DIGITAL THREAT ASSESSMENT®

INTERACTIVE RESOURCE GUIDE

SAFER SCHOOLS TOGETHER

ICDTA®
International Center for Digital Threat Assessment

TABLE OF CONTENTS

INTRODUCTION

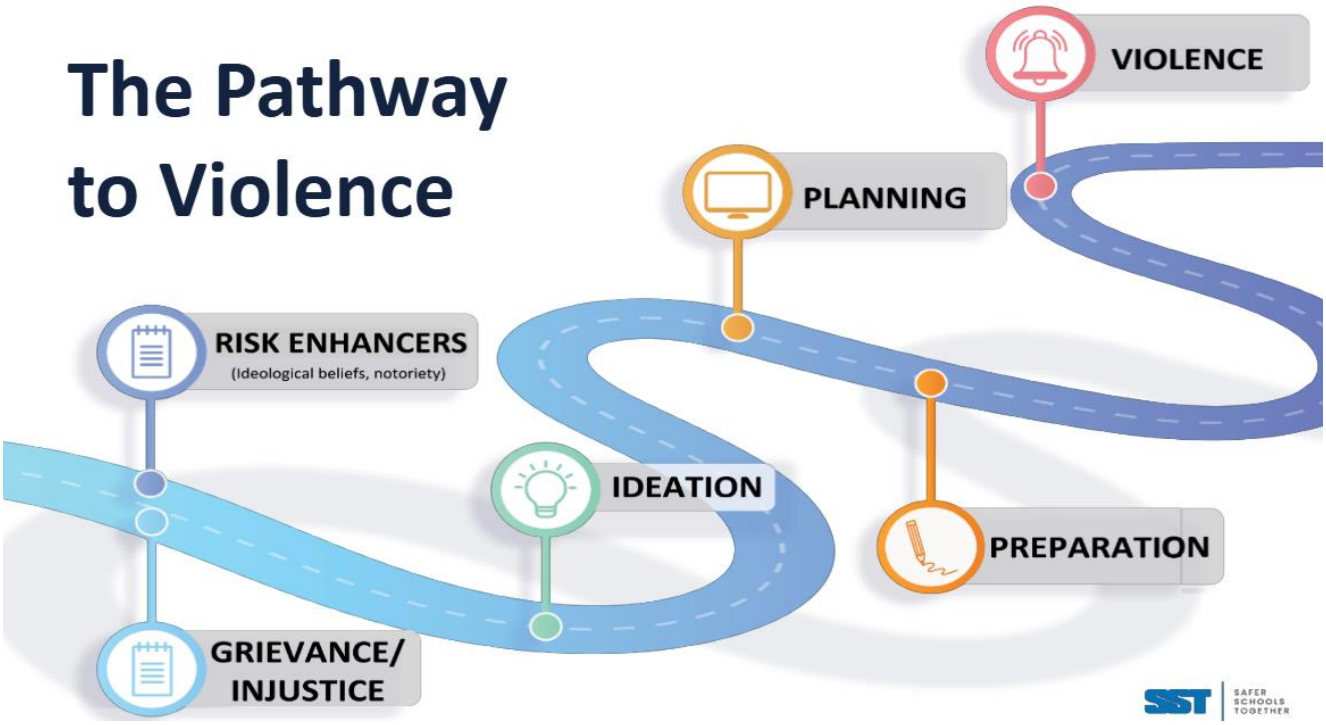
Most violent school attacks have had vital information leaked online in the form of social media posts. Knowing where, how, and when to look for this information is critical to the threat assessment process.

Digital Threat Assessment® was developed in 2015 by Safer Schools Together to keep pace with how ever-evolving technology and digital platforms can negatively affect school and public safety today. Digital Threat Assessment® training provides tools and open-source methods to establish the digital baseline of a threat maker by locating, documenting, and assessing social media data through a threat assessment lens.

The training and information provided will enhance the effectiveness of your multidisciplinary threat assessment process. Ideally, your school/school district should already have a multidisciplinary Threat Assessment Team (including law enforcement) in place, as well as processes and procedures for assessing threat-related behavior.

Note: Given that technology, the internet, and social media are constantly evolving, we do our best to keep these resources up to date. However, there is always the chance that they could be taken down, go out of business, stop working, or become obsolete. However, Safer Schools Together ensures to keep this guide up to date to provide the most effective resources.

The majority of individuals do not simply "snap" and engage in high-profile violence, instead, they evolve along a pathway to violence, during which individuals will typically leave leakage. This often provides evidence of their grievance or perceived injustice, ideation, planning, preparation, and potential violence.



'Remember that individuals may evolve along a pathway to violence.'

Engaging in online open-source data collection utilizing social media platforms, blogs, forums, and the dark web is the best practice for establishing a digital behavioral baseline. This often provides evidence of ideation and/or the manifestation of a grievance or perceived injustice.

Collecting and preserving evidence of the Subject of Concern's (SOC) digital baseline is key in ensuring all evidence is documented as we go. We want to ensure we save this information as you may never know when the SOC may remove a social media post. Once documented, review the information in a multidisciplinary team. These teams are critical in recognizing that online information needs to be considered within a larger context. It is recommended that School Safety / Threat Assessment Teams use dedicated social media accounts when needed as personal accounts are never recommended, this will be touched on later.

In most mass killings, there was leakage, whether that be telling friends, in person, by letting something out that revealed their intentions. “Leakage occurs when an individual intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes or intentions that may signal an impending violent act.”[1]

Now with the digital age, leakage has evolved and has become more prevalent, and more accessible. This is good news. Digital leakage was the factor for the creation of the Digital Threat Assessment® training and all the services we provide today.

[1] What is Leakage?

UNIT 1: BASICS OF THREAT ASSESSMENT

Digital Threat Assessment® (DTA) is one component of an overall violence prevention strategy, ensuring school communities are safe and caring environments. The primary objective of school violence reduction strategies should be to create cultures and climates of safety, mental wellness, respect, and emotional support within the school. Remember, no two cases are the same! Below are some basic components to consider when discussing DTA®.

Behavioral & Digital Baseline

Some professionals underreact to threat-related behavior and active threats of violence by not considering current behavioral and digital baselines, perceived grievances, and justification for the target and site selection.

Behavioral and digital baseline assessments are used to determine the SOC's behavioral baseline. If the behavior is not typical for the SOC or has shifted from the previously identified baseline, an increased level of risk should be considered.

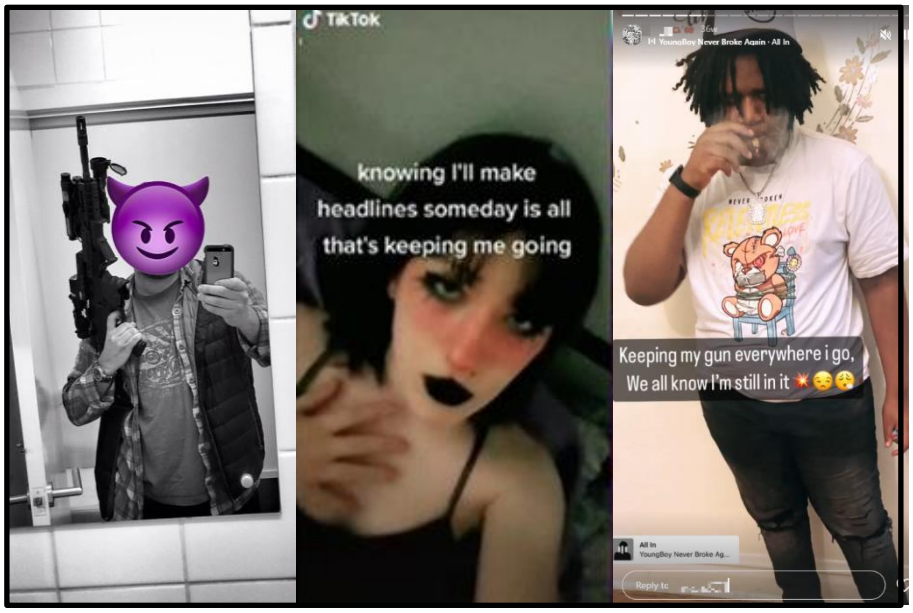
For example:
A student sends out a Snapchat regarding a vague threat stating, “Don’t come to school tomorrow.” Upon a check of their social media to establish a digital behavioral baseline you find out that this student has been posting on their TikTok numerous times to “not come to school.” Further interviews with peers indicate that the student has been saying these things similar to this every day for years now. They also do not appear to have any access to the means. As this behavior has been consistent over a period of time, this may denote a lower level of risk but should be monitored for any changes.

Defining a Threat

A threat is the expression of intent to do harm or act violently against oneself, someone, or something.

A threat can be spoken, written, electronic, symbolic, or through any other means. All threats are not created equal, and no two threat makers are the same. Therefore, it is imperative that we utilize multidisciplinary teams to determine the initial level of risk. Some individuals who are feeling helpless and out of options may see harm to themselves or others as the only way to solve a problem or settle a grievance.

Most threat makers are unlikely to carry out their threat, however, all threats must be taken seriously and the initial level of risk and immediate risk-reducing interventions should be completed as soon as possible.



'All threats are not created equal and no two threat makers are the same.'

Specificity of the Threat – Types of Threats

Direct: A threat that identifies a specific act against a specific target and is delivered in a straightforward, clear, and explicit manner. “I am going to stab Jason in the cafeteria at lunch.”

Indirect: A threat that tends to be vague, unclear, and ambiguous. “I could kill you; I could kill everyone in this school.”

Veiled: A threat that strongly implies, but does not explicitly threaten with violence. “My life would be better if you weren’t around anymore.”

Conditional: A threat that warns a violent act will happen unless certain demands or terms are met. “If you don’t give me the money you owe me, I am going to shoot you.”

Assessing Online Threats

Capacity – Physical and cognitive capacity and physical proximity to carry out attack.

Intent – Motivation and desire to carry out an attack.

Plausibility – An important variable in determining whether the verbal/written threat should be taken seriously enough to start a TA (i.e. threat to stab vs. driving a tank through the school).

Specificity – The amount of detail in the threat. Are there any grievances, target selection, site selection, times and dates, means to carry out the threat, etc.?

Behavioral Baseline – What is the known or current behavioral baseline of the SOC? Has there been any recent shifts in that baseline?

Attack-Related Behaviors/Access to Means – Have they engaged in any behaviors consistent with the threat? Have they attempted to access the means?

Access to the Means

A crucial question to ask in the initial response to a threat is: Does the threat maker have the means to carry out their threat?

If a student posts a picture of a firearm on social media and states that they are going to kill a classmate, law enforcement and the threat assessment team will need to ascertain if the student has access to a firearm to carry out the threat.

A key variable in the assessment of the threat is to find out whether this image is **stock** (sourced online - not original) or **likely unique** (not sourced anywhere else online - original). This is a foundational Digital Threat Assessment® tool that is covered at length in the Reverse Image Search section.

Zero Day - full movie (2003)

Inordinate Knowledge

Inordinate Knowledge can be defined as knowing a subject much more than usual or expected.[2] Note the characters above in the image, these individuals are Andrew Kriegman and Calvin "Cal" Gabriel. These are fictional characters from a Mockumentary called Zero Day, released in 2003. This is considered Inordinate knowledge, something we have seen referenced at a much higher rate since the 25-year mark of the Columbine tragedy. Multidisciplinary teams are imperative in understanding inordinate knowledge as what might be obvious for one Threat Assessment member might not be so obvious for another.

Perceived Grievance, Injustice, And Justification

Injustice collectors harbor resentment over real or perceived injustices. No matter how much time has passed, the injustice collector will not forget or forgive those wrongs or the people they believe are responsible for the injustices. The injustice collector may keep a hit list with the names of people they feel have wronged them.

Justification is the process through which the potential offender seeks or is given the means to justify the intended violence. The SOC uses these justifications to rationalize the purpose and intent of the intended violence. The process itself is highly subjective and tracking the process is highly dependent on context and individual factors.

Dehumanization

Dehumanization is the process that allows a person to emotionally, psychologically, and cognitively distance themselves from the nature of the act.

In our threat assessment practices, we need to consider the data. What data do we have to determine the level of potential dehumanization?

