BC Society of Transition Houses

Preserving Digital Evidence via Video Screen Recording

When technology-facilitated violence occurs, maintaining a record of events is important for criminal and civil legal matters. While screenshots are regularly used in criminal and civil courts as a way to exhibit and authenticate digital evidence, one of the easiest methods of preserving digital evidence is to record a video of a smartphone screen.

If your smartphone has the capacity to video screen record, there are some benefits to using the video record function of your phone for preserving digital evidence, compared to taking screenshots.

Screenshots are easy to manipulate with picture editing software, which may lead to the questioning of their authenticity. However, printed screenshots are often easier for the courts to view compared to videos.

Entire text conversations may be lengthy, lasting days or weeks, and require multiple screenshots to capture the entirety of the exchange. This could potentially lead to a significant number of screenshots that would need to be organized chronologically, which may take extra effort and time.

The following video screen recording information is for Apple iOS and Android devices of particular models and is accurate as of July 2020.

Depending what version of a phone you have, it may not have this particular recording function or you may need to look up different instructions if these ones do not match your current device. It can be easy to find these types of instructions by searching for them on YouTube. However, remember to use a safe computer or erase your search history if you are looking up this information as it may trigger additional abuse from the perpetrator if they discover you are looking for help.

Safety Check

Before you screen record evidence or download a screen recording app, always think through any potential risks to your safety. There may be a risk that the perpetrator is monitoring the activities on your mobile device.

This could be happening in several ways. Your smartphone could be monitored if the perpetrator has access to your device, which could be accessible if you share a home or they have made you share your passwords with them. If the perpetrator knows your cloud storage (i.e., iCloud, Google Drive, or Dropbox) ID and password, they will have access to some of your files, photos and videos. It is also possible for the perpetrator to be monitoring your smartphone or computer via mobile spyware, such as

stalkerware. If the perpetrator is monitoring your device these ways, it could alert them to you collecting evidence. If you suspect that the perpetrator has access to your devices, accounts, or files, you will need to make a plan on how to avoid detection when collecting evidence. This is both to protect you from additional abuse and to avoid the risk of the perpetrator deleting important evidence.

Look at your account settings on your email, social media and other accounts to see what devices are connected and disconnect them from the account if it is safe to do so. You can also check to see what IP addresses are being used to look at the account to see if an unusual IP address is accessing your accounts. This may be important evidence that the perpetrator is accessing your accounts without consent.

Research password safety and the importance of changing passwords on all relevant platforms and devices. If you have any concerns that your device(s) may be infected with spyware, work with an anti-violence support worker to research how to change the passwords without alerting the perpetrator.

If video screen recording is not a safe option for you, consider alternative ways to preserve evidence, which can be found in the BCSTH Digital Evidence Toolkit.

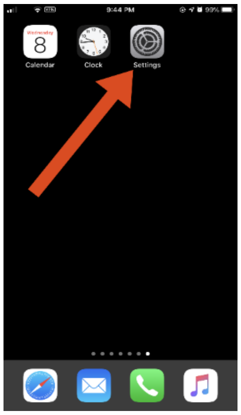
If you plan to use video screen recording on your phone as digital evidence in a court proceeding (drawn from an Apple phone or Android 3rd party app) you will need to authenticate your evidence in court. For more information about digital evidence and authentication, see BCSTH's "Authentication of Digital Evidence for Matters of Family or Civil Law in BC Courts" information sheet.

Apple IOS Video Screen Recording

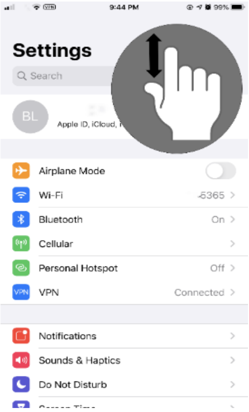
Since 2017 (the iPhone 6 generation), Apple's mobile devices have built-in screen recording functionality. However, this setting is not initially available to users by default and needs to be enabled. Enabling video screen recording can be done by following the steps below. If you'd like to see a video on how to do this you can watch BCSTH's Apple IOS Video Screen Recording Tutorial .

See the next page for directions on how to do this, including images on how to do this.

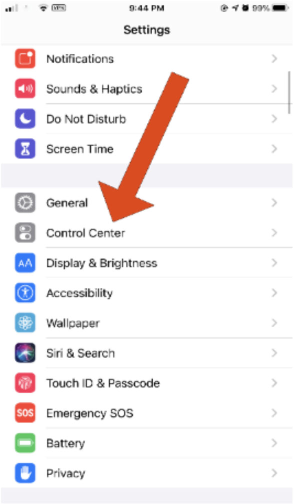
1. Go to Settings.



