping in the iTunes or App Store, accessing iCloud services, using iMessage or FaceTime, or contacting Apple support. Your Apple ID is typically an email address – it can be a personal email address or an email address that ends with @icloud.com (which is also used to access your iCloud Account).

It is possible to add alternative Apple IDs or emails to your account. To see which emails are associated with your account, log in to your account using your Apple ID and password. Once logged in, you can delete old email addresses that you're no longer using and ensure that no other additional emails were added. Here, you can also update passwords, security questions, and other contact information. When updating or creating new passwords, use a strong password, one that others can't guess, and change it if you suspect that someone else may know it. Read more tips about passwords.

iCloud Services

Most iPhone users also use Apple's iCloud services, which is a cloud-based service that allows users to store their music and other files, such as photos, apps, contacts, emails, and documents. Documents created in apps such as presentations, spreadsheets, images, and PDFs can also be saved to iCloud.

Access to iCloud can be through all connected Apple devices or by logging in to the iCloud account (usually the same as your Apple ID) from a computer. If you save your device backup to iCloud, after resetting or updating your phone, you have to sign back in to your account for all your apps and settings to automatically reset on your device.

There are pros and cons to using iCloud services. On the benefit side, if you purchase a new device or need to reset your device, logging in using your Apple ID will automatically update your device with your apps and settings the way you want it. If you're using iCloud Drive, you can also access the same documents or apps on other devices using the same Apple ID. However, if you are setting up a new device to avoid monitoring from an abusive partner, updating your new device with the same apps and settings can be a risk. See Safely Setting Up and Activating a Phone for more details

On the other hand, using iCloud means that your information is accessible from multiple places rather than only on one device. Multiple access points can make your information more accessible and, therefore, more vulnerable. If someone knew your Apple ID or your iCloud username/password, they might be able to access your data and information.

Security and privacy measures include changing the password to your iCloud account or limiting which information you want to be accessible from the cloud. To select what information on your iPhone or iPad will back up to iCloud, go to Settings/iCloud on your device and select what data (Photos, Mail, Contacts, etc.) is backed up to your iCloud. Under that setting, you can also select what you want to be saved to iCloud Drive.

iPhone Settings

The iPhone itself has many settings that allow you to control access to information on your device. Although time-consuming, one of the ways to ensure that your phone is as private and as secure as possible is to go through each setting. This will help you learn what each setting does, how much control you actually have over your device, and how much information is stored and potentially shareable on your device. It's best to go through each setting; the following are some major privacy settings to start with.

Find My iPhone

If the Find My Phone feature is turned on in the device settings, users can find the location of the device by logging in to iCloud. This feature is meant to help you find your device if it is lost or stolen; however, some people could use this feature to locate another person. Users concerned about their location privacy can turn off this feature on their device by going to Settings/iCloud and switching Find My iPhone to "off."

Family Sharing

The Family Sharing feature allows up to 6 different accounts to share iTunes, iBooks, and App store purchases; photos and videos; and a Family calendar. Each person needs to be invited and accept the invitation to be part of the Family Sharing group. The Family Organizer is responsible for paying for purchases initiated by other family members and could deny purchases.

Purchased content can be shared with anyone in the Family Sharing group.

When joining Family Sharing, you will be asked if you want to share your location information. You can always turn this feature off by going to Settings/iCloud/Share My Location; the setting allows you to determine which family member can or cannot see your location.

Location Settings

Many apps want access to your iPhone/iPad's location. For the most part, you can control which app can access your location information by going to Settings/Privacy/Location Services. There, you can turn off all location services or manually turn off location access for individual apps. Our recommendation is to turn off location access when you're not using the app. You can always turn the location back on when you need to use the app.

Another location setting to review is System Services, in which the iPhone uses your location information for other features or functionality. To access System Services, go to Settings/Privacy/Location Services and scroll to the bottom and select "System Services." Minimizing location information access here will also help conserve battery life.

Privacy Settings

Some apps want access to contacts, calendars, photos, or the camera. Under Settings/Privacy, you can allow or deny apps' access to other information on your device. Here, every app that has ever requested access to any information on your phone is listed, and you can control what information they access.

Specific App Settings

Scrolling down toward the end of your iPhone's Settings is a list of most of your apps. Under each specific app, you are given additional privacy settings. Remember that most apps have privacy, security, or notification settings within the app itself. Review all the apps you've downloaded, and make sure that the settings are set to your preferences.