- What role does the video game play in providing further justification to the target(s) or site?
- Are the video games the SOC is playing perpetuating a type of perceived or falsified grievance?

How many hours of the day or week are video games consuming the life of the SOC? Does the SOC have an addiction to video games? If yes, what is the potential impact from the number of hours during gameplay?

THE ROLE OF VIDEO GAMES IN DEHUMANIZATION AND MEDIA RESOURCES

Violent Video Game Montage
Raising Digitally Responsible Youth: A Parent's Guide.
Cyber-dehumanization: Violent Video Gameplay Diminishes Our Humanity.
How Self-Dehumanization Spirals Into Unethical Behavior.
Stop Worrying About Video Game Violence and Start Thinking About Dehumanization.

Identifying Worrisome Behavior

Worrisome behaviors are those that cause concern for members of the school and/or law enforcement agencies because of their violent content. They may be an early warning sign of more serious high-risk behaviors. Worrisome behaviors are specific to the individual and may include drawing pictures, writing stories, or making vague statements that do not necessarily constitute "uttering threats" as defined by law but cause concern for

[2] Inordinate Definition

some members of the school, family, or community. Following up on worrisome behaviors results in effective early intervention measures. Most often, if there is no intent to harm, worrisome behaviors can be managed through problem-solving, restorative practice, or strengthening existing supports.

A variety of situations call for schools to initiate a threat assessment and even possibly request law enforcement participation. Although not an exhaustive list, the following situations should lead to a threat assessment.

Safety leaders should ensure that teachers, support staff, and other members of the community understand what constitutes worrisome behavior and the importance of reporting signs of worrisome behavior.

- Serious violence or violence with intent to harm or kill
- Fighting and resulting grievances that do not subside
- Displays of aggression or violence
- Indicators of suicidal ideation as it relates to fluidity (both homicidal and suicidal)
- *Suicide risk assessment may be required
- Verbal/written/nonverbal (implied) and direct threats to kill others (“clear, direct, and plausible”)
- The use of technology (social media posts) or writings that suggest that the Subject of Concern (SOC) has engaged in threat-related behaviors or has demonstrated unusual interest in other instances of mass casualty attacks, radicalization, incels, and/or other content that encourages targeted violence.
- Possession of weapons (including replicas)
- Bomb threats (making and/or detonating explosive devices)
- Fire setting (contextual)
- Sexual intimidation, sextortion or assault
- Ongoing issues with bullying/cyberbullying behaviors and/or harassment
- Gang-related intimidation and violence
- Targeted hate incidents motivated by factors including, but not limited to; race, culture, religion, and/or sexual orientation
- Concerning changes in behavior or mental state

Anonymous Reporting Tools

An anonymous online reporting tool built specifically for students to report concerning behavior is a proven method of building trust between students and their school/school community. While SST understands the importance of cellphone policies, it is imperative students have the opportunity to report during school hours as we see almost half of tips submitted are during these hours. Examples of what students can anonymously report through our own PSST World Report It Now! tool:

- Bullying.
- Cyberbullying.
- Harassment.
- Social Media Issues.
- Inappropriate Sexual Behavior.
- Concerns about adult(s).
- Drugs/Alcohol.
- Gang Activity.
- Weapons or Threats.
- Mental Health Concerns.
- Suicide.
- School Attack/Shooting.

Although Reporting Tools can help foster a safe and caring environment; creating safe schools has everything to do with building relationships and investing in our communities. Here's a secret, school staff and safety resource officers are your best investment for helping students feel connected. The connections a student has, instill a sense of belonging and acceptance and do more to promote safe, healthy, and caring schools than anything else we can do.

UNIT 2: ACCESSING AND DOCUMENTING INFORMATION

You are presented with some information containing a threat: stay calm.

The first thing to remember is that not everything is as it appears. Posts, photos, conversations, and web pages can be falsified so always consider a source's validity. Assuming the immediate safety of others is secure, your next step is to begin a Digital Threat Assessment®. Determining an individual's baseline from online behavior will provide your team with a broader perspective, translating into a heightened ability to plan appropriate intervention strategies.

Find a starting point like a full name, username, photo, location, etc. This can be considered a seed - from that one piece of information, other information will amass, and additional starting points will be revealed.

EVERYTHING is information. Record the results of your Digital Threat Assessment®. A competent School Safety / Threat Assessment Team knows how to preserve data for later review and multidisciplinary team assessment.

During your documentation process, you may come across videos or other media such as GIFs, interactive profiles, etc. There are techniques that can be used to screen record your desktop or download video clips on different platforms such as YouTube, Instagram, and more.

What to Include in Digital Baseline Collection

- Usernames.
- Vanity Names.
- Real Names.
- Screenshots.
- Preserve Videos.
- Bios.
- Information on Others Tagged in Posts.
- Profile Web Addresses.
- Date and Time of Collection.
- Date and Time of Concerning Posts.
- Location of Post, if possible.
- IP Addresses, if possible.

Threat Assessment Accounts

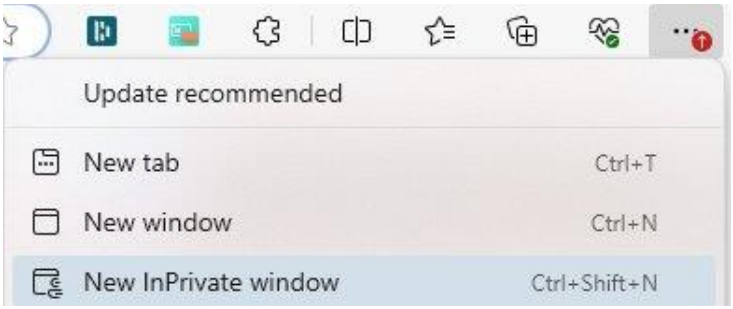
The methods we use to conduct a threat assessment online are imperative to our success. Most crucial is to ensure that you are not using a personal account that might inadvertently inform the individual you are researching about their activity. Consider how easy it is to accidentally double tap a post. That double tap sends a notification to the social media account holder that you, the user whose account name is currently logged in, just liked their post. The outcomes of this action could be harmful to the safety of that individual and your larger community.

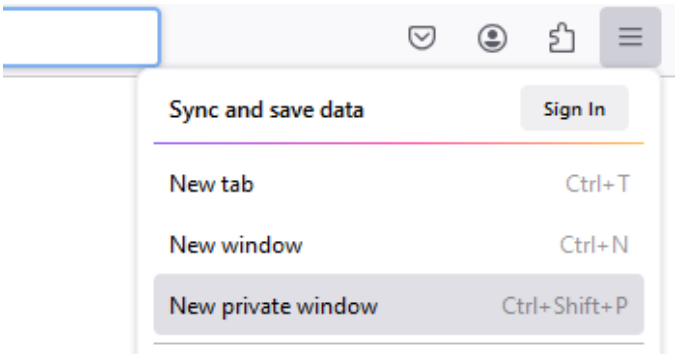
At Safer Schools Together, we recommend that Threat Assessment Teams create one social media account for each platform, only to be used for Digital Threat Assessment® research within that team. It is best practice to use the same email address and other verification information in the creation of all your threat assessment accounts.

When creating your social media accounts, we will want to use a threat assessment e-mail as well. Our team recommends using Tuta Mail to create your threat assessment e-mail. Once this e-mail is created, use it to create your threat assessment accounts. Please note that Tuta Mail can take up to 48 hours to verify your email, therefore, it is recommended that threat assessment accounts are set up proactively, not reactively.

So, how do we combat the effect of cookies and previous search history when conducting Digital Threat Assessments®? The answer is easier than you may have imagined - we enable Incognito or InPrivate browsing mode. Every browser has this functionality built in. Microsoft Edge calls it the InPrivate window. Firefox calls it the Private window. Chrome calls this functionality the Incognito window. The net effect of an Incognito or InPrivate mode is to halt the collection of cookies being stored on your computer and to ignore any previous search histories.

To open the private mode in your browser, click on the more button, often referred to as the three dots or the hamburger menu, at the top right-hand corner of your browser. If you prefer using keyboard shortcuts, pay attention to your preferred browser's shortcut which is displayed beside the private or Incognito option. For example, the keyboard shortcut to open a private window in Firefox is control shift P.





Documenting Content

When it comes to social media content, timeliness is everything. A social media post or video can be online and available one moment and when you refresh the page, it is gone. “Page not found,” “Video has been removed by author,” “Post no longer available,” etc. are all messages that you never want to see if you haven’t saved and documented that content.

So, as a rule of thumb, it is very important to document and save all notable content (images, videos, comments, pages) as soon as you come across it. The following section will walk you through screenshotting images and videos and saving them as .jpg (image) and .mp4 (video) files.

When establishing a digital behavioral baseline, it can be helpful to paste (once copied to the clipboard) or drag the screenshot into a working document.

SCREENSHOTTING

	Windows Key + Shift + S Prt Scn (if updated) Snipping tool
	Cmd + Shift + 5 Cmd + Shift + 4
chromebook	Ctrl + Shift + Switch Windows

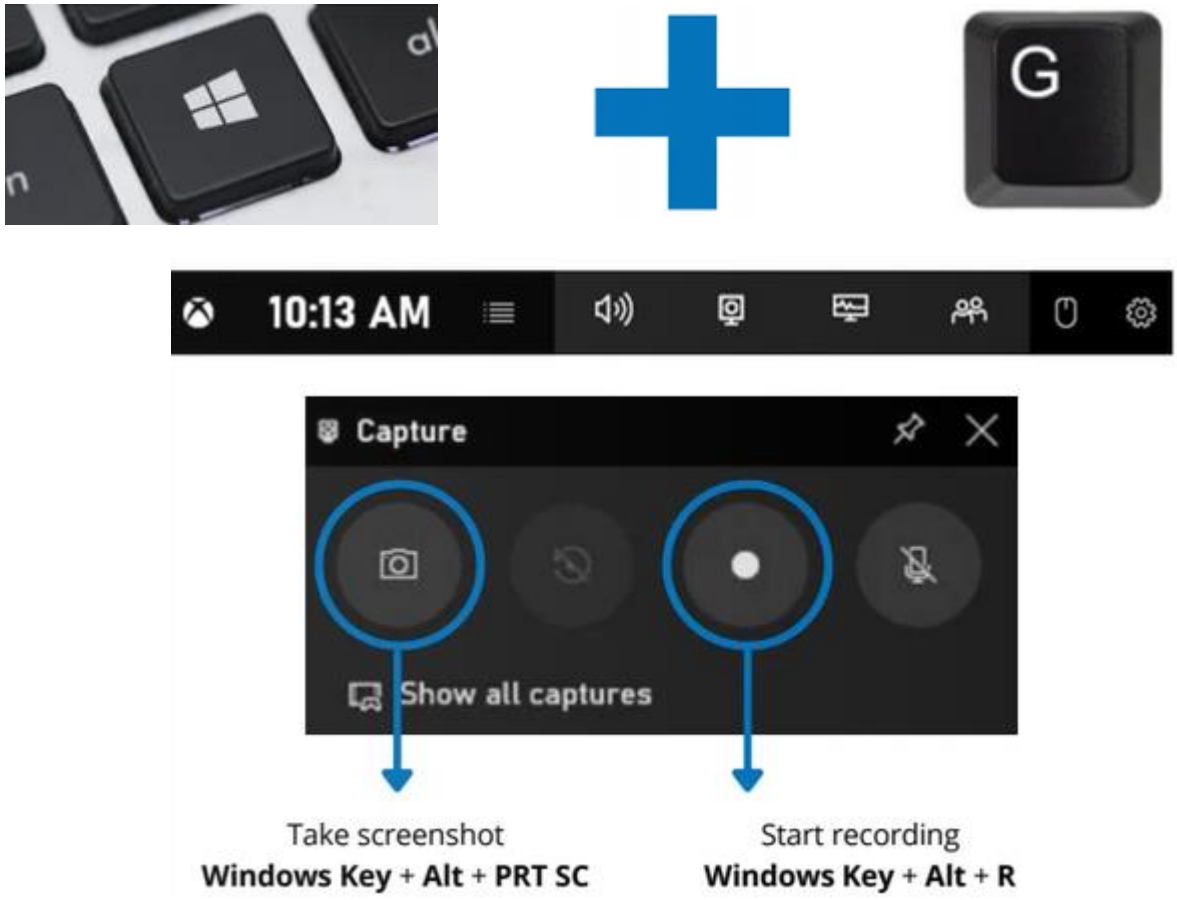
Additional Options for Screenshotting:

Be mindful when screenshotting, certain mobile platforms will send a notification (Snapchat).