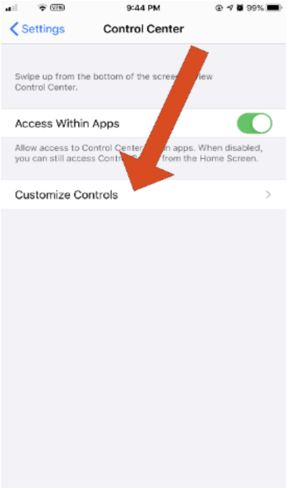
2. Scroll to “Control Center”.



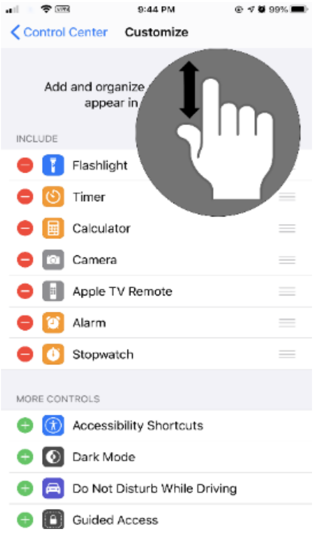
3. Open “Control Center” settings.



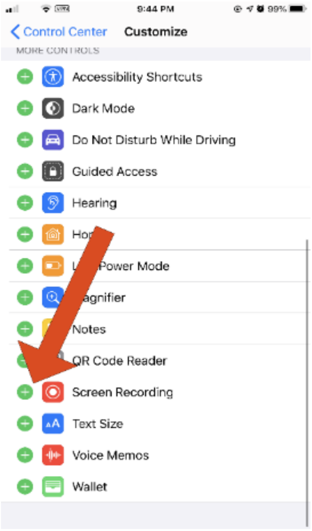
4. Select “Customize Controls”.


9:44 PM
99%
Settings
Control Center
Swipe up from the bottom of the scree view
Control Center.
Access Within Apps
Allow access to Control Center n apps. When disabled,
you can still access Contr from the Home Screen.
Customize Controls

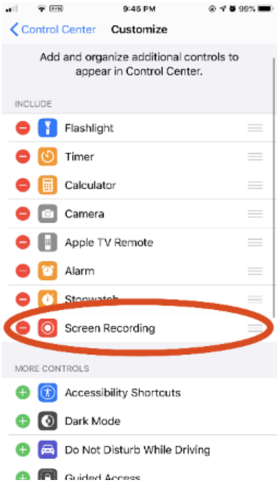
5. Scroll to “Screen Recording”.



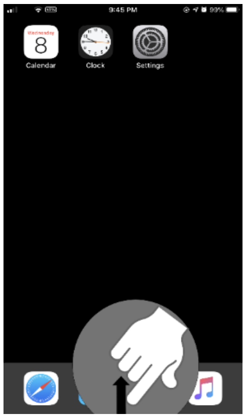
6. Add “Screen Recording” to the Control Center by selecting. ⊕



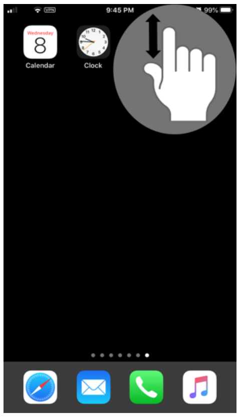
7. Check that “Screen Recording” is added in the “Include” section.



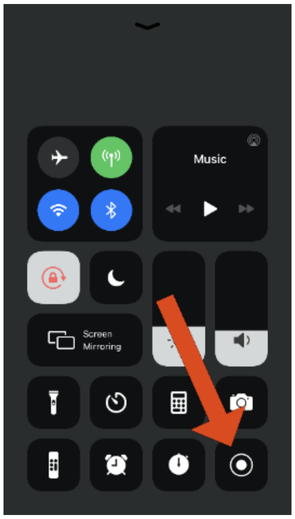
8. Return to the home screen and swipe up from the bottom of the screen to open the Control Center. Note: some newer models ask you to swipe down from the top right corner of the screen.