FaceID, Touch ID, and Passcode

Depending on the model of your iPhone, there will be options for FaceID, Touch ID, and passcode under General Settings. You can update your FaceID, Touch ID, and passcode there. You should always use a passcode on your devices to prevent anyone from picking up your device and going through it while unattended. iPhone 5s or later, iPad Pro, iPad Air 2, and iPad mini 3 or later all have Touch ID, which uses your fingerprint to access your device. iPhone X or higher will have the FaceID option, which uses a mathematical model of your face so that you can scan your face to access your device. In addition to the Face ID and Touch ID features, you can also set up a custom passcode that is either a 4–6-digit numeric code, a custom numeric code (that is longer than 4 digits), or a custom alphanumeric code (combination of numbers and letters). The more complex the passcode, the harder it will be for someone to guess.

Jailbreaking iPhones

Some people will “jailbreak” their iPhone, a process in which the hardware restrictions by Apple and the wireless carrier are removed (the equivalent term for Android devices is “rooting”). This allows for downloading additional software and applications that are not available in the Apple App Store. This process will make the phone more vulnerable to malware and spyware. Most – if not all – of the commercially available spyware products require a jailbroken iPhone to install.

One way to know if your iPhone is jailbroken is to access the Spotlight Search page (swipe down on your screen) and search for the Cydia app, which is one possible indication that your device might be jailbroken. If your phone is jailbroken or you believe that it is, do a restore of the device and make sure you are running the latest iOS on your device. This will remove software that was downloaded outside of the Apple App Store.

Additional Tips

Have strong passwords. Make sure you have a strong password and don’t share it. If someone learns your password, change it as soon as possible.

Limit access to your information. Smartphones make it very easy to access your information from multiple devices. Weigh convenience and privacy to determine what is safest for you.

Log out of accounts. If you’re not using a particular app, consider logging out. It might be inconvenient to log back in each time you want to use it, but it will prevent someone from getting into your accounts.

Don’t share your devices. The safest option is to not use someone else’s device and not share your own device. If you must borrow someone’s device, ask to delete your personal information from the device once you’re done, such as deleting the phone number you dialed or text message you sent. If you need to use a map app, access the map via the web browser and turn on the browser’s in-private mode feature. Don’t forget to log out of any online accounts you accessed while on someone else’s device.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don’t need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV’s Safety Net project, based on their resource iPhone Safety and Privacy Guide.

Android Privacy and Security Guide

Please note: This handout is up to date as of December 2022. If you have a newer model or operating system, please check the brand’s website for the latest capabilities.

Smartphones store a lot of personal information, including email or social media accounts, reminders and notes, the number of steps we take each day, and even personal biometric data such as fingerprints and facial recognition. While all this can make life easier, perpetrators and stalkers can also misuse this information to monitor, control, and harass victims.

This guide will help users enhance security and privacy when using their Android smartphones. Although all Android phones use the same operating system, depending on the brand (Samsung, Google, LG, Huawei, Motorola), each phone’s settings can be quite different. Use this handout as a general guide, rather than step-by-step instructions.

There are two areas to look at when increasing your smartphone's privacy and security: (1) the privacy and security mechanisms built into your device (which may be slightly different depending on the brand of your phone) and (2) the Google account (which is essential to all Android smartphones) associated with your smartphone.

Android Device Settings

Although each Android smartphone will have slightly different settings, there are some standard privacy and security settings you can configure to give you more control over the information on your device. Although time-consuming, one of the best ways to ensure that your phone is as private and secure as possible is to go through each setting. This will help you learn what each setting does, how much control you have over your device, and how much information is stored and potentially shareable on your device. The following are some major privacy or security settings to start with.

Screen Lock and Passcodes

The most obvious – and most important – security setting you should start with is securing your Android phone with a passcode. This will prevent anyone from picking up your device and going through it while unattended. Depending on your Android phone, you will probably have many passcode options to choose from. The most common passcode is a 4 to 6-digit code. Other options include a custom numeric code, an alphanumeric code (combination of numbers and letters), or a pattern. Some Android phones include options such as face recognition or fingerprint recognition. On most Androids, you can find the passcode options under Settings / Lock Screen and Security.

Some Androids will have additional settings, such as deciding whether notifications or shortcuts should be visible when your phone is locked. Whether you choose to display that information depends on whether you would be comfortable if someone picked up your device and saw that information. You can find this under Settings / Lock Screen and Security.

Smart Lock

Smart Lock can unlock your phone if:

- You are at a "trusted location," such as your home;
- The smartphone wants to connect to a "trusted device," such as your Bluetooth speaker;
- The phone is on your body;
- The person looking at your phone is recognized as a "trusted face," or
- Your device recognizes your voice as a "trusted voice."

Under these circumstances, your smartphone will unlock without you needing to put in a passcode. While Smart Lock can be convenient to use – for example, you're juggling bags and opening doors and need to unlock your phone – it can also make it easier for someone else to have access to your phone. Think about your privacy concerns and balance convenience with privacy and security. You can generally find this setting under Settings / Lock Screen and Security / Secure Lock Settings/ Smart Lock.

