VAULT APPS

INTERACTIVE RESOURCE GUIDE

SAFER SCHOOLS TOGETHER

ICDTA®
International Center for Digital Threat Assessment

This is an interactive document. Click the underlined links to read more or navigate to the correlating section of the document.

TABLE OF CONTENTS

INTRODUCTION

This Interactive Resource Guide and accompanying Micro Module will provide School Safety/Threat Assessment (SS/TA) Teams with a functional understanding of vault apps and their utility in online data collection.

To best utilize this training, we encourage SS/TA Teams to use this guide in conjunction with the module training. In line with the recommendations provided in our Digital Threat Assessment® (DTA) training, we suggest that your SS/TA Team create a covert(s) account for data collection. Safer Schools Together (SST) recommends against using your personal accounts when searching, as there is a possibility that the searching methods demonstrated may notify the Subject(s) of Concern (SOC).

This Micro Module will discuss the most common ways digital users intentionally conceal photos, videos, and files on their digital devices and the specific steps you can take as a professional or parent/caregiver in identifying, detecting, and preserving digital content. In the past few years, SST's Threat Analysts have seen an increase in the number of incidents regarding digital devices, particularly cell phones, from school administrators and members of law enforcement. Social media and other digital communication platforms such as Anonymous Apps are also commonly involved. Many of these incidents include dangerous communications or the distribution of worrisome, concerning, or threat-related content. As a result, it's common for users, particularly today's youth, to take mitigation measures to conceal certain content including photos and videos.

The purpose of this module is to focus on how today's individuals store digital files in alternative locations, often with the intention to hide or conceal content. There are three primary ways a user can conceal digital files, including photos and videos:

- Utilizing the capabilities and settings of the device itself; this may vary depending on whether a user is using an Apple iOS device versus an Android device.
- Downloading third-party applications; these applications specifically focus on storing and saving digital files to an alternative location outside of the device's photo gallery/photo album.
- Utilizing specific features and functions within popular social media applications.

THE VISUAL EXPERIENCE

By nature, humans are visual creatures – in fact, studies suggest that we are 90% visual beings.[1] The evolution of social media has allowed us to communicate as well as connect with others more efficiently, however, it has also advanced our mode of communication into much more of a visual experience as opposed to simple voice or plain text communication such as texting, email, or instant messaging. This visual experience is particularly appealing to and commonly used by today's youth. Popular social media applications including Snapchat, Instagram, and TikTok capitalize on this visual experience to further the platform's unique features and algorithm capabilities, which make these apps more attractive to both today's youth and adults alike.

Gif Courtesy of Emakina.

[1] We are 90% visual beings - Visual Information (ernestoolivares.com)

THE CONCEPT OF YOUTH CONCEALING INFORMATION

The idea of youth concealing information from their parents/caregivers is not a new concept. When thinking back to your childhood, it may have been common to have specific items or belongings stored in a 'secret' place to avoid detection by others, especially your parents/caregivers. You may have even felt that this area was exclusively under your control and that anyone who accessed this area without your permission would seriously breach your trust and personal privacy.

Today, the quintessential box under the bed now exists in digital form, particularly on mobile devices, and the ability to hide content such as images, videos, and digital communications continues to advance and become more sophisticated.

HOW IMAGES ARE CONCEALED ON MOBILE DEVICES

Some of today's youth do take intentional measures to cover their digital tattoo, even if the activity isn't necessarily harmful in nature. When attempting to conceal online behavior via mobile devices, the following strategies are often implemented:

- Using private browser mode.
- Deleting recent browser activity.
- Frequently deleting private messages.
- Using platforms that delete messages after a certain time frame.
- Creating social media accounts with fictitious identities.
- Enabling certain privacy settings within the device or application.
- Intentionally storing digital files in alternative locations.