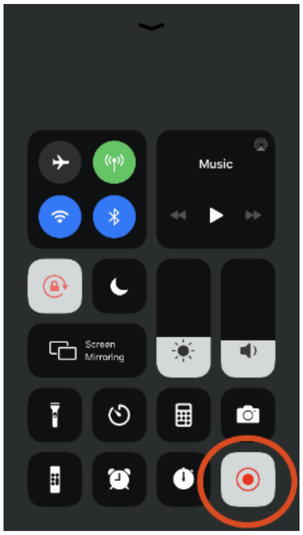
OR



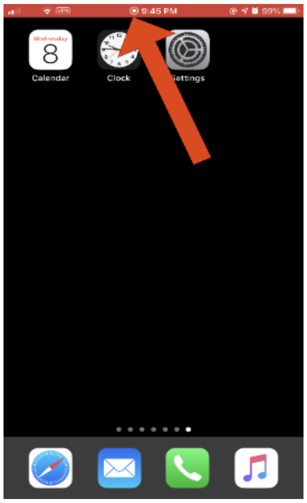
9. To start a recording, press the record button.



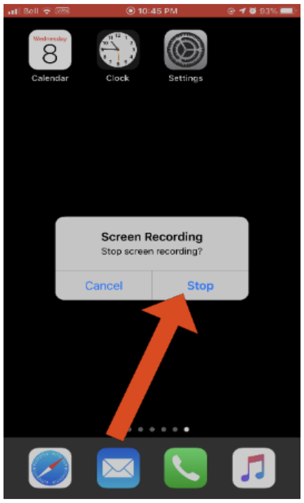
10. When the record button is red, your device is recording the screen.



11. The top of your device's screen will have a red bar indicating that recording is active. To stop a recording, tap the red bar.



12. Then select "Stop." The screen recording will be saved to your photos as a video.



Screen Recording

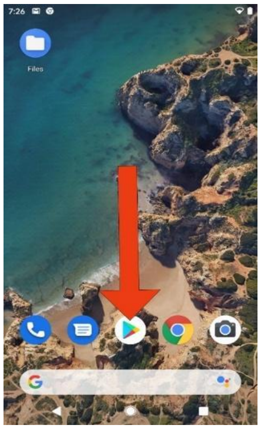
Stop screen recording?

Cancel Stop

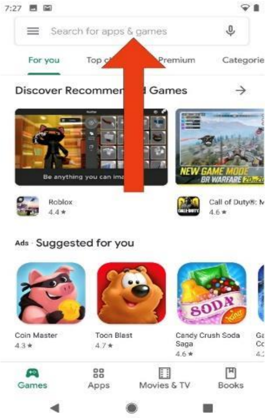
Android: Video Screen Recorder App

Android phones require a video screen recorder app to be installed in order to screen record. Varieties of screen recording apps are available for Android devices. For this walkthrough, the free app “Screen Recorder – No Ads” will be used.

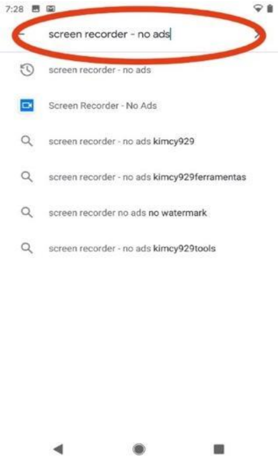
Step 1. Go to the Google Play Store



Step 2. Open a search.



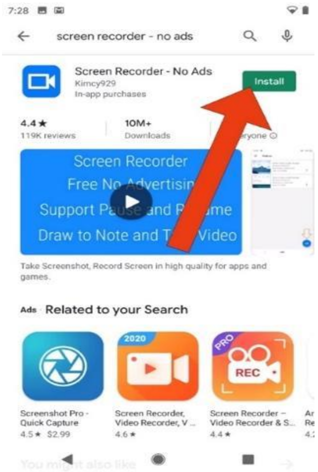
Step 3. Open a search and go to find the app, “Screen Recorder – No Ads”.



screen recorder - no ads

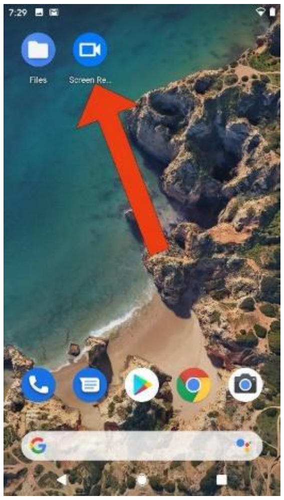
- screen recorder - no ads
- Screen Recorder - No Ads
- screen recorder - no ads kimcy929
- screen recorder - no ads kimcy929ferramentas
- screen recorder no ads no watermark
- screen recorder - no ads kimcy929tools

Step 4. Install the app.