Location Settings

Location is another setting you should check on your Android. You can generally find this under Privacy and Safety. Under Location settings, you have the option of turning your location on or off globally for all apps. Under this setting, you will also be able to see which apps have recently requested your location. If you don't want a specific app to have access to your location, you will need to go into each specific app and manually turn the location off. For the most

privacy, turn off the location if you aren't using it. You can always turn the location back on when you need to use the app.

Under your Location settings, you can also decide how your location is accessed, whether by GPS, Wi-Fi, mobile networks, all those options, or a combination of those options. In general, when all location options are turned on, your location will be most accurate. This is important if you are using safety apps that need to know your exact location. Some people may choose GPS or mobile networks only, to save their battery.

Bluetooth Settings

Another setting to turn off if you're not using it is Bluetooth. If you've ever connected with a Bluetooth device, which could be your car, portable speakers, or even a printer, it could automatically connect once you're in range. Turning off Bluetooth will prevent automatic connection and you can turn it back on when you need it. This setting can generally be found under Settings / Bluetooth.

Apps' Access to Device Content

When you download an app, you will get a message that tells you what content on your smartphone the app will need access to, such as contacts, calendars, photos, camera, microphone, SMS, sensors, storage, etc. On the latest Android OS, you can pick and choose which content a particular app can have access to under Settings / Apps / App Permissions. Under each category, you will see which app wants access to which content and can turn access on or off. On Android phones running older operating systems, you may need to go to the Application Manager and go through each app manually.

In some cases, you may not have the option to deny a particular app's access to your smartphone content, or if you don't allow it to access, the app may not work properly. For example, Google Maps needs access to your location to give you directions. In these situations, determine if you're comfortable allowing the app access to your device content versus how much you need to use the app.

Installing Apps from Unknown Sources

Another setting to toggle is not allowing apps outside of the Google Play Store to be installed on your device. Unlike the iPhone, your Android phone allows you to install apps outside of the Google Play Store, such as from a website or via your computer. This is often how smartphone spyware and other malware get installed, so it's important that this is turned off. You can find that setting under Lock Screen and Security / Unknown Sources.

Encryption

Your device is likely already encrypted by the manufacturer if you are running Android OS Marshmallow or above. Otherwise, if you're concerned about security you can turn on encryption, found under Settings / Security / Encryption. An encrypted phone will make it more difficult for someone to access the data on your phone unless they have the encryption key, which is usually your passcode.

You can also choose to encrypt your SD card (even if your phone comes already encrypted). You can generally find this setting under Lock Screen and Security/ Encrypt SD Card. Note that encrypted SD cards can only be read on the device used to encrypt them.

Backup and Reset

Android phones offer many ways to back up the data on your phone. Google Backup and Restore not only backs up your phone content, but it also will back up all your Google app data, such as calendar, Chrome browser, contacts, and photos. Once backed up, if you have to set up a new phone, just log in with your Google account and all your data will be synced. While incredibly convenient, it's important to ensure that your Google account is secure. Take advantage of Google two-step notification so that if someone else were to sign in to your account, you would know.

Another method of backing up your account data is through online cloud services, such as Google Drive or Dropbox. Many people use these services to back up their photos or videos. Again, while convenient and helpful in clearing space on your Android, be sure that your account is secure when using these services.

Google Account and Services

Since the Android mobile operating system is built by Google, your Android smartphone is intimately connected to the Google platform. To purchase apps through the Google Play Store, you will need a Google account. For most users, that Google account will also be used for all the other Google products and services on the device, including Gmail, calendar, contacts, Chrome browser, and YouTube. Having all those services connected to one account can be convenient and helpful. For example, when you look at a website on your Android's Chrome browser, the Chrome browser on your laptop will remember it in its history. Your browser history is saved to your account, as well as on the specific device.

Depending on your situation, you may find it helpful to have your information saved and integrated across devices under one account, or you may require more privacy and not want your information to be remembered across devices. If all those services were under one account and someone should gain access to your Google account, they will learn quite a lot about your phone activity. The good news is that Google does give users a lot of privacy options. Below are some suggestions for more privacy and less connection.

Go through Google Settings

Google gives you a lot of choices to increase your privacy and security while using their products, which you can find in Google settings. You can access these settings on your Android by going to Settings / Google. You can also access these settings online via a web browser at https://myaccount.google.com. We suggest going through all the settings. This is the best way to be aware of and increase your privacy and security. An easy way to do this is to go through Google's Security Check Up as well as their Privacy Check Up (both can be done from within your settings on your phone or via your browser). Below are some settings to go through, but keep in mind that this is not an exhaustive list. We highly encourage you to go through all your Google settings to meet your specific privacy and security needs.