SCREEN RECORDING

Windows OS Recording:

Press and hold Windows Key and G at the same time to open the Windows OS Recording tool. Visit WindowsCentral for more information.



Mac OS Recording:

If you're using macOS Mojave or later, from Command + Shift (⌘)+5 on your keyboard to see onscreen controls for recording the entire screen, recording a selected portion of the screen, or capturing a still image of your screen (direct shortcut to this is Command + Shift (⌘)+4).

Record the Entire Screen

1. Click the on-screen controls. Your pointer changes to a camera.
2. Click any screen to start recording that screen, or click Record in the on-screen controls.
3. To stop recording, click the menu bar or press Command + Control + Escape.
4. Use the thumbnail to trim, share, save, or take other actions.

Record a Portion of the Screen

1. Click the on-screen controls.
2. Drag to select an area of the screen to record. To move the entire selection, drag from within the selection.
3. To start recording, click Record on the on-screen controls.
4. To stop recording, click the menu bar or press Command + Control + Escape.
5. Use the thumbnail to trim, share, save, or take other actions.

Visit HERE for more details on Mac OS Screen Recording.

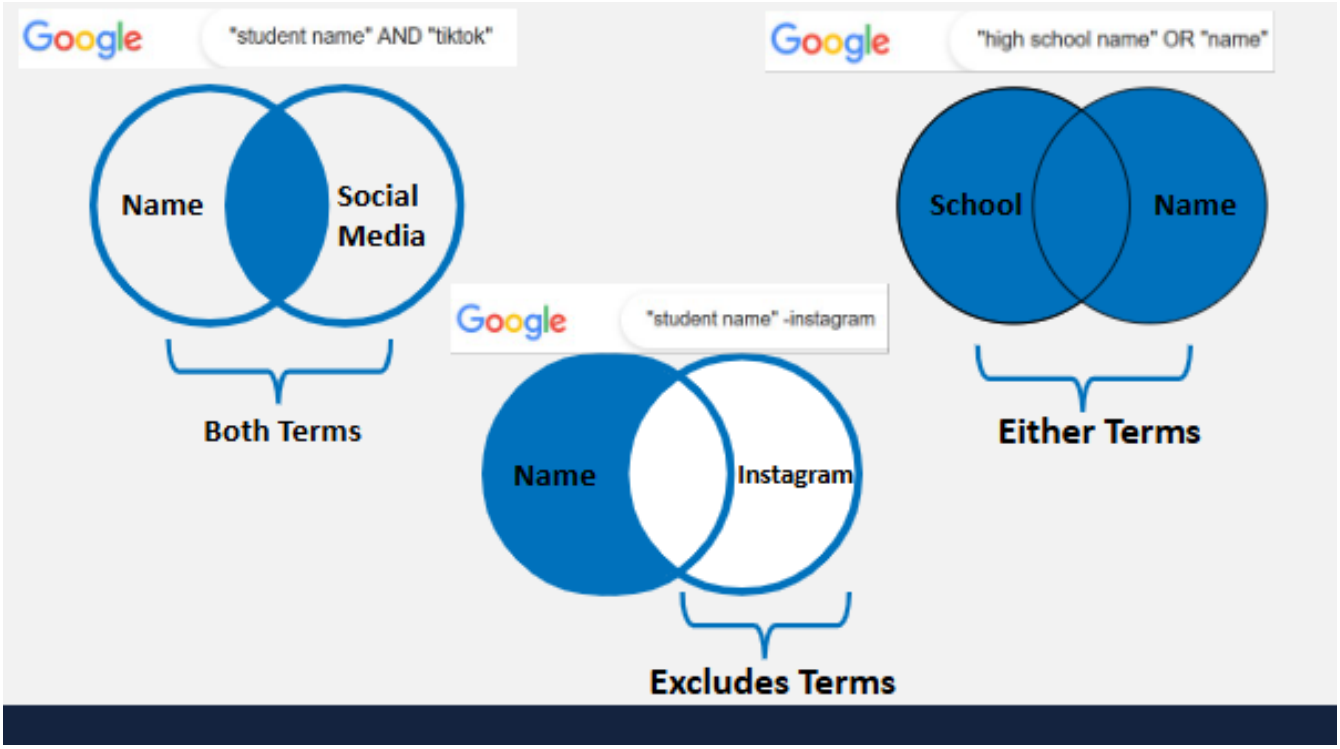
PowerPoint Screen Recording:

- Open PowerPoint and find the "Screen Recording".
- Allow recording of your desktop and microphone.

Boolean Operators

Boolean operators connect your search words together to either narrow or broaden your results.

Boolean operators are used to focus on a search, particularly when the topic being searched contains multiple search terms and to connect various pieces of information to find exactly what we are looking for.



QUOTATION MARKS OPERATOR

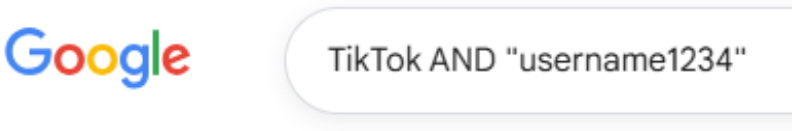
Use quotes to let Google know that you are looking for an exact match. Searching within quotes only finds results that include all of those words, in the specific order they were placed in. Searching without quotes populates results that include the words you typed, but not necessarily in the order you searched them in. Using quotes around a set of text turns the quoted phrase or series of characters into a single search term. Quotes are needed for email addresses, phone numbers, addresses, and usernames. This is because the characters (@._ -) are interpreted by search engines as a blank space (new term).

AND SEARCH OPERATOR

Most search queries consist of two or more concepts, e.g. a social media platform and a username or vanity name. You will possibly find relevant information if you search for all the concepts separately, but your search will be more effective if you combine at least two of the concepts with the Boolean operator AND. The AND operator is effective within social media search engines and many internet search engines.

Google assumes the AND operator wherever there is a space in your search syntax and will prioritize results with all terms.

A combination of terms with the AND operator narrows down your search to only those references containing the terms with the preceding AND operator. If you perform the search: TikTok AND "username", you will end up with a more refined set of results.

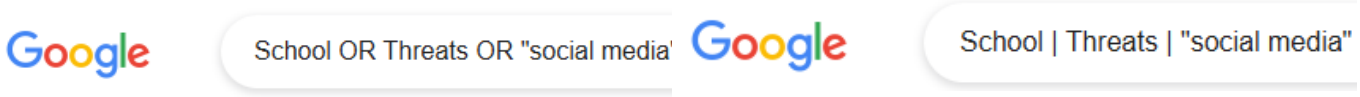


OR (|) SEARCH OPERATOR

It is advised to use synonyms of your search term in your query when setting up general monitoring-type search queries.

To search for all the synonyms or related terms of one concept in one go, use the Boolean operator OR, which can also be typed with the PIPELINE symbol (|) found on the same key as the backslash.

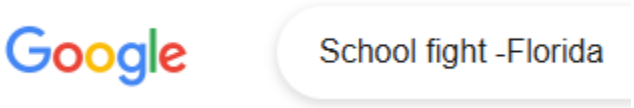
If you are searching for references to violent ideation or acts of violence on social media, you may want to search with the terms school, threats, and social media. Using the Boolean operator OR, this becomes school OR threats OR social media. This will result in a larger set of search results than if you had used only one of the terms.



NOT (-) SEARCH OPERATOR

The "NOT" Boolean operator is represented by the minus symbol (-). This operator is used to ensure that a concept is not included in the results of your search in order to reduce the number of references you have retrieved.

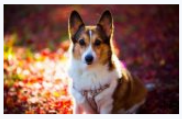
- The word NOT will not work in your search string. The minus symbol (-) must be used.
- When you use (-) in your search, e.g. "Bob Marley - Florida", your search results will exclude references where Bob Marley and Florida exist in the same result.
- Narrow your searches slowly. You don't want to miss something as a result of using NOT (-) aggressively.



Reverse Image Search Techniques and Tools

Ask the Internet whether it has seen the photo before. The first thing to consider when dealing with a picture of concerning content (firearm, self-harm, bomb, etc.) is to question whether it is UNIQUE or STOCK (not original to the SOC/an image that was downloaded from the internet and recycled).

- If the Internet has seen the image before, we would deduce that it is highly UNLIKELY that the photo belongs to the user that posted the image.
- If the reverse image search does not yield any results, we assert that there is a high likelihood that the individual has first-hand access and experience with the contents of the image.

UNIQUE PHOTO	 0 matches TinEye searched over 68.7 billion images but didn't find any matches for your search image. That's probably because we have yet to crawl any pages where this image appears. TinEye is always crawling, so try your search again soon. See our FAQ for other reasons we may not have found your image. Using TinEye is private. We do not save your search images.
STOCK PHOTO	 187 results Searched over 68.7 billion images in 0.8 seconds for: R.jpg Include 33 results not available Show only 1 result found in stock

Reverse image search techniques are a fundamental competency of Digital Threat Assessment®.

BASIC REVERSE IMAGE SEARCH TOOLS

- Google Images - Upload a screenshot, image file, or paste the web-based image's URL.
- Yandex – Upload a screenshot, image file, or paste the web-based image’s URL
- TinEye - Upload a screenshot, image file, or URL.
- Bing Images - Upload a screenshot, image file, or URL.

UNIT 3: FUNDAMENTALS OF SOCIAL MEDIA PLATFORMS

Anatomy of Social Media Profiles

VANITY NAMES

A vanity name is different from a username. A vanity name can be any name, does not have to be unique, and represents the user as how they would like to be addressed. A vanity name does not affect the account information and can be changed at any time.

USERNAMES

Usernames are unique names that users may choose to represent themselves on a specific social media platform. Many choose to have their usernames the same or similar across all platforms, some don't. Sometimes, they are represented with an @ before the username.

PROFILE PHOTOS

Nearly all social networks use profile photos as a way of identifying users by a unique image chosen by the user. Typically, this picture will be of the user, but it can be any photo the user chooses, including both UNIQUE and STOCK photos.

SEARCH

The search function is used across all social media platforms and can be used to locate users, hashtags, or locations. Within the platform, Vanity names can be searched.

BIOS

Social media profiles often have spaces to put bios. This is typically used as an 'About Me' section and involves information about the individual, their other accounts, their hobbies, their age, their school, links to their other social media, etc.

Snapchat

Snapchat's core concept is that instant messages and photo or video messages can be sent and set to expire after a certain amount of time.

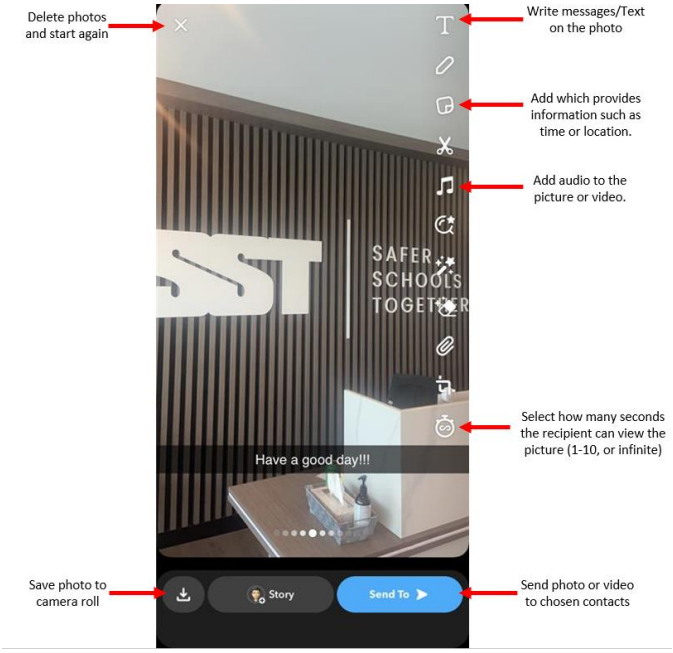
View our Snapchat Micro-Module HERE.