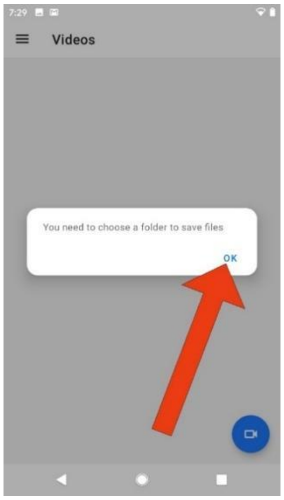


Take Screenshot, Record Screen in high quality for apps and games.

Step 5. Open the app from your home screen



Step 6. You will get some pop-us from the app to enable its settings.

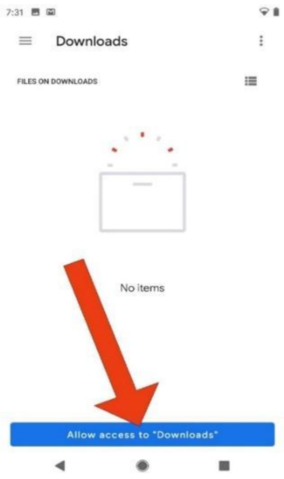


Videos

You need to choose a folder to save files

OK

Step 7. Give access to the “Downloads” folder on the phone to the app. This is where videos will be saved.



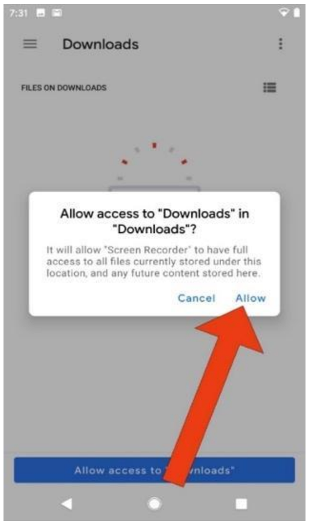
Downloads

FILES ON DOWNLOADS

No items

Allow access to "Downloads"

Step 8. Select “Allow”.



Downloads

FILES ON DOWNLOADS

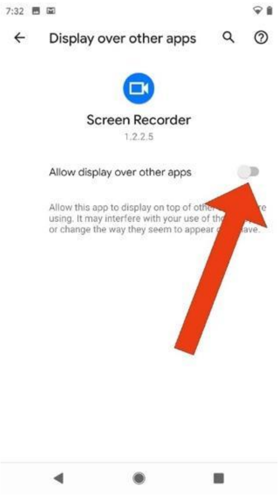
Allow access to "Downloads" in "Downloads"?

It will allow "Screen Recorder" to have full access to all files currently stored under this location, and any future content stored here.

Cancel Allow

Allow access to "Downloads"

Step 9. Select “Allow”.


7:32

Display over other apps

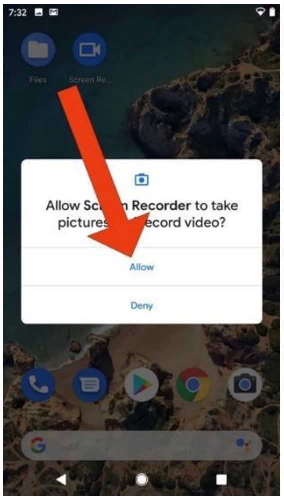
Screen Recorder

1.2.2.5

Allow display over other apps

Allow this app to display on top of oth re using. It may interfere with your use of th or change the way they seem to appear ave.

Step 10. Enable “Allow display over other apps”.

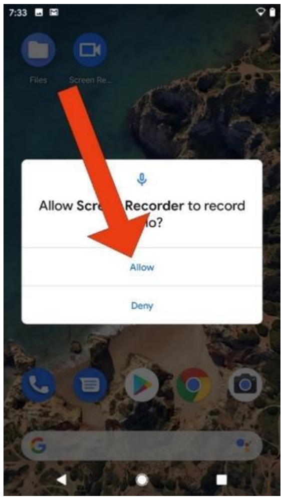

7:32

Allow Sc n Recorder to take picture ecord video?

Allow

Deny

Step 11. Enable “Allow Screen Recorder to record audio”.

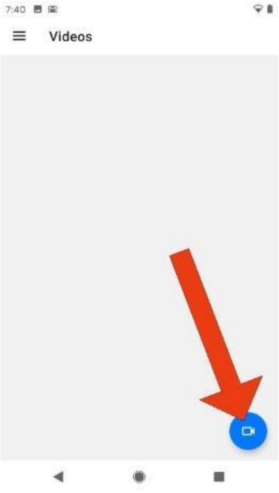

7:33

Allow Scre Recorder to record io?