Minimize Google's Collection of Device Activity

One way to prevent Google from collecting your information is to go through your settings and set it to "not collect your activity." You can find these settings under Settings / Google / Personal Info & Privacy / Activity Controls. Here, you can set up your preferences regarding which of your activities Google remembers and saves to your Google account (e.g. Web & App Activity, Location History, Device Information, Voice & Audio Activity, YouTube Search History, and YouTube Watch History). Choose "pause" to stop Google from collecting this information. Keep in mind, however, that pausing the tracking of any of the above activities does not delete previously recorded activities. To delete those, you will need to do that separately through the Review Activity settings. These can be accessed through your Settings / Google/ Personal Info & Privacy /My Activity. Also keep in mind that even if the setting is paused, Google may still temporarily track some of your activities (e.g. web searches to improve the quality of your current search session).

Pay Special Attention to Location History

Another area to turn off is Location History. When this is turned on, Google will track everywhere you go through your smartphone (this is different from using Google maps). The purpose of this is so Google can recommend improved map searches, among other things. However, from a privacy perspective, if someone were to gain access to your Google account, they could see everywhere you have gone (and possibly predict where you will go). Determine if the privacy risks of someone knowing everywhere you go outweigh the convenience of a quicker map search or a Google recommendation based on your current location. Turn off location history by going to Settings / Personal Info & Privacy / Your Personal Info / Location Sharing.

Find My Phone

Many people will use the Find My Phone feature to track down their phone's location if it is lost or stolen. However, if someone were to have access to your Google account, they could sign in to your account and find where your phone is through this feature. Whether you use this setting is up to you. Consider the security of your Google account and how likely it is that someone could use this to track your location vs. the security of being able to find your phone if is lost or stolen.

Remove Connected Devices and Apps

Your Google account can be logged on from multiple devices (such as an Android smartphone and laptop). To help you manage where you've connected, Google will tell you which devices have accessed your account in the last 28 days or are currently logged in. You can find this in your settings on your phone under Google / Sign-in & Security / Recently Used Devices. If there are connected devices you don't recognize or you logged in somewhere and forgot to log off, this is where you can remove those devices' access. This is also helpful if you lose your Android and need to disconnect the device from your Google account.

Remember that your Google account can also be logged in to other online accounts, such as apps or other online services. Unless you know your Google account is secure and you are comfortable using it to sign in to other accounts, it is generally best to create a new username and passwords when signing in to other online accounts. However, if you do choose to use your Google account, you can check which apps and/or online accounts your Google account is signed in to. Go to Settings / Sign-in & Security / Connected Apps & Sites to check or remove access to any apps or accounts.

Sign Out of Google Products on Your Android

While some Google services require you to sign in to be able to access it – such as Gmail or the Google Play Store – not every Google product requires you to sign in for it to work. When you are signed out, what you do on those apps will not be saved in your Google account. However, keep in mind that while your Google account won't remember your activities, the app on your Android will remember. For example, if you're not logged in while using the Chrome app on your Android, your Google account won't remember what websites you visited, but your website browsing history will be saved in your Android's Chrome app. If you don't want any trail, consider deleting your Chrome browsing history or using the Incognito mode.

Additional Android Security

Security Apps

While the Android phone itself has built-in security settings, if you're very concerned about the security of your phone, you can download a security app. Third-party security apps have a wide range of features, including malware and virus protection, tracking your phone if it gets lost or stolen, or remotely wiping all the data off your phone.

You could also download specific anti-malware apps, which will protect your phone from getting viruses or prevent other types of malicious software from installing. Depending on the type of Android smartphone you have, it may already come with anti-malware protection. If it does not (or you want to explore other options), you can go to the Google Play Store and search for anti-malware apps. Another way of looking for good anti-malware apps is to google "best anti-malware apps for Android" and read the reviews.

When downloading third-party apps from the Google Play Store, look at the reviews. The closer it is rated to 5 stars, the better, but also look at how many people have downloaded the app and read some reviews.

"Rooting" Your Android

Some people will "root" their Android, which is a process that allows you to modify the Android operating software code and install other software blocked by the manufacturer (the equivalent term for Apple devices is "jailbreaking"). Unfortunately, a rooted phone can be more vulnerable to malware and spyware, void your warranty, and make software updates impossible. Software updates are important because they can include security patches and make your phone less vulnerable to hacking. One possible way to know if your Android is rooted is to download a root-checker app from the Google Play Store. To "unroot" your phone, google instructions online since there is more than one way to "unroot" your Android.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from WESNET's Tech Safety Net project, based on their resource Android Safety and Privacy Guide.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada
Femmes et Égalité des genres Canada
Canada