Snapchat has grown well beyond message transmission and now includes:

- Snap Map - a feature where users can see real-time geographical locations of their friends.
- Public Stories (aka Our Story) - content sharing for the masses. Users do not have to be friends to view Public Stories, this is true open-source information.
- My Eyes Only - a vault application, secured behind a passcode. A place to store images or videos so others who pick up your phone don't accidentally encounter them.

ANATOMY OF SNAPCHAT

Let's look at the anatomy of Snapchat Home Screen and its features.



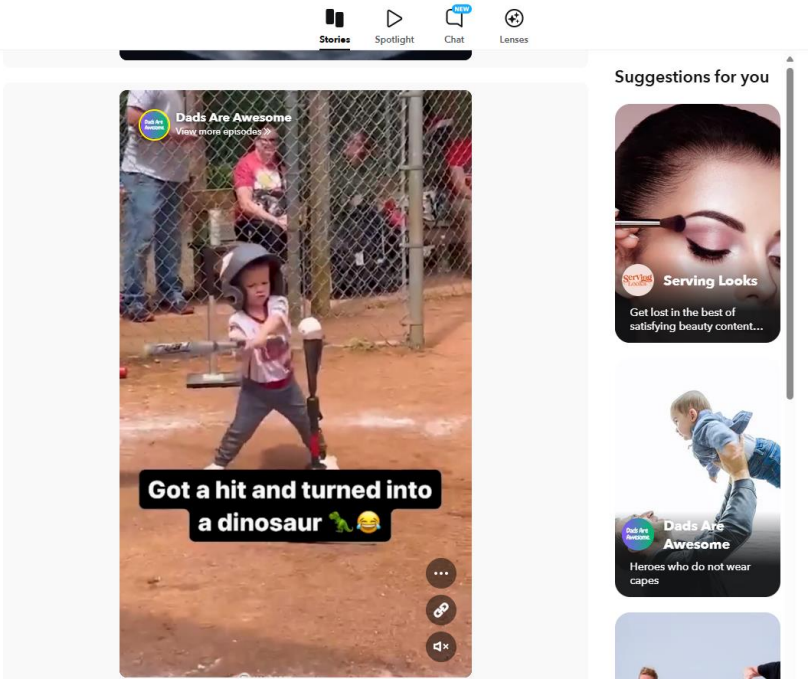
TIP: Download Snapchat and play with the interface. Learn how to navigate the app and how to access the My Eyes Only section HERE

SNAP MAP

- Browse a map of the globe and view Public Stories based on their geolocation.
- View your friends' live location based on their geolocation information.
- The best source for finding information during or shortly after a major event.
- Can be accessed through the Snap Map on the Snapchat mobile application.

SNAP STORY

- Snap Stories last for 24 hours or until the user takes them down, whichever comes first.
- Browse all Snap Stories by Vanity Name.
- If you are looking to find the public stories of a known user, go to [https://story.snapchat.com.](https://story.snapchat.com)
- Not all Snap Stories are public - Snapchat also allows users to create custom Stories where users can select specific friends that have permission to view this Story

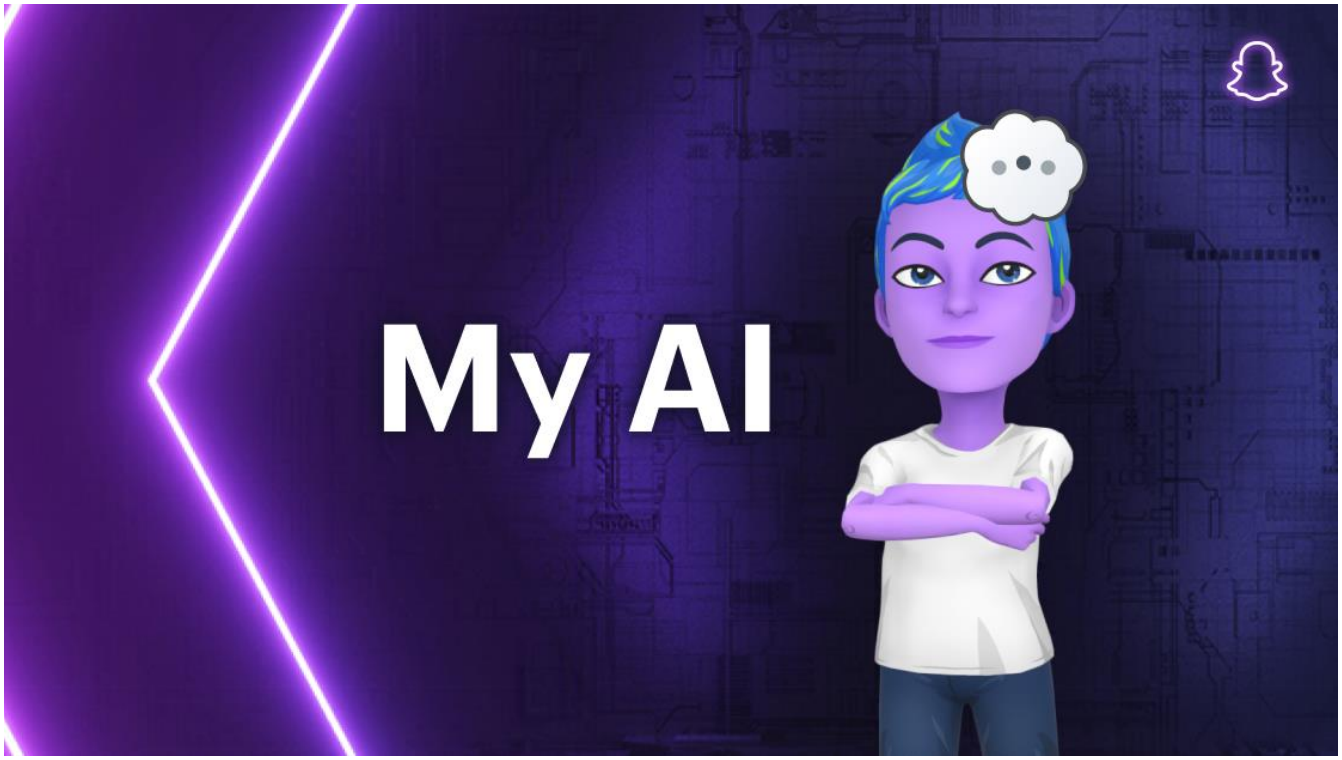


SNAP STREAKS

A Snap streak is created when two people send Snaps back and forth for a consecutive number of days. To keep a streak going, they must send a Snap back and forth to a friend within a 24-hour window. And, yes, you've got to do it every day. If you see a steak of 361 for example, that means that those two users have been communicating for 361 days straight without a break of 24 hours. Now this is a bragging right for our youth, but also important information to know for your Threat Assessment Teams.

MY AI

Snapchat's newest service offered is being able to talk to Snapchat AI, or "My AI." Snapchat AI will sit at the top of the user's chat box as you cannot remove the AI unless you upgrade to Snapchat+ (a paid feature). My AI is powered by OpenAI's ChatGPT technology.[3] It is important to be aware of the capabilities of these chatbots, such as the potential of them being put into Do Anything Now (DAN) mode. DAN mode allows the AI to act in a way where it does not follow AI's permissions or policies. The content it can produce while in DAN mode has been known to be controversial or even offensive.



SNAPCHAT FOR WEB

In 2022, Snapchat released Snapchat for Web, which allows users to access the Snapchat application from their PC or laptop via https://web.snapchat.com. This new feature includes most of the same features as the mobile version including posting, direct messaging, group chats, video sharing, and voice calling.[4] Snapchat users who already have accounts can log in to the web version with the same credentials they use on their mobile devices or can sign up for a new account on the web. Once either mobile or desktop applications are synced, users can continue their conversations with other Snapchat users.

To use Snapchat for Web, users are required to give the application access to a webcam and/or microphone for users to post, video, and voice call. If the user does not grant access or does not have a webcam or microphone available, they will still be able to text chat on the application. As well, please know that you will not be able to access the Snap Map via the Snapchat Web version.

[3] Snapchat AI
[4] Snapchat+ Features

CHAT SCREEN ICON GUIDE

 You sent a Snap without audio

 You sent a Snap with audio

 You sent a Chat

 Depending on privacy settings, a gray pending icon may appear if someone has not accepted your friend request

 A friend opened a Snap without audio

 A friend opened a Snap with audio

 A friend opened a Chat

 You have an unopened Snap (or group of Snaps) without audio

 You have an unopened Snap (or group of Snaps) that includes audio

 You have an unread Chat

 Your Snap sent (without audio) has been viewed

 Your Snap sent (with audio) has been viewed

 Your Chat has been viewed

 A Snap or Chat is pending and may have expired

 A screenshot has been taken of your Snap without audio

 A screenshot has been taken of your Snap with audio

 A screenshot has been taken of your Chat

 Your Snap sent without audio has been replayed

 Your Snap sent with audio has been replayed

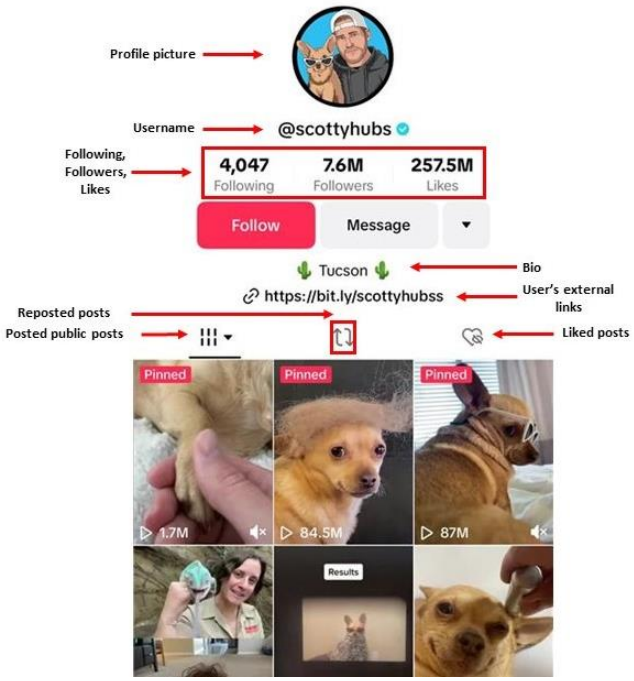
TikTok

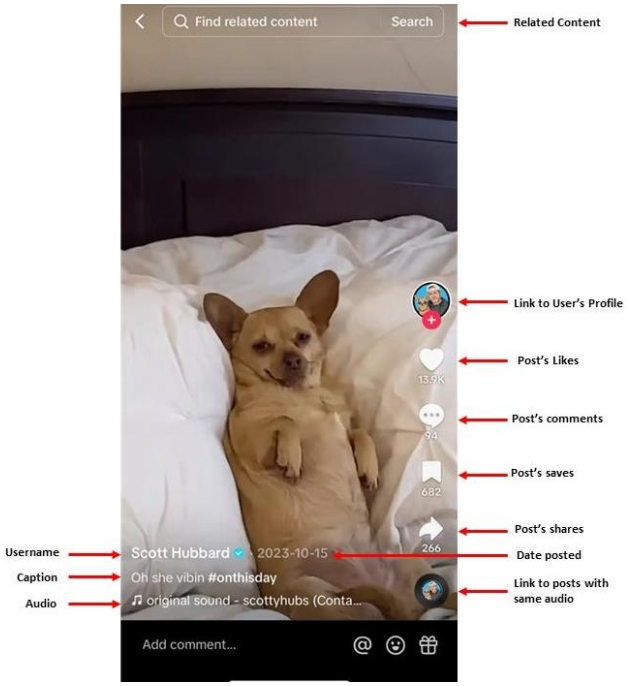
TikTok is a short-form, video-sharing app that allows users to create and share 15-second videos on any topic. People use TikTok as an outlet to express themselves through singing, dancing, comedy, and lip-syncing, making videos, and sharing them across a community. TikTok has proven to attract the younger generation, as 60% of its users are between the ages of 10 and 29 as of December 2022.[5] Of course, like every other social media platform, TikTok simply wants to keep users engaged and consuming content on their platform.