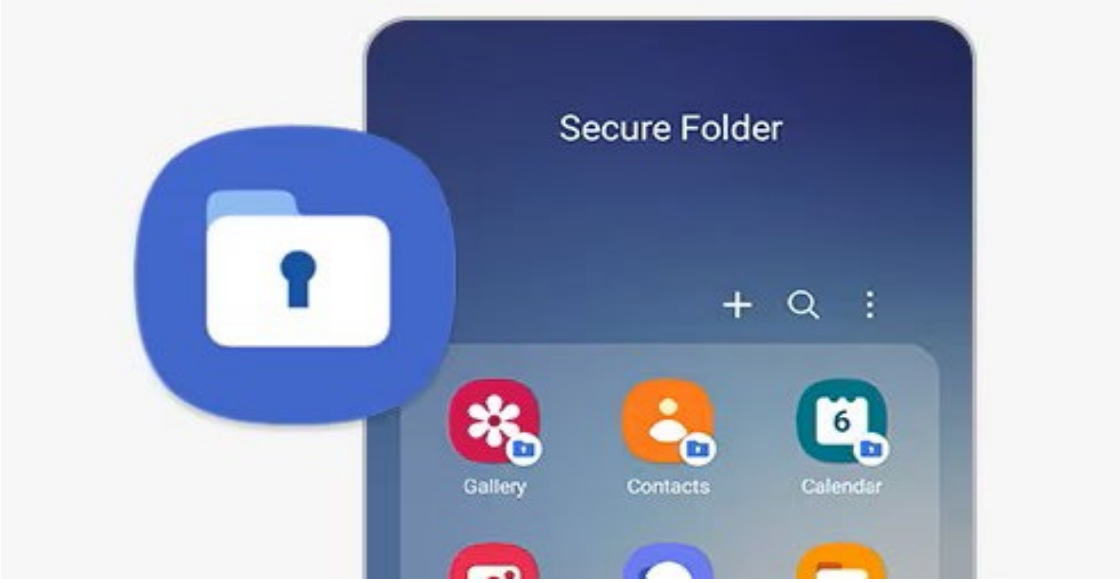
Device Capabilities & Settings

There are a couple of basic ways individuals can hide photos, videos, and/or files using the capabilities and settings within their own digital devices on both iPhone (iOS) and Android devices.

Android Secure Folder

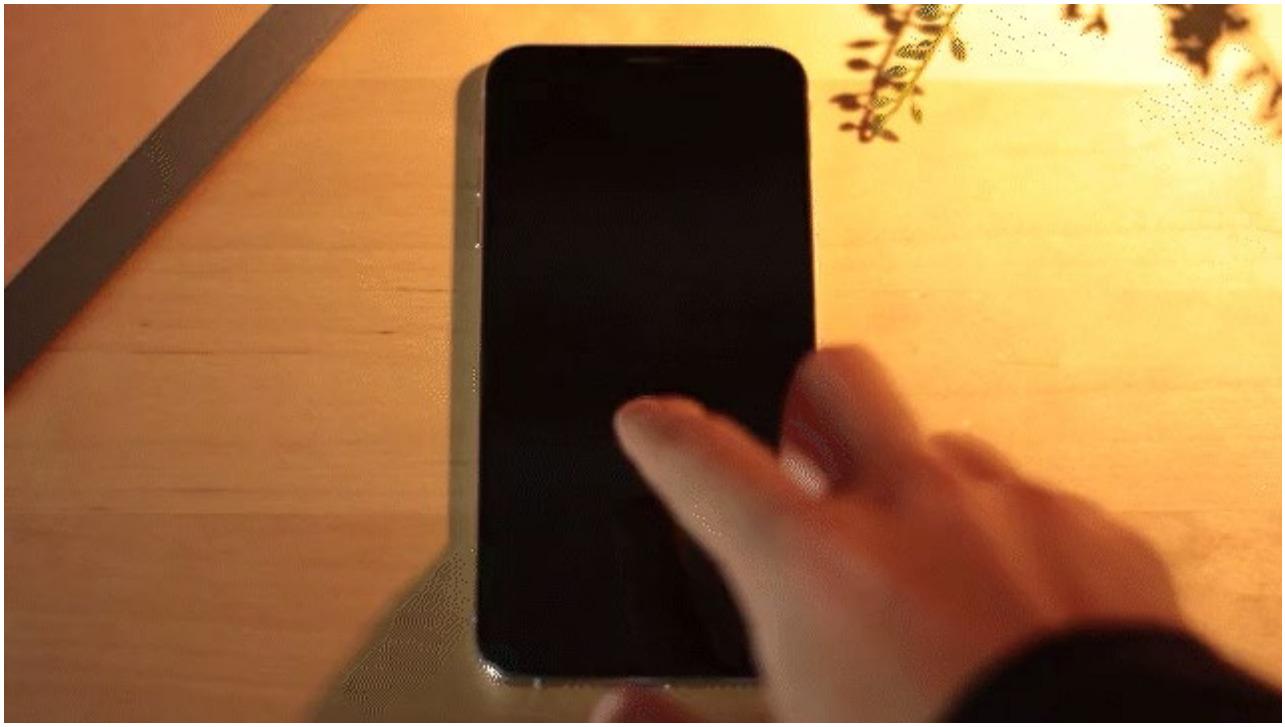
The secure folder on an Android device is an encrypted space that allows a user to store any content or data that they may want to keep private, including photos and videos.