Allow

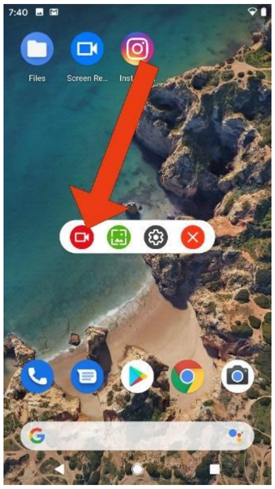
Deny

Step 12. Select the blue camera icon.

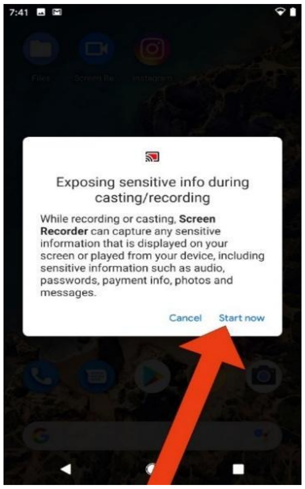

7:40

Videos

Step 13. An overlay will appear with 4 options. Selecting the red camera will start a screen recording.



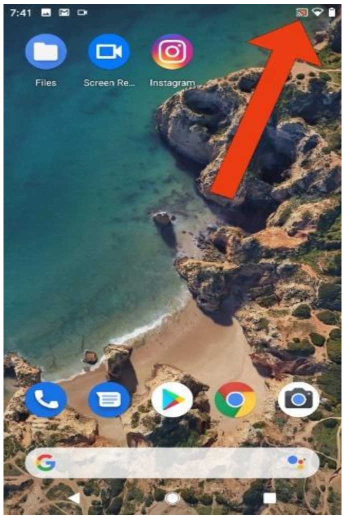
Step 14. You may see a pop-up stating that everything on the screen, from this point forward, will be recorded. Press "Start now" to continue with the recording.



Exposing sensitive info during casting/recording

While recording or casting, **Screen Recorder** can capture any sensitive information that is displayed on your screen or played from your device, including sensitive information such as audio, passwords, payment info, photos and messages.

Step 15. If a recording is active, a little red icon will be present on the top corner of your screen

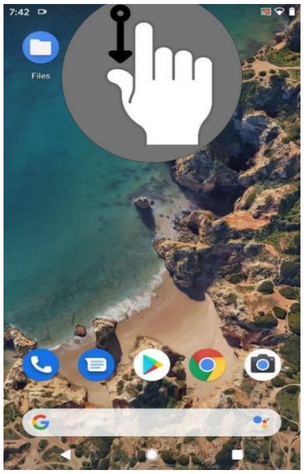


.

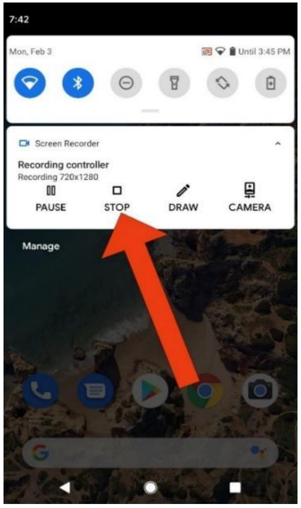
Step 16. To stop the recording, you have 2 options:

A) Swipe down from the top of the screen

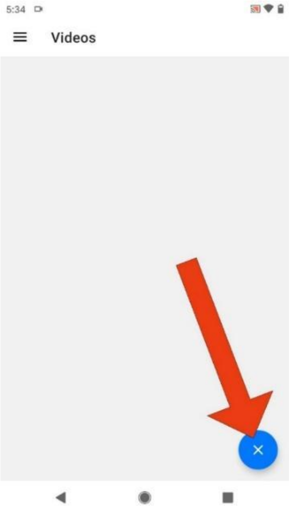
B) Return to the Screen Recorder app



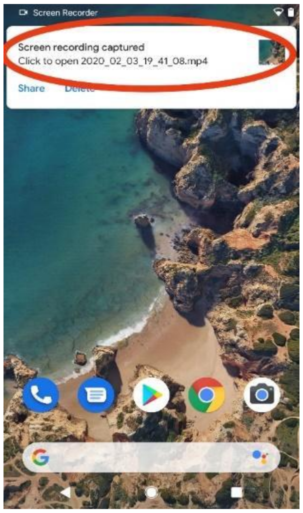
Step 17. Locate the widget for the Screen Recorder and then press “Stop”.