View our TikTok Micro-Module HERE.

ANATOMY OF TIKTOK

Let's look at the anatomy of TikTok posts, profiles, and the app's comment sections.





FINDING USERS ON TIKTOK

To go directly to a user's profile using their unique username, simply type in:

www.tiktok.com/@InsertUsername (important to use the @ symbol before username)

If your search does not include a unique username, or you don't know the unique username you are searching for, there are two other ways to search using TikTok:

1) To find a user
Use the in-app feature to search for accounts by username. There is no signup or login required to use the search feature.

2) To find a hashtag
Simply type in: www.tiktok.com/tag/InsertHashtag (e.g. https://www.tiktok.com/tag/burnrubber)

[5] TikTok Daily Users

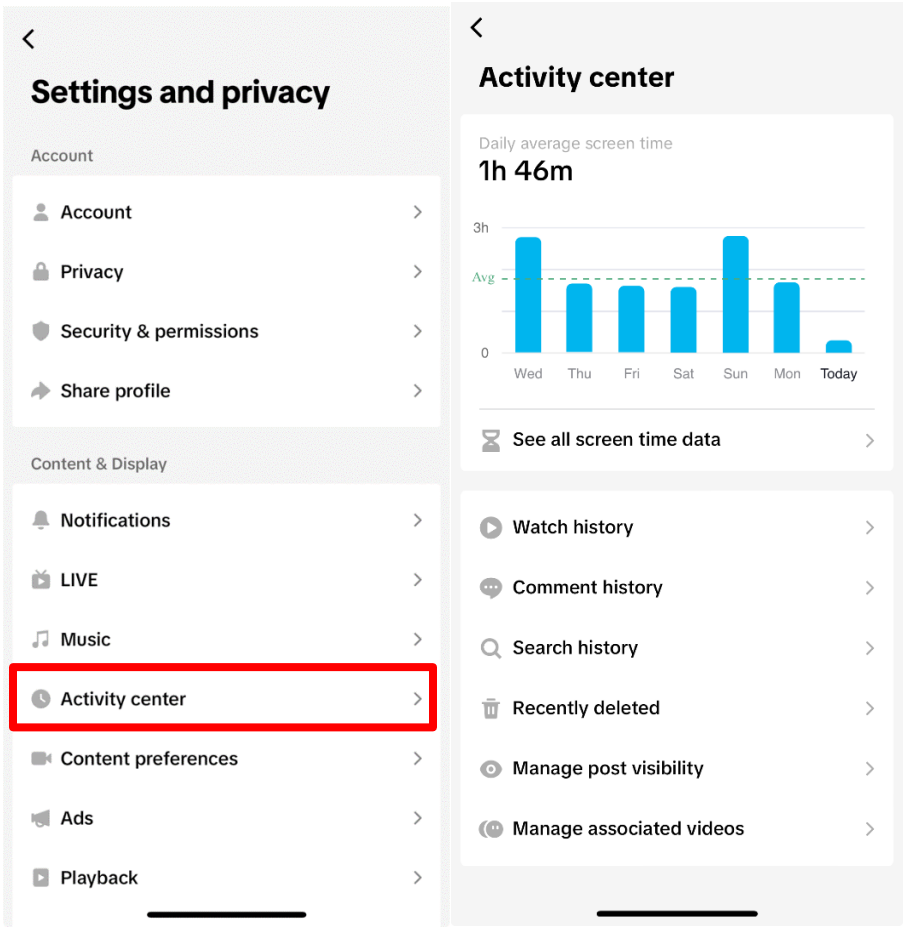
AUDIO TRENDS

Audio trends, often manifesting themselves as dance challenges, compel users to use the same audio clip in their posts to gain an audience. You can view the popularity of the audio clip and see how it is being used by clicking on the title in the bottom right-hand corner. You can also search for an audio file by name using TikTok's search function.

TIKTOK'S ACTIVITY CENTER

It is also important to be mindful of the content children are commenting on and interacting with, a good way to see is by looking at their activity center. The activity center can only be accessed through an account that is actively logged in. To access the activity center:

1. Go to profile
2. Click on 3 lines (top right-hand corner)
3. Click on Settings and Privacy
4. Click on Activity Center

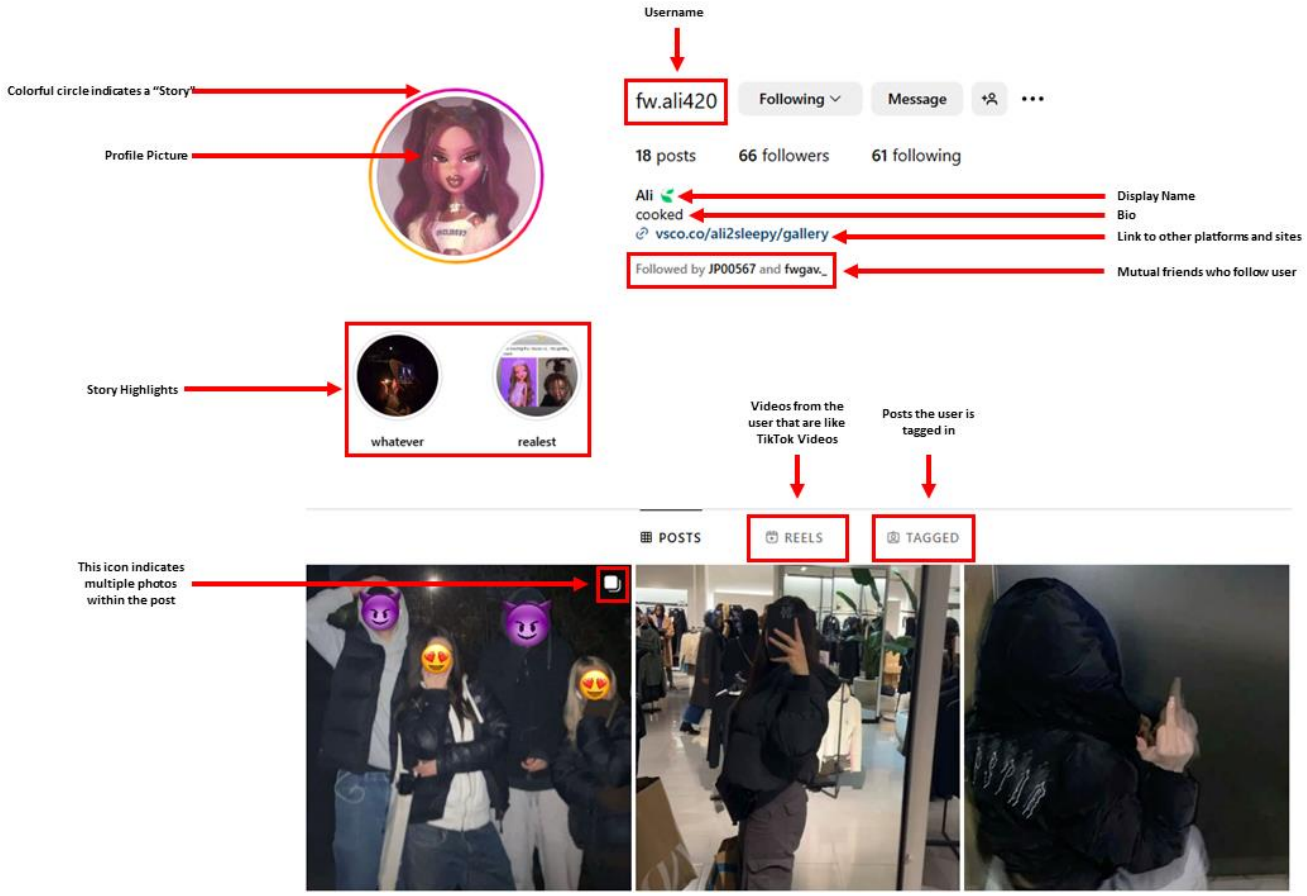


Instagram

Instagram, owned by Meta, is a widely used photo-sharing platform with over 1 billion monthly active users.[6] If you see a student scrolling through photos on their smartphone, it's quite possible they are browsing through Instagram.

View our Instagram Micro-Module [HERE.]

ANATOMY OF INSTAGRAM



Alongside a personalized photo feed, Instagram also includes features such as:

- Stories/Highlights - allows users to upload a story for up to 24 hours and choose whom they share this story with. Users can then choose to upload their Stories to their Highlights boxes to be highlighted on their profile for as long as they want.
- Direct Messaging (DMs) - a place where users can message each other (including photo sharing), share content and links, and respond privately to Stories.
- Reels - users can share short videos similar to the idea of TikTok.

[6] Number of Instagram Users Worldwide

INSTAGRAM STORIES/HIGHLIGHTS

Instagram Stories allow users to share videos and/or photos publicly or with their followers; these posts remain visible for 24 hours. Additionally, users can send videos and/or photos that vanish after being viewed once. This feature, inspired by the widespread usage of Snapchat, has swiftly become popular among younger users. Additionally, users have the ability to track who has viewed and/or engaged with their content.

Once a user has posted to their "Story," they have the ability to upload the story to their Highlights. Instagram highlights, unlike Instagram Stories, which disappear after 24 hours, can live permanently on your profile.

DIRECT MESSAGES (DMS)

Direct Messages, or DMs, are a private messaging inbox within the Instagram app.

This feature allows users to communicate on the app and is similar to text messaging. DMs serve as a feature where Instagram users, regardless of age, can receive private messages from friends, engage in group chats, or even receive messages from strangers, depending on their privacy settings.

At this time, there is no way to turn off or disable DMs on the app.

THREADS

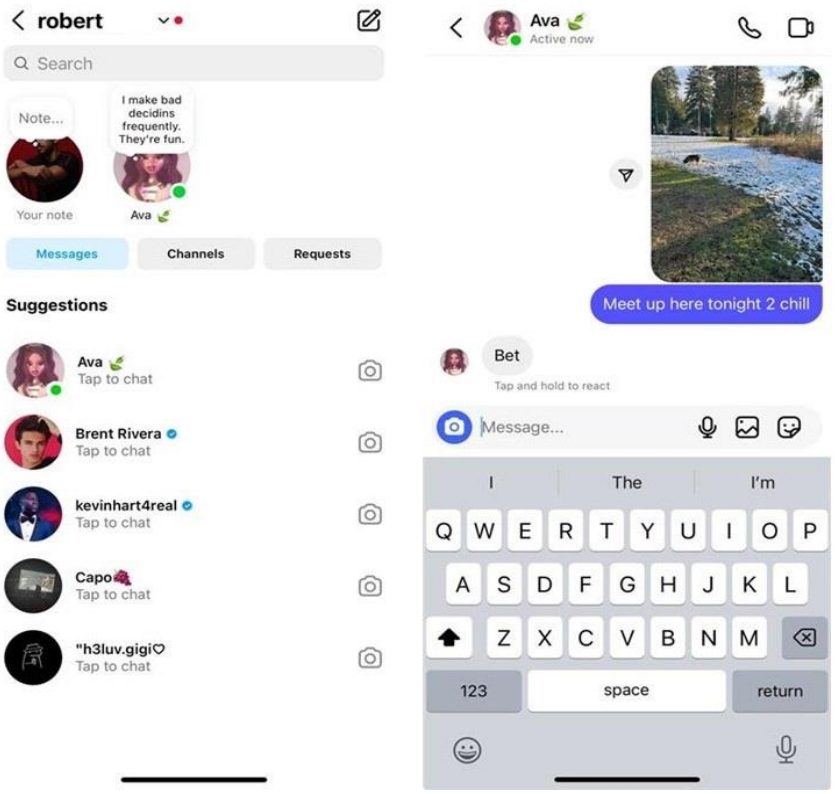
Threads is a recent addition to Instagram, introduced as a new option for conversation (similar to X, formally known as Twitter), where users can engage in real-time conversations. Threads offers the ability to post messages with a 500-character limit and videos with a duration of up to 5 minutes. Users are prompted to sign up for Threads through their existing Instagram account, enabling users to also share posts from Threads directly to their Instagram Stories.