Users can store almost any type of digital content on their device inside this secure folder, including contacts, calendar events, as well as other applications including internet browsers and social media apps. If an app is stored within the secure folder, this will be indicated by a small folder keyhole icon, located in the lower right-hand corner of the application.



iPhone Hidden Album

The main purpose of the 'Hidden Album' feature on iPhone/iOS devices is to conceal photos and videos from being seen by the individual who is in control of the device. Previously, any user who was in control of an unlocked iPhone could locate photos in the 'Hidden Album' so long as they knew how to navigate to this location. However, iOS updates have implemented a default setting that now locks the albums labeled 'Hidden' and 'Recently Deleted'. Due to this new security feature, Face ID or Touch ID are required to access these locations.

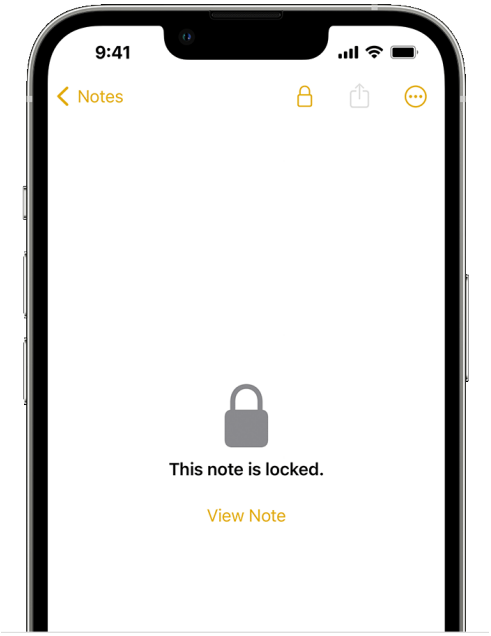


Gif Courtesy of gfycat.


15:48
Edinburgh
19°
Mostly Cloudy
H:19° L:13°
Weather
Phone
Messages
WhatsApp
Apple Frames
BBC Sport
Things
Twitter
Apollo
BBC News
Podcasts
Safari
Mail
Photos
Slack
Settings
15:49
Settings
Measure
Shortcuts
Health
Music
TV
Photos
Camera
Books
Podcasts
iTunes U
Game Center
1.1.1.1
7M Workout
ActivityTracker
Airbnb
15:49
Settings
Photos
Download and Keep Originals
If your iPhone is low on space, full-resolution photos and videos are automatically replaced with smaller, device-sized versions. Full-resolution versions can be downloaded from iCloud at any time.
Upload to My Photo Stream
Upload your last 30 days of new photos and view them on your other devices using My Photo Stream. Photos from other devices can be viewed in the My Photo Stream album, but are not automatically saved to your library.
Shared Albums
Create albums to share with other people, and subscribe to other people's shared albums.
Hidden Album
When enabled, the Hidden album will appear in the Albums tab, under Utilities.
Mobile Data
Turn off mobile data to restrict updates to Wi-Fi, including Shared Albums and iCloud Photos.
PHOTOS TAB
Auto-Play Videos and Live Photos


1:55
Search
Albums
Portrait
Panoramas
Time-lapse
Slo-mo
Bursts
Screenshots
Screen Recor
Animated
Utilities
Imports
Hidden
Recently Deleted
593
Hidden Album
When enabled, the Hidden album will appear in the Albums tab, under Utilities.
Cellular Data
Shared Albums and iCloud Photos.
Reset Suggested Memories
1:56
Albums
Photos 3.427
358
28
64
66
5
216
17
54
Imports 25
Recently Deleted 593

Storing Files on iPhone Notes App



Hiding or securing files on an iPhone/iOS device can also be done by utilizing the device's Notes application. Many of today's iPhone and iPad users don't know that they can store digital files such as documents, photos, and videos within the Notes app. Apple also allows users to secure some of this content further by 'locking' the note behind a password-protected privacy wall.