Step 18. From the app, select the blue X.

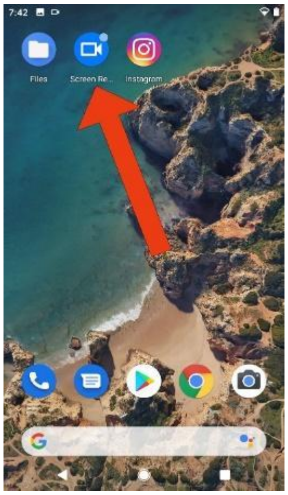


Step 19. You should then see a notification confirming that the recording was captured. If you made a mistake, you can delete the video at this point and start again.



Screen recording captured
Click to open 2020_02_03_19_41_08.mp4

Step 20. Return to the app. From the home screen, you then may see a blue icon on the app indicating a new recording has been saved. Open the app.

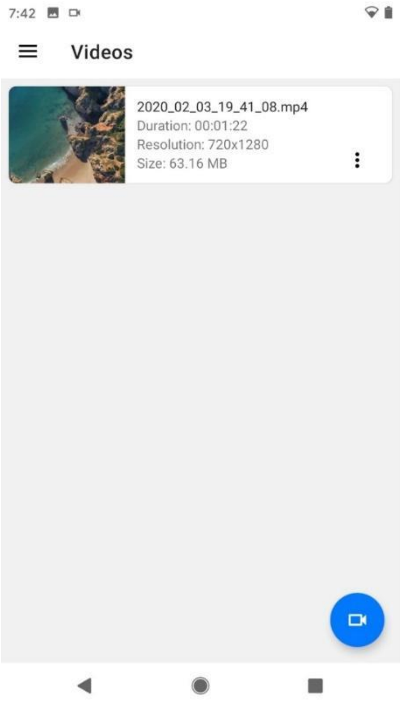


Step 21. You can now access your saved recordings here.

Alternatively, you can find the video by navigating in “files” on your device. However, finding the video in the app is more efficient.

Selecting ⋮ will give you sharing options to send, copy, and upload the file where you want.

Note: Deleting the app will not delete the videos. Delete the videos from the app before removing the app if you want to remove the videos. Alternatively, you can remove the videos from within your “Files” app.



2020_02_03_19_41_08.mp4
Duration: 00:01:22
Resolution: 720x1280
Size: 63.16 MB

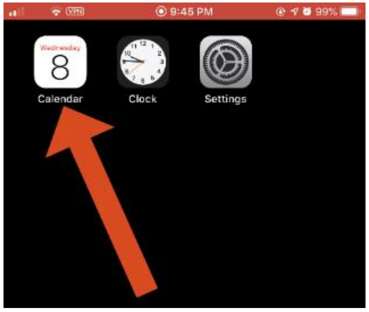
Evidentiary Tips for Using Apple & Android Phones to Video Screen Record

Date & Time

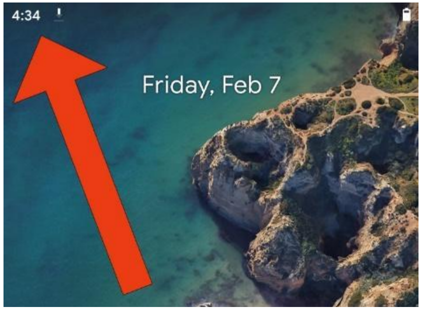
Date

When your video recording is starting, make sure you capture the date your phone displays. This can either be done by opening a calendar app installed on your device or by finding the date displayed elsewhere.

Example: **Apple iOS**



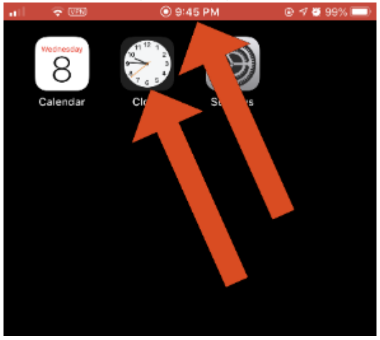
Example: Android



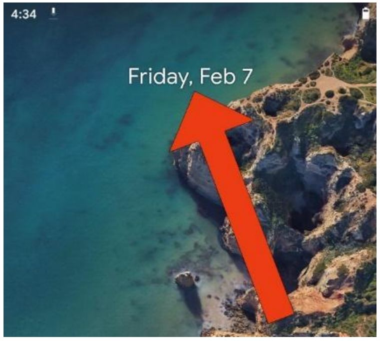
Time

Your recording will likely capture the clock (typically displayed on the top of the device). If this is not the case, after the recording, you should record the date and the time on your phone by navigating to your clock.