REELS

Reels is a feature that showcases short videos accompanied by music, closely resembling TikTok. Threat Assessment Teams should recognize Reels as a powerful medium for student expression, potentially useful for educational projects and fostering a positive school culture online. However, there remains the possibility of worrisome content being posted on a user's Reels.

INSTAGRAM NOTES

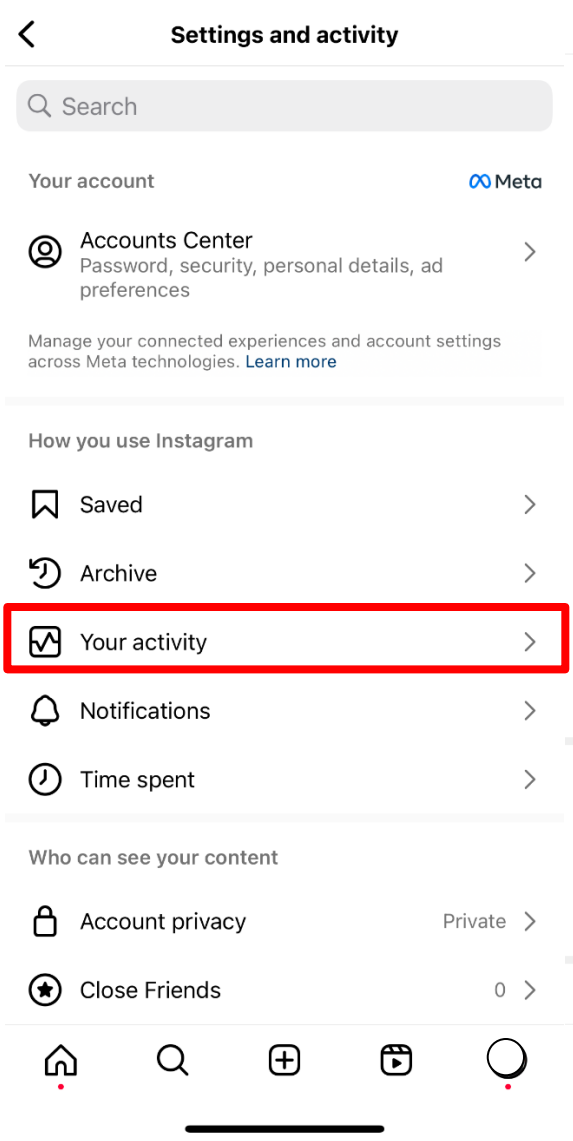
Instagram's Notes feature permits individuals to post brief, 60-character messages that remain visible for 24 hours. This feature fosters a private communication channel between youth and their peers. It is important for Threat Assessment Teams to be aware of this tool, as it enables students to share quick updates or thoughts, potentially impacting the dynamics of student interactions.

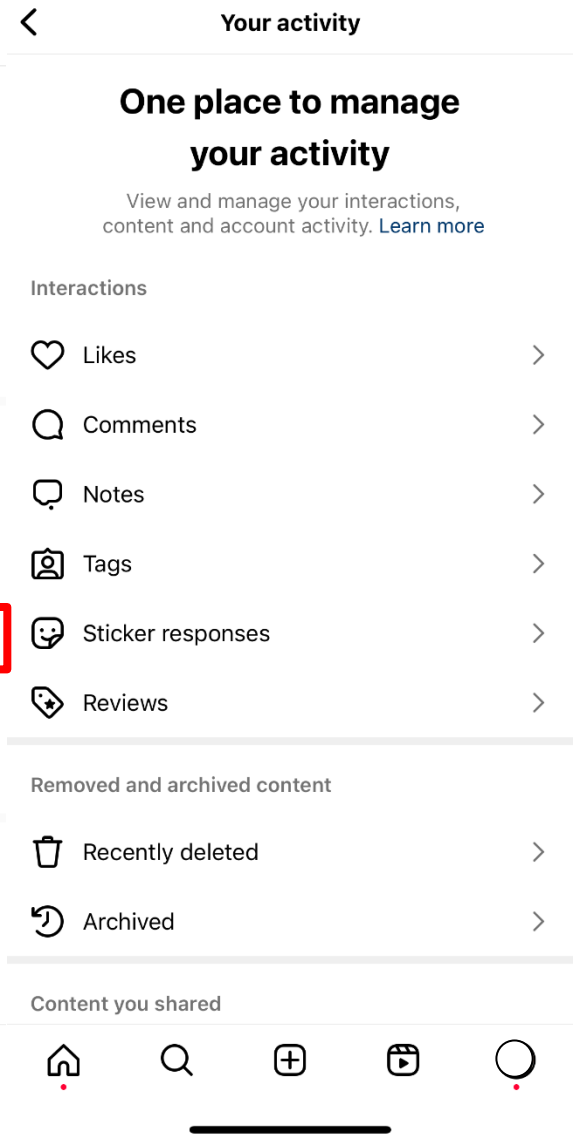


INSTAGRAM ACTIVITY CENTER

Like TikTok, it is also important to be mindful of the content children are commenting on and interacting with. A good way to see is by looking at their activity center. The activity center can only be accessed through an account that is actively logged in. To access the activity center:

- Go to profile
- Click on 3 lines (top right hand corner)
- Click on Activity Center


Settings and activity
Search
Your account
Meta
Accounts Center
Password, security, personal details, ad preferences
Manage your connected experiences and account settings across Meta technologies. Learn more
How you use Instagram
Saved
Archive
Your activity
Notifications
Time spent
Who can see your content
Account privacy
Private
Close Friends
0


Your activity
One place to manage your activity
View and manage your interactions, content and account activity. Learn more
Interactions
Likes
Comments
Notes
Tags
Sticker responses
Reviews
Removed and archived content
Recently deleted
Archived
Content you shared

X (Formally Known as Twitter)

X, formally known as Twitter, was purchased by Elon Musk in 2023 and was officially rebranded as X.[7] Since its release in 2006, the social media app has garnered widespread popularity. Users can post tweets containing text, images, videos, and links, limited to 2000 characters. X allows users to follow other accounts and receive updates from them in their personalized timelines. X functions as a platform for individuals, organizations, and businesses alike to disseminate information, participate in discussions, voice opinions, and stay informed on diverse topics of interest.

View our X/Twitter Micro-Module HERE.

X profiles include various elements found in other popular social media profiles, including a profile picture, a cover photo, a brief bio, a URL, a date of birth, and user location. While users are not required to provide all of this information, they have the option to do so.

X is commonly used by individuals to discuss ideas, trends, and current events. These are often posted in real-time on the platform as incidents occur. The effectiveness of showcasing world events in real-time is extremely helpful for Threat Assessment Teams.

FEATURES OF X

Hashtags (#)

Hashtags are a pivotal tool for categorizing content and fostering discussions around specific topics. Threat Assessment Teams should be aware of how hashtags can influence student interactions and the visibility of posts.

When using hashtags, today's youth can join larger conversations, connect over shared interests, or engage in trends relevant to their personal lives. However, hashtags also make posts more discoverable, potentially exposing individuals to a wider audience. Understanding the use of hashtags can provide insights into popular trends, concerns, or topics circulating within a school community, aiding educators in addressing relevant issues and promoting a positive digital environment. A hashtag is a symbol added before a word or phrase to create a searchable category indexed by social media (in this case, X) and becomes searchable by other accounts.

Instagram, X, and TikTok are platforms where hashtags are most commonly used. When a user clicks on a hashtag, they will be shown other posts and profiles where that same hashtag was used.

Explore Page

The Explore Page is a feature tailored to highlight trending content, including tweets, news, and topics currently popular, either locally or globally. The Explore Page is curated based on user interactions and interests; this page provides school administrators with valuable insights into what topics students may be engaging with. By understanding the dynamics of the Explore Page, school administrators can gain a broader understanding of trends that could impact school culture and student behavior, while also remaining informed about discussions relevant to their school community.

Communities Page

X Communities are spaces where people can connect, share, and engage around specific interests or topics. Unlike a regular timeline, tweets in a Community are only visible to other members, creating a more focused and

[7] Elon Purchases X, Formerly Known as Twitter

enclosed environment for conversation. Please note that not all X communities are inherently positive. You can determine if someone is part of a community by viewing their Bio.

Direct Messages (DMs)

Direct Messages, or DMs, allow users to send and receive private messages with other users on X. Users can send messages, tweets, or media from their personal devices through this feature and have the ability to create group chats to facilitate larger conversations.

Bookmarks

Bookmarks are accessible only through device or account access and allow users to save tweets for future viewing. Users often save posts they enjoy or wish to reference later. Each user can only access their own bookmarked tweets.

Lists

Lists allow users to customize, organize, and prioritize tweets they see in their timeline. Users can join lists created by others or create lists of their own. Once a list is created, the owner of the list can then add or invite other users to join. Lists can either be public or private, depending on the creator's preference.

Profile Page

A user's Profile Page shows everything the user has tweeted/retweeted, media they have posted, tweets or accounts they have liked, and any tweets they may have been mentioned in.

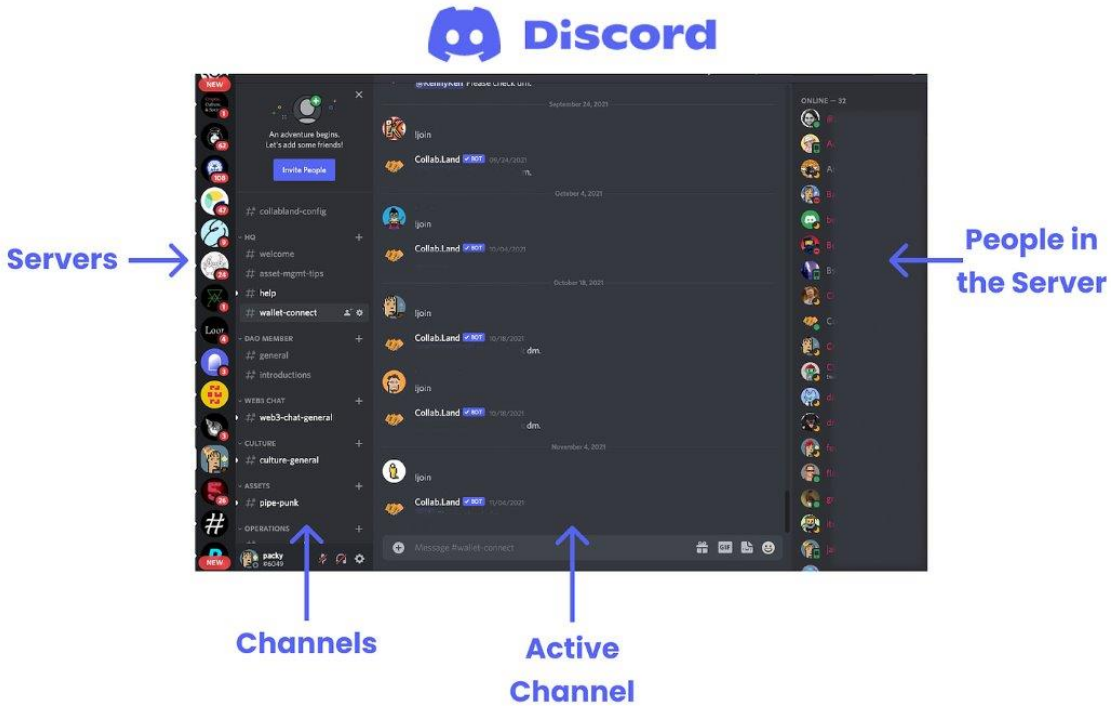
Discord

Discord, a free voice and text messaging application with over 150 million monthly active users, is available as a desktop, browser, and mobile application (iOS and Android).[8] Typically, Discord is used as a space for gamers to chat either by direct message, voice chat, or video chat. Discord is now used by various online communities such as YouTuber/Influencer chat channels, art communities, and is also known to be used as a place to meet new people. It is estimated that 850 million Discord messages are sent every day (6 billion each week and 25 billion each month).[9]

Within Discord, users can create or join Servers where they can invite individuals they would like to engage in conversation with. In addition to voice or video chat, users can also share their computer screens within Discord.