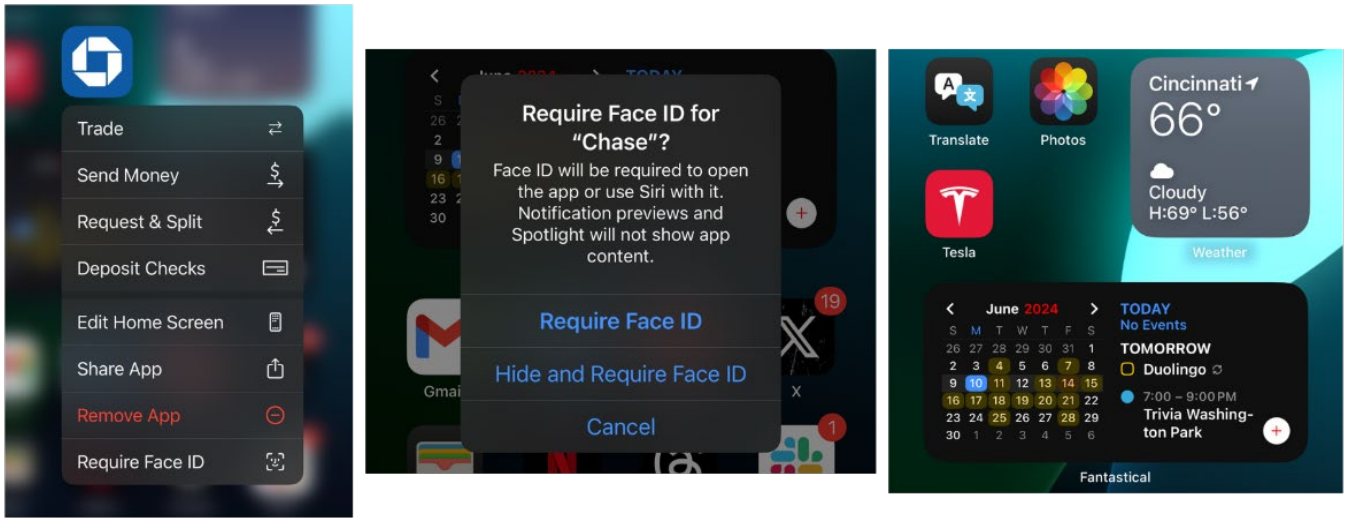
***Disclaimer**:* Please keep in mind that sometimes the nuances and particulars of these features may change over time. However, as of the most recent iOS update, Apple does not allow users to lock a note if the note contains a video or audio file(s). However, currently, the note can be locked if it contains photos. Therefore, this capability would be a very creative way for a user to hide photos on an iPhone and/or an iPad.

iPhone Locking and Hiding Apps

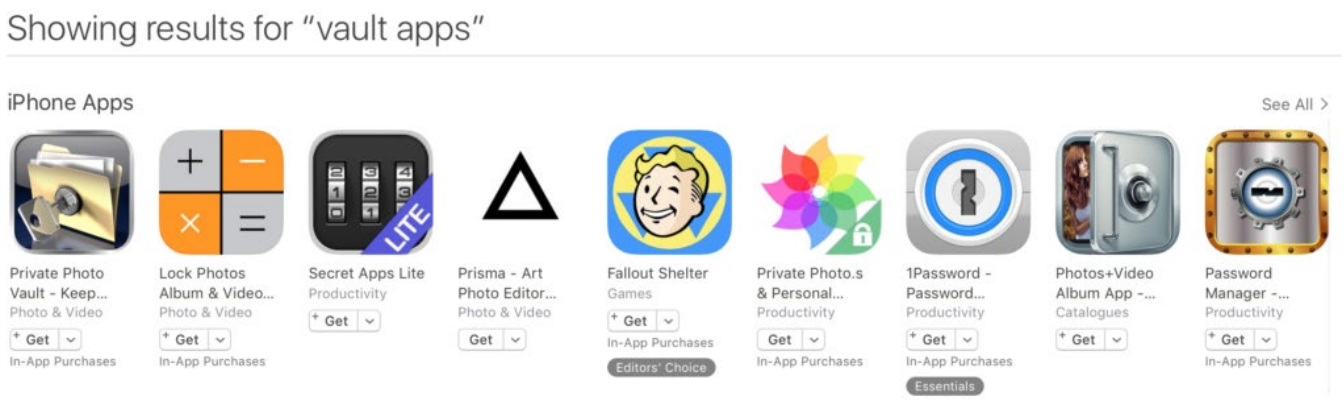
With the release of iOS 18, Apple has now launched a new feature that allows users to lock their apps, as well as hide apps from the home screen. When the app has become "hidden" it will be hidden everywhere except for an area in the settings, as well as the hidden apps folder. To access the hidden apps, you will need either your Face ID, Touch ID, or a passcode to gain access.

Additionally, Apple will now allow users to lock any apps they may wish to add an extra layer of protection. To access the locked app, you will need either Face ID or Touch ID. To lock an app, you will need to follow the steps below.

1. Press and hold on any app.
2. Select Require Face ID.
3. Then choose between Require Face ID or Hide and Require Face ID.
4. The latter will remove the app from your home screen altogether and place it in a hidden apps folder at the bottom of your last apps page.



THIRD-PARTY APPLICATIONS



There are several stand-alone third-party applications that have been engineered and designed specifically to help users hide digital content on their mobile devices. Most of these apps can be downloaded for free from the Google Play Store or the Apple App Store. Many of these apps can be categorized as 'freemium', meaning that they are free to download and use, but offer premium versions that come with a monthly subscription fee. Usually, this paid version of the app comes without pop-up ads that appear with the free versions. Paid versions may also offer additional features and capabilities that are not typically available on the free version of the app.