Example: Apple iOS



Example: Android



Access

Open the application that has the evidence you want to collect. This can be text messages, email, social media, or anywhere else where conversations are occurring that you want to preserve.

Sender Information

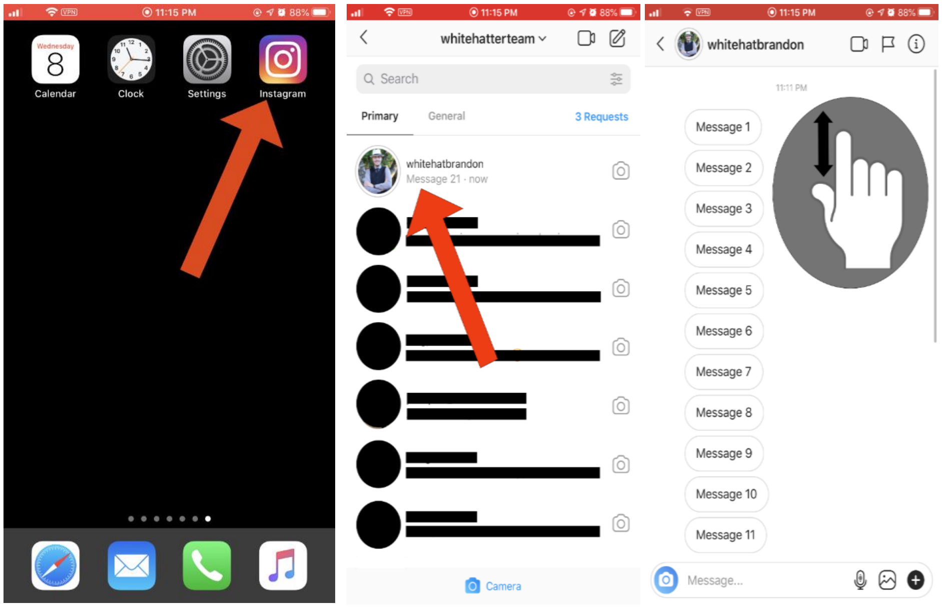
Make sure you are able to see the name, usernames, phone numbers, and emails of the people involved.

Capture the Entire Conversation

Once you have navigated to the content you want to preserve, ensure you start from the beginning of the conversation.

From the start of the conversation, use smooth, slow movements to scroll until you reach the end of the messages. You do not want the video to be blurry. Think about going the speed of a Star Wars opening segment.

EXAMPLE: INSTAGRAM



whitehatbrandon
Message 21 · now

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Message 1
Message 2
Message 3
Message 4
Message 5
Message 6
Message 7
Message 8
Message 9
Message 10
Message 11

How to Store Recordings

Once you have recorded all of the information you need using the screen recording app and you stop the recording, keep the saved video files in a safe place. Remember to back up a copy of the file on a secondary device or storage space. File storage options will depend on your circumstances. For example, your safety may be at risk if the perpetrator still lives in the same home as you and is able to access your smartphone, and uncovers the saved recording. In that case, you may want to ask a trusted friend to back up the files for you, or save them on an email or digital storage space that the perpetrator does not have access to.

Storing digital evidence on a device

If you cannot keep the recording on your smartphone, transfer the file elsewhere (see below) and delete the file from the device. Once deleted, remove any “recycle bin” copies made. Some devices like Apple iOS store deleted photos and videos in a “Recently Deleted” album for 30 days, or until actually removed from the device. Navigating to this album and ensuring the photos and videos are deleted from all spots on the phone can be an important part of a safety plan.

External storage options

Storing digital evidence on an external storage device like a USB memory stick is a good alternative. You will need to know how to transfer the recording off your smartphone and onto another device. To do this, you will likely need to use a computer with a USB attached to it. Make sure you are using a safe device that the perpetrator does not have access to. Check your device for what is needed to transfer files from your smartphone to an external hard drive or USB memory stick, and if it is possible for the model of your smartphone iPhones, for example, may need specific apps and adapters to transfer files from the smartphone to the USB memory stick. Most Android devices require the same connectors as your phone.

> *#TechSafetyTip:* It is best to transfer the audio file as few times as possible in order to minimize questions about the authenticity of your recording.
>
> *#TechSafetyTip:* Keep a record of the steps you took to record and transfer all digital evidence, every time you transfer it, email it, or save it to a new device.