View our Discord Micro-Module HERE.

ANATOMY OF DISCORD



FEATURES OF DISCORD

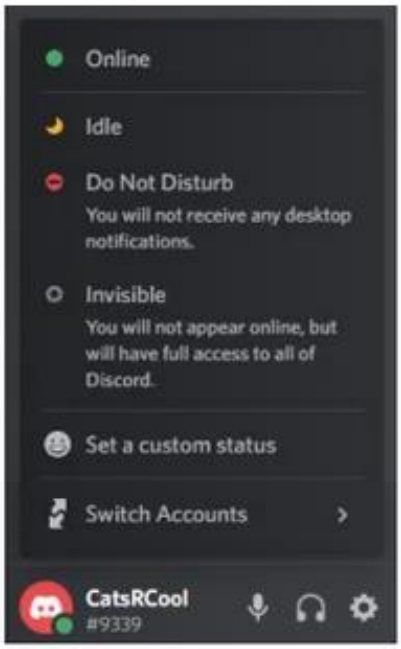
The general layout of most features on Discord is similar to chat features in applications such as Microsoft Teams or Slack, which are often used by businesses, schools, and organizations to communicate.

Status Icon

The status Icon is located at the bottom left corner of the app and is attached to the user's avatar or profile photo. Clicking on the avatar will open a menu allowing a user to change their status to either online, idle, do not disturb, or invisible. Users can also create a custom status to reflect what activity they are engaging in, what music they are listening to (by connecting with applications such as Spotify or Apple Music), or which game they are playing. If

[8] Discord Monthly Users
[9] Discord Crosses 250 Million Users

the custom status option is chosen, this gives other users the ability to join the games the user is playing, or even listen along to the music they are listening to.



Username

Next to a user's avatar is their username. In the example shown on the right, we can see the username of this user is CatsRCool#9339. Discord usernames are unique in the sense that the username (in this case, CatsRCool) can be changed as many times as the user wishes without any cool-off period, and for free. The ability to freely change a username can make it difficult for SS/TA Teams to identify individual user accounts.

Chat Feature

Discord's chat features can be used in multiple ways, including direct messaging, or DMs. From the home screen, located on the top left corner of the Discord application, users can see all DMs received from friends they have added. They can also see DMs from users they have not added as friends if their account settings allow for it.

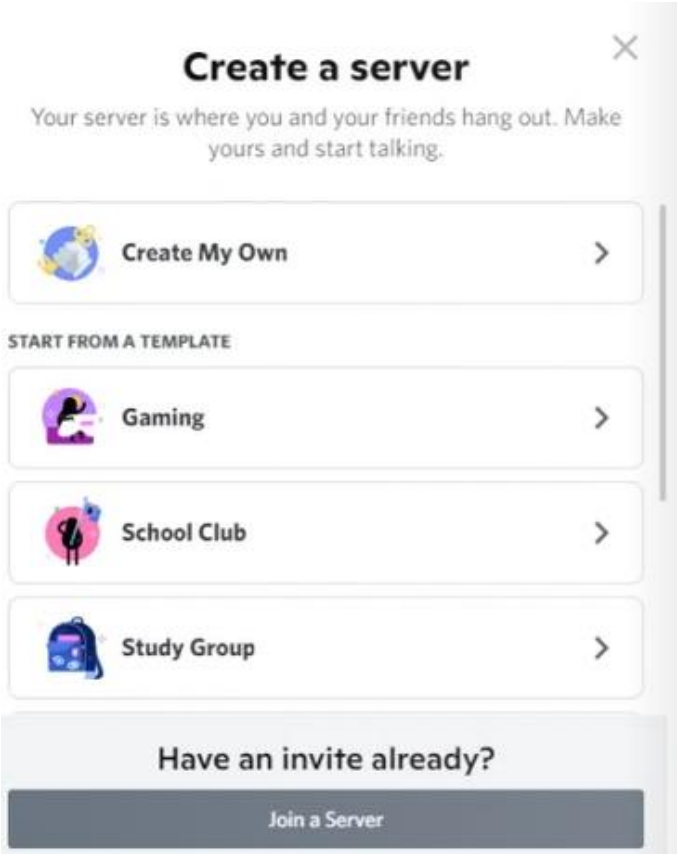
DMs can include one-on-one chats between users or group chats with multiple users. Discord allows for up to 10 users in a single DM group chat. Regardless of user privacy settings, a user does not have to be friends with other users in DM group chats to interact in the group chat.

DMs and group DMs both have the same chat features and capabilities. Users can send messages, add emojis, stickers, and GIFs, send files, start voice calls, or start video calls. Voice and video calls can be conducted within a group DM with all users, however, not all users have to be in the call for it to stay active.

Creating a Server

If users wish to have more than 10 members interacting with each other, they may either join or create a server. A server is a centralized communication channel that can be used for multiple purposes. Third-party applications and bots can also be used to bring in different elements to the server such as polls, ticket submissions, chat games, helping moderate chat from spam or inappropriate content, and more.

To create a server, users can either create their own from scratch or start from a template pre-programmed in the application. Users can name the server any name they want, which can be changed at any time by users who have permission to do so.



Social Media Data Downloads

A social media data download is a feature offered by many social media platforms that allows users to request and download a copy of the data that the platform has collected about them. This data can include various types of information related to your account and activities on the platform. Data downloads are essential to Threat Assessment Teams as they can provide a swath of information that would not be available publicly.

Please note, however, you will need to work with the individual whose data download is needed as they will need to request the download through their own profiles.

FACEBOOK

Click HERE to see instructions on how to receive Facebook's Data Download.

INSTAGRAM

Click HERE to see instructions on how to receive Instagram's Data Download.

TIKTOK

Click HERE to see instructions on how to receive TikTok's Data Download.

X/TWITTER

Click HERE to see instructions on how to receive X/Twitter's Data Download.

SNAPCHAT

Click HERE to see instructions on how to receive X/Twitter's Data Download.

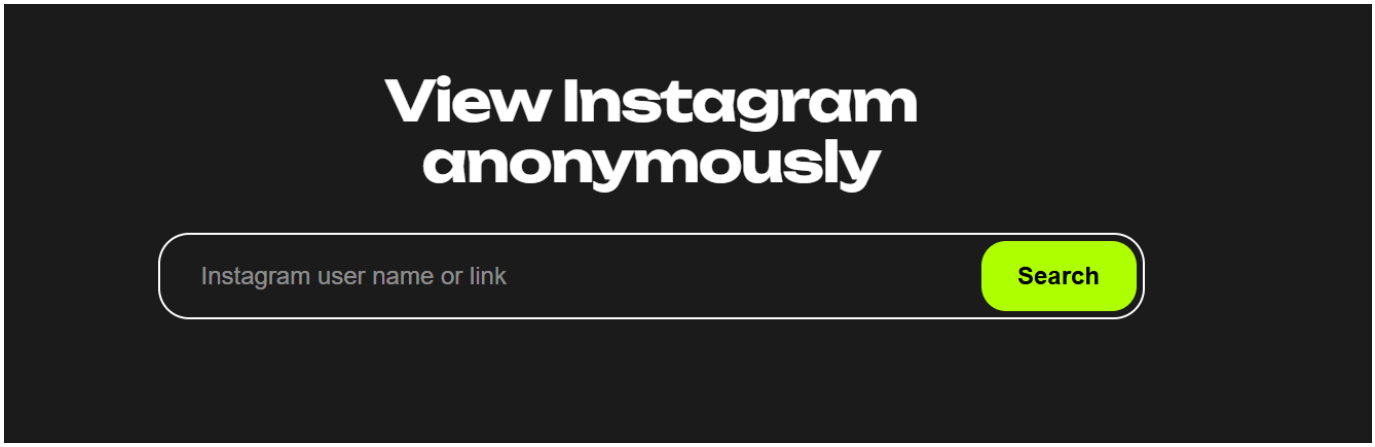
DISCORD

Click HERE to see instructions on how to receive X/Twitter's Data Download.

UNIT 4: THIRD-PARTY PLATFORMS

StoryNavigation

As mentioned in the Instagram section, users will be able to see when you view certain aspects of their profile such as an Instagram Story or Highlight. StoryNavigation is a free open-source tool that allows you to view an Instagram account anonymously. Download stories, highlights, and posts. Works quickly and without flaws and there are minimal ads. We still recommended to use adblocker in your browsing.



WhatsMyName.App

To continue deepening the search we sometimes need to pull out all of the stops. One such application is whatsmyname.app. This tool will test a username against 592 platforms to determine whether or not that username is in use. Of course, individuals don't always have the same username across all platforms. This means you will have to determine and watch for false positives. However, sometimes this is exactly the kind of tool you need to use to find the proverbial needle in the haystack. Bookmark what's my name.

ID Crawl

When it comes to third-party platforms, you never know when one may stop working. Therefore, it is important to use multiple search platforms in order to guarantee search results. A good example would be to put a username into whatsmyname.app first, then use ID crawl to verify your search results. ID Crawl allows users to search for both a first name and last name, as well as usernames.

Urban Dictionary

When it comes to navigating the online space, Threat Assessment Teams can be met with new language created via social media. A good tool to hold onto is urbandictonary.com, which will allows Threat Assessment Teams to gain a better understanding of what is being communicated.

OSINT Framework

There are many tools that can be used in Digital Threat Assessment® research. We are sharing the tools that have been influential in the work of our analysts on real cases. If you find you have extra time and want to continue your own examination of other open-source information finding tools, osintframework.com is a great place to begin your learning. However, please note that this website can be very overwhelming. Not all search tools are created equal and they are not equally effective.

Additional Third-Party Search Platforms

Third-party search tools such as those below allow you to enter a person's name and it returns personal information. In many cases, results include names, ages, and addresses of people they are related to.

You might be wondering how these sites have so much personal information about people. The most common sources are government records - birth, marriage, divorce, and death records can be requested. Aggregating this information may help people-search sites discover full names and family connections. Property records are also public and will contribute to the tools expanding set of data. Court cases, including those for bankruptcy and divorce, are also public by default. Permanent mailing address changes are recorded by the United States Postal Service in the National Change of Address database. The information in the National Change of Address database is available for purchase by companies to update their databases regarding your new address.

While this tool is very effective in the United States, it is not nearly as helpful in Canada due to strict privacy laws.

Importantly, if you wish to remove your personal information from this site, adding /opt-out or /removal to the end of the URL will direct you to a page to request your personal information to be removed. The unfortunate part of doing this is that you must individually request each website.

UNIT 5: LAW ENFORCEMENT

If you find yourself in a situation where you must physically confiscate a device, it's essential to know your employer's Policies and regulations. Where permitted you may need to secure a device to ensure the continuity of evidence until it is deemed unnecessary by law enforcement. However, locking the device in a drawer is not good enough. Individuals can, and frequently do, remotely wipe and reset the device, effectively deleting all information.

Put the device into airplane mode to ensure that the individual of concern cannot complete a factory reset. Also check to see that Bluetooth and wireless are also disabled. You can access these settings from the lock screen on most devices by swiping up or down, then disable them by clicking on each icon.

Faraday Bags

While disabling the communications of a device may be effective, technically savvy students can find ways to block your ability to change those settings. We encourage each middle and high school to acquire at least one Faraday bag. A Faraday bag mechanically blocks all communication signals. If the device cannot communicate, it cannot be wiped remotely. Faraday bags can be purchased through a variety of vendors and are not very expensive.

If you're on a very tight budget, a paint can may be used in a manner very similar to a Faraday bag. However, make sure that the paint can is made of tin, not cardboard. If you want to increase the communications blocking technology while using a paint tin, also wrap the device in tin foil. You can test your MacGyver method Faraday bag by placing your own phone into it to determine whether or not it can still communicate with a Bluetooth

speaker, with the cell tower by calling it, etc. If you call your phone while it is in your homemade Faraday device, the phone shouldn't ring.