Some of these apps, including Private Photo Vault and KeepSafe, are transparent as to their purpose and functionality. However, other apps operate in a more concealed manner by disguising the photo vault as something else. This is a common trend, for example, SST Threat Analysts often notice photo vault apps disguised as a mobile device's calculator.

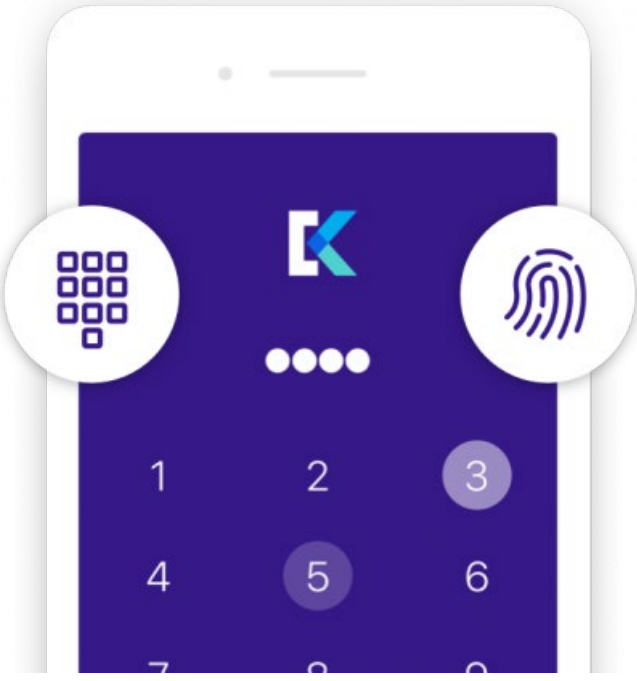
Even though some of these apps may have different features and capabilities, they all share a common general objective which is to store photos and videos in an alternative location instead of in the device's main photo album or gallery.

POPULAR VAULT APPS

KeepSafe

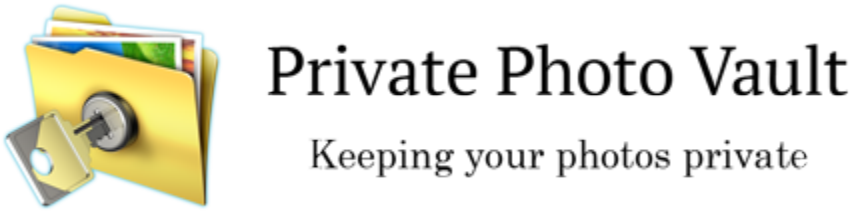
KeepSafe is one of the most popular vault apps and allows users to protect private photos, videos, and internet activity in a secure location. Any digital file stored within the KeepSafe app is saved behind the privacy wall of a simple four-digit passcode. Only an email address is needed to sign up for a KeepSafe account.

Once a user has successfully imported photos and/or videos, the user will receive a message stating 'Import Complete' once all the files have been transferred from the device's gallery to the KeepSafe app; these photos will no longer appear in the device's main photo album/gallery.



The KeepSafe app can be downloaded for free, however, a premium version of the app is available for a monthly subscription fee. The premium version allows users to store up to ten thousand files in KeepSafe, while the free version is limited to two hundred files. Another key feature offered with the premium version of KeepSafe is called 'Break-in Alerts'; if an unwanted third party (such as a concerned parent/caregiver) attempts to gain access to a user's KeepSafe account, the app will log the date and time as well as discreetly capture a photo of the individual attempting to gain access using the phone's front-facing camera. This recorded information can then be reviewed by the account holder within the settings of the application or emailed to the user, depending on the user's settings.

Private Photo Vault



Another popular app used to conceal photos/videos is called Private Photo Vault, which was developed in 2011 and is available on the Google Play Store and the Apple App Store. In terms of its capabilities and functionality, Private Photo Vault operates similarly to KeepSafe. During setup, the user establishes a standard four-digit passcode. They then have the option to have the passcode emailed to themselves in case the passcode is ever forgotten or misplaced. Once the account is established, users have the option to import photos/videos from their gallery, much like any other hidden photo vault application. The Private Photo Vault app also allows users to transfer files from a laptop or desktop computer via a wireless syncing capability. Other features of the paid premium version of Private Photo Vault include a private camera, photo editing software, break-in alerts, and a secondary passcode that unlocks a decoy vault.

Being aware of decoy vaults is crucially important, particularly for law enforcement. If a SOC seems overly willing to grant consent to search their Private Photo Vault app and is quickly relinquishing their passcode, be vigilant. If the passcode reveals photos/videos that seem to be innocent or inconsequential, this may very well be a decoy vault from the primary vault containing potentially concerning, worrisome, or threat-related content.