Cloud storage

Storing the recording in the Cloud using an online storage solution like Dropbox, Google Drive, iCloud or others can be a great option if having a physically saved copy is a safety risk. This option can also be simpler than external storage options and may remove the need to purchase any other devices or adapters.

Many cloud storage providers offer free trial plans that are limited in storage. Despite being limited in size, in most cases, these services offer enough storage for a fair amount of screen recordings.

Some example services are:

- Dropbox
- Google
- Amazon
- PCloud
- iCloud

Safety planning around cloud storage

The following are cloud storage safety planning considerations:

- Do not download a video screen recording app for your cloud storage provider that connects directly to your account and/or indicates you have used such an app. The exception would be if you normally use the app for other personal reasons, such as using one for work purposes. You may want to turn off the function of automatic downloading.

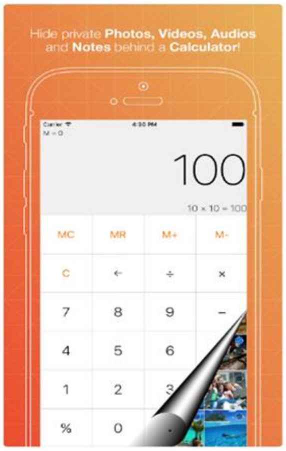
  #TechSafetyTip: if you are using a cloud storage app for personal reasons, create a different account when uploading digital evidence. This will help keep you organized and may protect you from the perpetrator accessing the files if they have access to or know of your personal account.

- Sign up for these services with an email account that the perpetrator does not have access to.

  > *For example, if using a shared email account with the perpetrator or if they know your email password, the perpetrator can use a password reset on the cloud storage account to gain access to it.*

Updates from your cloud storage provider likely will be communicated via email and can signal to the perpetrator that you have an account.

- Create a new email specifically for uploading your digital evidence to the cloud. There are a lot of free email account services. Below is a sample of some services. As a bonus, some email providers also offer free limited cloud storage.
  - Mail.com
  - Gmail.com
  - Outlook.com
  - Protonmail.com
- Be cautious when accessing an email or cloud storage website with a web browser. By default, web browsers keep a browsing history. To remove this digital trail, delete your history after visiting any sites where you are storing your video screen recordings.
- When apps are downloaded from an app store, often the history of what apps you have currently and previously installed will be assigned to your app store account.
- Typically, most online storage options are based in the United States and therefore, bound by US law. Despite how private you may think your cloud storage account is, there is also a possibility that US law enforcement sources may have access to it. Generally, this poses low risk to users, but this still must be considered.


Hide private Photos, Videos, Audios and Notes behind a Calculator!
100
10 × 10 = 100
MC
MR
M+
M-
C
←
÷
×
7
8
9
−
4
5
6
1
2
3
%
0

Decoy Apps

In many app stores, there are apps commonly referred to as "decoy apps." These are file storage apps designed to avoid suspicion by pretending to be different apps.

A common example is a calculator decoy app. This app works exactly like a traditional calculator. But, type in a special code like "36x%29=" and it will open a file folder within the app to save pictures or videos.

It is important to note that even if you are using a decoy app, the files are still stored on the device, although hidden, when using decoy apps. There are ways

to determine if a device contains a decoy app and if a device is being monitored by stalkerware, the perpetrator will have access to everything on your phone.

For more information about stalkerware see BCSTH's information sheet on Mobile Spyware

Connect to an Anti-Violence Worker or Legal Advocate for Support

If you are unsure how to preserve evidence of technology-facilitated violence, contact an anti-violence program in your area for support and to develop a safety plan that includes technology safety considerations. Legal advocates available in BC communities may be able to assist.

BC anti-violence programs and legal advocates:

- VictimLink BC
- Legal Aid BC
- Rise Women's Legal Centre
- Shelter Safe Map
- BCSTH technology safety planning and A Guide for Canadian Women Experiencing Technology-Facilitated Violence: Strategies for Enhancing Safety

Technology Safety Project

This document is a part of a series that details how to preserve evidence related to the misuse of technology in experiences of domestic violence, sexual assault, and stalking. The series is part of the Preserving Digital Evidence of Technology-Facilitated Violence Toolkit. This document, or any portion thereof, may be reproduced or used in any manner whatsoever as long as acknowledgment to the BC Society of Transition Houses is included in the product.

This document was published March 2021.

BCSTH thanks and gratefully acknowledges Brandon Lauer of the White Hatter for his expertise and guidance regarding this information sheet.

BC Society of Transition Houses

THE WHITE HATTER

THE LAW FOUNDATION OF BRITISH COLUMBIA