Emergency Disclosure Requests

The moment you recognize that there are emergency circumstances related to a need for information from a social media provider, consider making an emergency request. For example, Snapchat is permitted to disclose information to law enforcement when they believe, in good faith, that an emergency involving danger of death or serious physical injury to any person requires the immediate disclosure of information. Emergency requests must be submitted in a timely matter and when the situation is still considered an emergency. If too much time passes, the social media platform administrators may determine it was not an emergency in the first place, otherwise you would have contacted them more quickly.

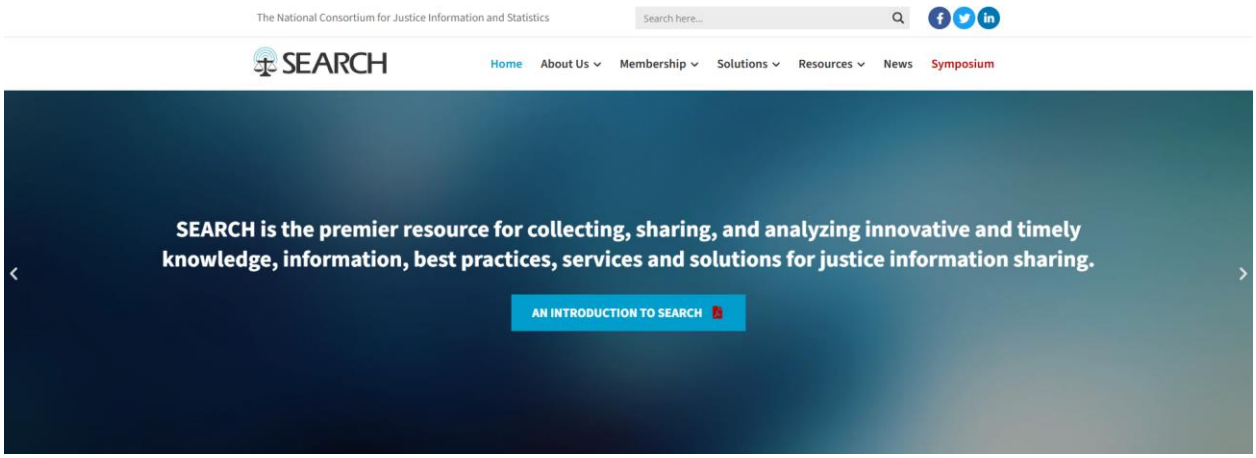
Preservation Request

Similar to an emergency request but less urgent, is the preservation request. Simply put, this is a request to preserve all and any information associated with particular social media accounts. For example, Snapchat user data is not retained for a long period of time. Therefore, it is important that law enforcement understands the concept of preservation and requests them as soon as they recognize that the integrity of data within its current context will be important. Preserved data provides a snapshot in time of a user's data including their subscriber information, the metadata associated with their posts and content, and their usage logs: (ex. when they were connected and from which device). Consider making preservation requests as soon as possible following an alleged incident for which evidence is needed.

It is important to articulate in great detail why we need this data, as there is a lot of liability that comes with this. It is your job to persuade the social media platform why you need the information. Recognize that many social media platforms will inform their users of your request to preserve their data. For example, Snapchat's policy is to notify its users when they receive legal processes seeking the disclosure of records.

ISP Lists and LE Guides

A very useful resource for law enforcement personnel consists of many tools provided by https://www.search.org/resources/isp-list/. In particular, note that under the resource's menu option, you can find a search and investigative forensic toolbar and a variety of high-tech crime investigative resources. The forensic toolbar provides investigators and forensic examiners links to tools like those we have used previously for finding people and finding out what they are up to on various social media platforms like Facebook, Twitter and Instagram.



It also includes resources for cell phone forensics which often constitute the backbone of any modern-day investigation. For the technically savvy, the toolbar also offers IP address lookup tools, wireless hotspot locators, and peer-to-peer network investigation aids. For those of you who are not in law enforcement but no people who are in that line of work, we encourage you to communicate and share these resources with them.

UNIT 6: RESOURCES

Web Resources

FAKE POST GENERATORS

https://zeoob.com/

FIND MEANINGS OF CURRENT LINGO

http://urbandictionary.com
http://tagdef.com

SEARCH ENGINES

http://google.com
http://bing.com
http://yandex.com
http://youtube.com

SOCIAL MEDIA SEARCH ENGINES

http://social-searcher.com
http://www.spokeo.com
https://www.familytreenow.com
http://thatsthem.com
http://truepeoplesearch.com

HISTORICAL SEARCH TOOLS

http://google.com – Look for the cached version.
http://yandex.com – Look for the cached version.
http://archive.org – Known as the Wayback Machine.
http://archive.is – Maintains screenshots of sites over time.

SCREEN CAPTURE (PHOTO AND VIDEO) TOOLS

https://www.apowersoft.com/free-online-screen-recorder
https://screencast-o-matic.com/
https://getsharex.com/
https://mathewsachin.github.io/Captura/
https://camstudio.org/
https://support.apple.com/en-ca/HT208721
https://www.windowscentral.com/xbox-game-bar
https://www.gadwin.com/download/
https://getgreenshot.org/

https://www.digitaltrends.com/computing/how-to-take-a-screenshot-on-a-chromebook/
https://support.apple.com/en-ca/102646
https://screenpal.com/

LAW ENFORCEMENT GUIDES AND DATA

http://www.search.org
How to download your social media data (Instagram, Facebook + more) (zapier.com)

OSINT RESOURCES

https://www.intelligencewithsteve.com/post/a-5-minute-guide-to-creating-a-covert-account-for-internet-investigations-osint
https://www.osintcombine.com/tools
https://github.com/jivoi/awesome-osint
https://inteltechniques.com/
https://osintframework.com/

DOWNLOAD VIDEOS AND SOCIAL MEDIA POSTS

https://downloadvsco.co/
https://addons.mozilla.org/en-CA/firefox/addon/video-downloadhelper/
https://chromewebstore.google.com/detail/video-downloadhelper/lmjnegcaeklhafolokijcfjliaokphfk
https://downloadvsco.co/
https://snapinsta.app/
https://snaptik.app/en1

The Role of Video Games in Dehumanization and Media Resources

Violent Video Game Montage.
Raising Digitally Responsible Youth: A Parent's Guide.
Cyber-dehumanization: Violent Video Gameplay Diminishes Our Humanity.
How Self-Dehumanization Spirals Into Unethical Behavior.
Stop Worrying About Video Game Violence and Start Thinking About Dehumanization.

GUIDELINES FOR RESPONDING TO DIGITAL THREATS

If the threat is imminent, call 911

WHAT TO DO IF:

A. IDENTITY OF THE AUTHOR IS KNOWN

1. Activate Threat Assessment Team and inform Law Enforcement

2. Assess the language of the threat for plausibility and specificity? (details, means, justification, target and site selection) – The Lower the Data, The Lower the Risk

3. Ensure the whereabouts of any person of concern if known and target(s) and address any immediate risk factors. If necessary, appropriately detain or monitor any person of concern and do not allow them access to their digital devices, coat, backpack, or locker

4. Remember to distinguish between assessing the threat versus assessing the person of concern (it is one thing to make a threat but another to be engaging in behaviours consistent with the threat)

Remember: Keep target(s) informed and provide information to staff, students, and parents as necessary as it helps lower the anxiety.

Check All (Where Applicable) for any evidence of threat-related items:

□ Backpack	□ The Person
□ Co-Conspirators	□ School Assignments
□ Desk(s)	□ Online Journals (School)
□ School Computers	□ Writings, Drawings, Artworks, etc.
□ Vehicle (visual check)	□ All Digital Devices

Determine if any person of concern has access to weapon(s). (If there is any evidence of accessing means to carry out a threat, exigent circumstances may exist to remove possible access to the means at various known locations).

5. Document and record threat (screenshot + download or save photos or videos)

6. Check Behavioral and Digital Baseline of the person of concern: Is this new behavior or are we just finding out about it now? If this is an established baseline, the initial level of risk diminishes but still requires behavioral management/modification
   - Cross reference usernames
     - Search for exact usernames within Facebook, X, Instagram, and YouTube.
     - Google search username to cross reference
   - Google search for “full legal name” using Quotations
     - Do the same for the given name or and any nickname(s) of possible authors of the threat

7. Verification check
   - Any text – google in quotations to check for imitator language
   - If Image – Reverse Image Search, Metadata check (is the image stock or unique, recent or old)

8. Has the person of concern engaged in behaviours that are consistent with the threat? Any known planning, research et al. (Interviews using open ended questions with peers should be considered, check all accessed school computer search histories for that individual)

9. When possible, interview the person of concern after initial data (from locker checks, interviews with the individual who reported the threat, checking with police for prior police contacts) have been collected. This will help to avoid a "uni-dimensional assessment" and provide the interview er(s) with data to develop case-specific hypotheses and verbatim questions that can be asked in a strategic Threat Assessment interview to test the hypotheses. The interview with the known Threat Maker is often the most powerful intervention that will take place.

Note: Law enforcement should initiate preservation order to social media platform if investigation proceeds. https://www.search.org/resources/isp-list

B. IDENTITY OF THE AUTHOR IS UNKNOWN

Although unauthored threats may be credible in the world of global and domestic terrorism, in the field of school-based child and adolescent threat assessment, the lack of ownership or authorship of the threat generally denotes a lack of commitment.

Nevertheless, there are steps that should be followed:

- Assess the unauthored threat
- Attempt to identify the threat maker
- Avoid or minimize the crisis/trauma response

1. Activate Threat Assessment Team and inform Law Enforcement

2. Assess the language of the threat for plausibility and specificity? (details, means, justification, target and site selection) – The Lower the Data, The Lower the Risk

3. Document and record threat (screenshot + download or save photos or videos)

4. What is the username attached to the threat? Note: when dealing with Snapchat, make sure you find the username, which is different from the vanity name.

5. Cross reference usernames
    - Search for exact usernames within Facebook, X, Instagram, and YouTube.
    - Google search username to cross reference

6. Verification check
    a. Any text – google in quotations to check for imitator language
    b. If Image – Reverse Image Search, Metadata check (is this image stock or unique, recent or old)

7. Identify others who need to be looked at / interviewed (Targets of the threat, individuals who would have perceived grievances)
    a. Who shared the threat with the school? (Possibility of cry for help and sometimes the one who found the threat was the actual threat maker)

Note: Law enforcement should initiate preservation order to social media platform if investigation proceeds. https://www.search.org/resources/isp-list/

BEHAVIOURAL AND DIGITAL THREAT ASSESSMENT TOOL KIT

SAFETY CONSIDERATIONS FOR IMMEDIATE RISK-REDUCING INTERVENTIONS

DOES THIS SITUATION REQUIRE IMMEDIATE LAW ENFORCEMENT RESPONSE?
IS THERE IMMINENT RISK TO A SPECIFIC TARGET OR SITE?

☐ No ☐ Unknown ☐ Yes

If No/Unknown

↓

Proceed with additional safety considerations below and continue the threat assessment process.

If Yes

↓

IMMINENT RISK

Call your local law enforcement agency and follow your emergency response protocols. Continue with a threat assessment process when safe to do so.

DOES THE SUBJECT OF CONCERN HAVE IMMEDIATE ACCESS TO THE MEANS TO CARRY OUT A THREAT?

(Did the threat come from social media containing an image of a weapon or other means? Check digital baseline for comments, images, and videos consistent with the threat, and be sure to reverse image search concerning photos to verify authenticity.)

☐ No ☐ Unknown ☐ Yes

If Yes: Immediate risk reducing intervention is to remove access to the means (e.g. firearm, Molotov cocktail, knife or other related weapons).

If no or unknown

↓

PROCEED WITH STEP 1 SCREENING

If yes to the above

↓

IMMINENT RISK

If data reported indicates immediate access to the means, immediately contain SOC (i.e., SRO/LEO).

Work with law enforcement to remove access by Search Warrant and/or Exigent Circumstance (See Appendix G).

If apprehended/held under a State Mental Health Act – still remove access to means.

If digital evidence is found, share with LE and recommend they complete the Search Warrant Template (see Appendix G) to obtain digital records.

Engage supervision, monitoring, and parents/guardians.

Complete Step 2: Comprehensive Multidisciplinary BDTA.

SAFER
SCHOOLS
TOGETHER

International Center for
Digital Threat Assessment