Photo Vault Calculator Apps

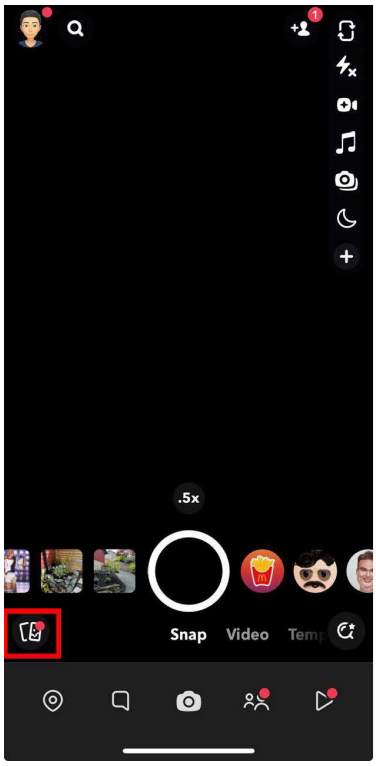
Mobile application developers have become very creative by disguising hidden photo vault apps as other useful tools and applications. One of the most common methods used by developers is making these applications appear as a mobile device's calculator. There are several photo vault apps that appear as calculators, including but not limited to Calculator#, xCalculator, and Calc Box. The availability of these apps may vary depending on if an individual is utilizing an Android or iOS device. However, by reviewing the names of these apps, it's clear to the user what the purpose and intention are behind the app's true capabilities.

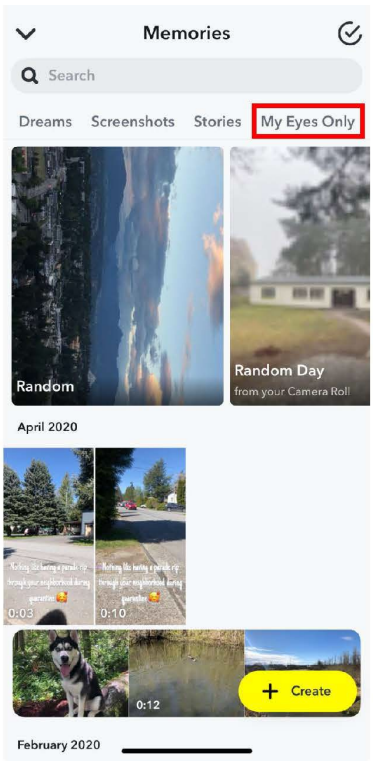
Photo vault calculator apps usually can function as a standard digital calculator; however, the calculator capability is only a smoke screen to conceal the application's true intentions. Even though each of these apps is different, the general premise of their operations is consistent.

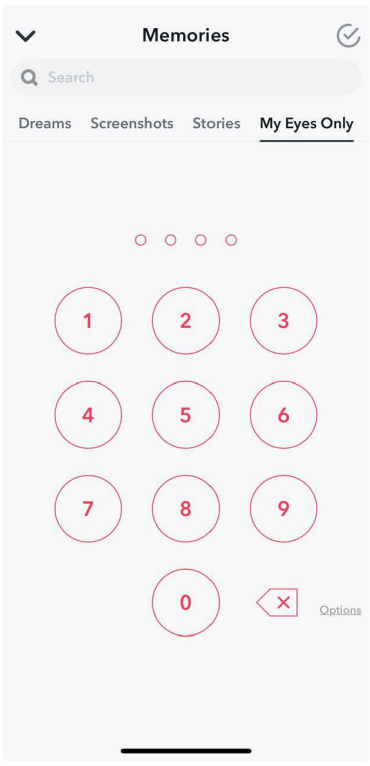
A common question SST's Threat Analysts receive from concerned parents/caregivers is: "How do I know if a calculator app is being used as a photo vault?" Here are two reliable indicators to watch for:

1. In the mobile device's settings, check the 'Digital Storage Summary'. This will give a breakdown as to how much digital storage space each application on the device is using/is capable of. A regular default calculator should occupy little storage space, approximately less than one megabyte.
2. Considering most of these apps are free to download, they typically display pop-up ads in the form of banners and videos. You'll never see any sort of advertising appear on the device's normal default calculator.

