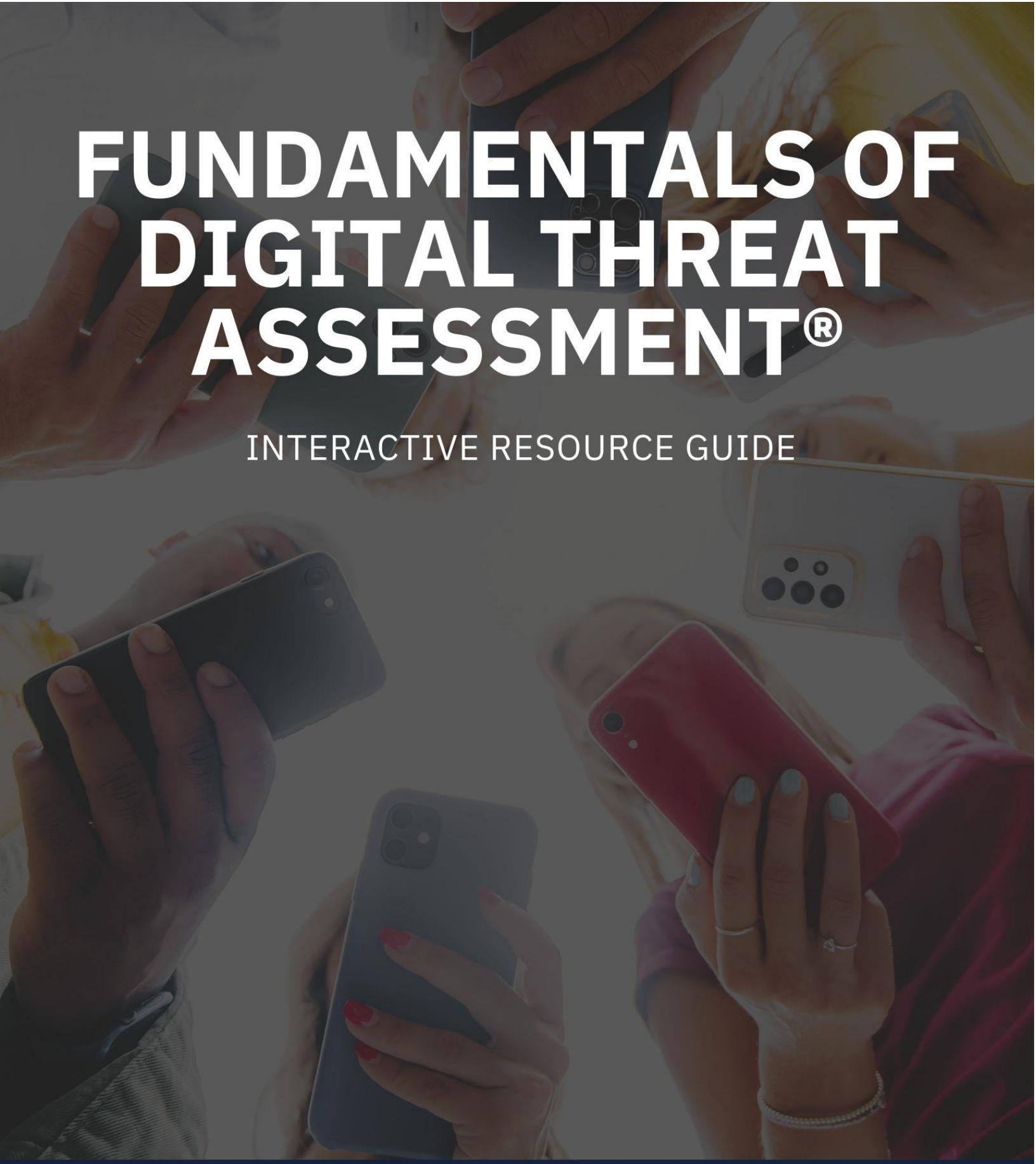
FUNDAMENTALS OF DIGITAL THREAT ASSESSMENT®

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

The Fundamentals of Digital Threat Assessment® is an introduction to the concept of Digital Threat Assessment® (DTA) and its place within the practice of Threat Assessment. Proactive and evidence-based, Fundamentals of DTA® will assist your team in identifying individuals who may pose a threat to the safety of themselves or others. By learning how to use open-source social media platforms to establish the digital behavioral baseline of a subject of concern (SOC), your team can prevent tragedy and intervene at the first sign of worrisome behavior.