Snapchat ‘My Eyes Only’



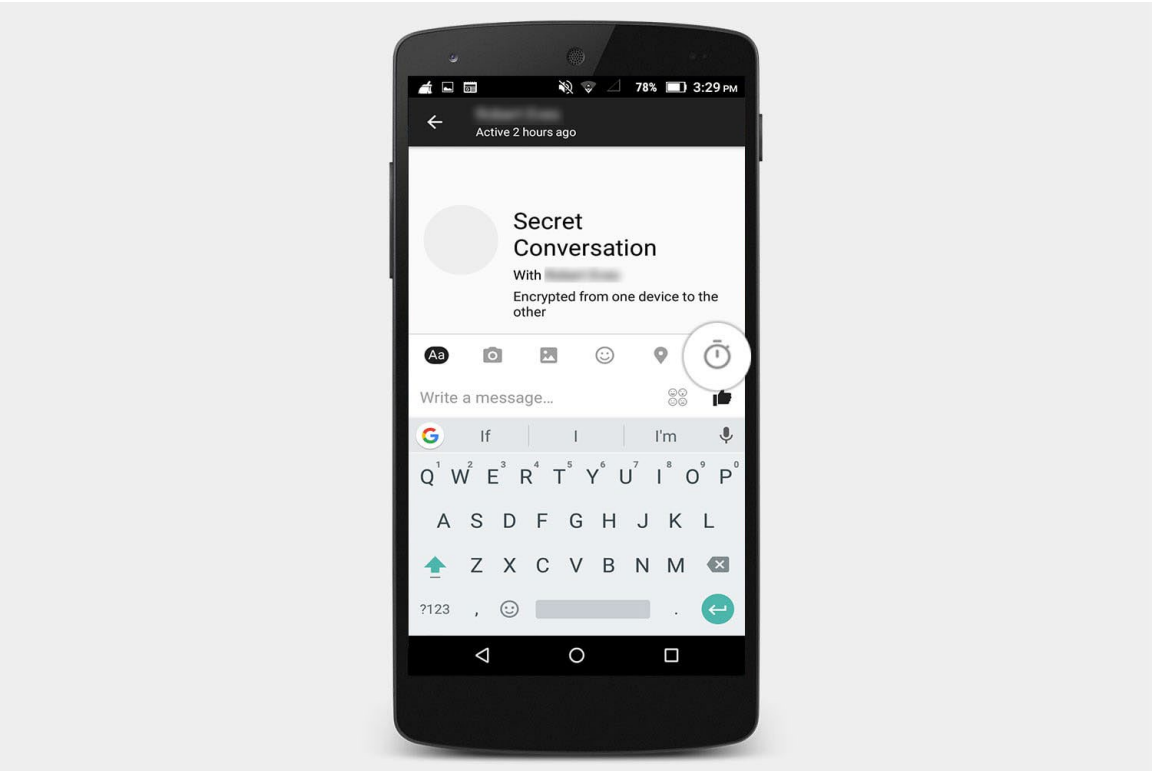




While there are a plethora of photo and video-hiding apps available, Snapchat has a feature available within the application called ‘My Eyes Only’ which allows users to easily hide sensitive images and videos. ‘Snaps’ that are hidden in this section are encrypted and accessible only by using the four-digit passcode created by the user. Snapchat can’t retrieve any of the content saved within the ‘My Eyes Only’ feature due to encryption; this is particularly important information for law enforcement.

Users can also move photos/videos from their camera roll through Snapchat to the ‘My Eyes Only’ section; they can then delete those photos/videos from appearing in the device’s main photo album/gallery.

Messenger's 'Secret Conversations'



With over 263 million+ downloads in 2023,[2] Messenger is one of the most popular apps individuals use to communicate with their friends and family. The app and accompanying online platform via Meta's Facebook utilize instant messaging capabilities.

Certain private messaging apps, including Signal, WhatsApp, Wickr Me, and Telegram, offer end-to-end encryption. Encrypted messaging apps can help protect a user's privacy as they make it difficult for anyone to eavesdrop on your private conversations including the social media companies holding these records.

Messenger includes a setting that will keep certain conversations behind an encrypted privacy wall. This feature is called 'Secret Conversations'.

[2] https://www.statista.com/statistics/1230745/facebook-messenger-annual-downloads-worldwide/

LEGAL IMPLICATIONS OF SHARING INAPPROPRIATE CONTENT

Due to the nature of today's digital landscape, it is imperative to discuss the legal ramifications surrounding the sharing of intimate images/videos that depict children. Statutorily, these types of files are commonly classified as child pornography, child exploitation materials, and/or child sexual abuse materials.

Depending on your jurisdiction, the possession, distribution, and/or production of such files can carry significant legal consequences. Typically, these laws do not differentiate between self-production and the production of others; meaning that it's important for today's youth to think twice about requesting, capturing, and/or sending an inappropriate photo(s)/video(s) of themselves and/or others.

SST's Threat Analysts have identified countless adults who express tremendous amounts of regret for sharing inappropriate photos/videos of themselves when they were minors. Unfortunately, the photos/videos shared did not stop with the person they were originally sent to and were continuously redistributed by more and more individuals. These regretful decisions can and often impact individuals personally, professionally, and relationally throughout their adult years.

Due to the advances in technology and the internet, the facilitation of various child sex crimes has unfortunately become more predominant. Given that these types of crimes involve society's most vulnerable victims (youth), legislators and lawmakers have increasingly implemented stiffer penalties under the law. For example, under United States Federal Law, a first-time offender convicted of producing child pornography faces a statutory minimum of 15 years in prison.[3]

SST often illustrates the following to parents/caregivers as well as students: If a student has sexually explicit images of an underage individual saved on their device and that device is in the student's backpack, locker, or pocket, that is no different than if the student was in possession of a dangerous, controlled substance like cocaine or heroin, which the possession of could result in serious felony charges.

Responsible adults and/or youth who have observed concerning online content involving minors can report such incidents through any of the following methods:

- Contact local law enforcement agencies directly.

[3] https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography#:~:text=Any%20violation%20of%20federal%20child,30%20years%20maximum%20in%20prison.

- Utilize any anonymous reporting tool promoted by your school district such as PSSTWorld.[4]
- Submit a request to Take it Down to potentially remove the Intimate Images/Videos.[5]
- Submit the information to the National Center for Missing and Exploited Children.[6]
- In Canada, incidents can be reported to Canada's online tipline for reporting the online sexual exploitation of children (Cybertip).[7]

***Disclaimer**:* Do not give explicit/intimate images and/or videos a second life. If these images/videos are brought to your attention, and the information needs to be preserved, the best practice is to seize the device, disconnect the device from all cellular, Wi-Fi, and Bluetooth connectivity, and pass the device along to law enforcement. Never screenshot, take photos/videos of, email, text, or further distribute explicit/intimate images and/or videos.

[4] https://www.psstworld.com
[5] Take it Down
[6] https://report.cybertip.org
[7] https://cybertip.ca/en/

TOOLS FOR PARENTS/CAREGIVERS, EDUCATORS, AND LAW ENFORCEMENT

Digital devices and digital platforms are here to stay and will continue to be a part of our daily lives, especially that of today's youth. SST feels it is imperative for parents/caregivers to have these conversations with their children about the responsible use of technology and digital platforms. We encourage these conversations to occur, not only prior to youth receiving their first mobile phone or tablet but also to continue to have discussions about digital responsibility throughout their adolescent years.

It's not a matter of if, but when, a child sees something concerning online, receives an inappropriate/uncomfortable message, or observes a friend engaging in risky behavior. Youth who feel comfortable enough to disclose such incidents to their parent/caregiver or a trusted adult can make a huge difference in how a worrisome incident is handled, often resulting in a higher chance of a positive resolution.

Luckily, there are several remarkable online resources available for parents/caregivers, educators, and law enforcement to help promote healthy and safe online activity for today's youth:

- **Netsmartz**
  - A program established by the National Center for Missing and Exploited Children (NCMEC).[8]
  - PowerPoint presentations, educational videos, tip sheets, and classroom activity resources tailored to students of specific age groups designed to help School Resource Officers (SROs) and educators organize fun and essential instructions for students while promoting online safety within their schools and communities.
- **Cybertip Canada**
  - Free online safety resources for parents/caregivers and children, including activity books and an interactive series that gives youth an opportunity to have fun exploring online safety through games, comics, quizzes, and more.
- **Safer Schools Together**
  - Free Parent/Caregiver resources,[9] including Raising Digitally Responsible Youth: A Parent/Caregiver's Guide, Sexting Safety Agreement, Social Media Checklist for Parents/Caregivers, Common Sense Media Digital Contract, and Internet Lingo & Slang Terms.

[8] https://www.missingkids.org/netsmartz/home
[9] https://saferschoolstogether.com/resources/parent-resources/

CONCLUSION

SST hopes that the material and information in this training module and accompanying resource guide will equip you with the knowledge, skills, and power to make a positive impact in your schools, communities, and the life of every student you interact with.

SST stands committed to helping promote positive, safe, and caring learning environments for every student, staff, parent/caregiver, and individual within your schools, districts, and communities. We are here to support you throughout your training and beyond; if you require assistance or have any additional questions, please contact us at info@saferschoolstogether.com.

ADDITIONAL RESOURCES

Safer Schools Together: https://www.saferschoolstogether.com

International Center for Digital Threat Assessment: https://www.icdta.org

Anonymous Online Reporting Tool: PSSTWorld: https://www.psstworld.com

SAFER
SCHOOLS
TOGETHER

ICDTA®
International Center for
Digital Threat Assessment