Whether you have been trained in SIGMA, Salem-Keiser, Virginia, CSTAG, VTRA, or any other behavioral threat assessment framework, our DTA® training fills an important void for School Safety and Threat Assessment (SS/TA) Teams as they learn how to access real-time digital content from social media and other lesser-known parts of the internet.

HOW THE INTERNET HAS CHANGED

Have you ever looked up from your phone and wondered where the past 30 minutes have gone? If so, you're not alone. According to Backlinko, the average person spends nearly 6 hours per day on their phone.[1] Much of that time is spent on social media apps such as Instagram, TikTok, and Snapchat. Apple and Android devices can also tell us how much time we spend on our screens with Screen Time Tracking, a feature that breaks down how much time we spend on each app.

It's worthwhile to understand how we spend time on our devices. Obtaining the device of a Subject of Concern (SOC) is especially important when it comes to addressing a school safety concern. If School Safety/Threat Assessment (SS/TA) Teams have access to the subject's physical device, they can gain insight into what is occupying that subject's time.

Cell phones have evolved significantly over the years—from the 1985 brick phones to the flip phone, and now the smartphone. It has never been easier to connect to the Internet than it is today, and we can do so with the tap of a finger on a handheld device that fits nicely in our pocket.

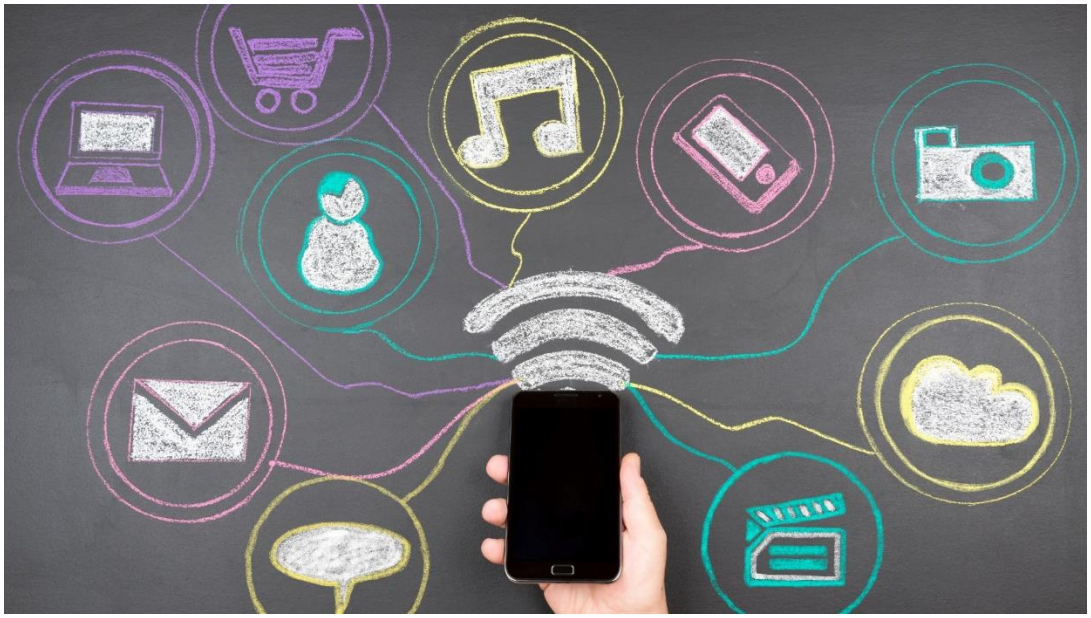
Just like cell phones and the Internet, social media platforms have also evolved. When many of us were growing up and wanted to see where our friends were, we would look for the house with all the bikes and scooters lined up outside. Now, students have access to Snapchat and the Snap Map (which you can learn about in our Snapchat Micro Module). Through the Snap Map, students can see where their friends are at any given time. What if somebody checks the map and sees that six of their friends got together without inviting them? How would that affect their mental health? Social media companies fail to consider these things when they develop new ways to engage online.

Before the Internet was so easily accessible, most families had access to the Internet on their home computers or would have to access it by visiting the library or an Internet café. At first, social media didn't look or operate the way it does today. The original function of Instagram, for example, was to upload and edit photos to share with friends. Now, people are creating and launching entire careers, brands, and advertising campaigns all through Instagram. X (Previously known as Twitter) similarly started as a simple microblogging platform; "Likes" and commenting came much later. The biggest thing driving our attention to our phones now is unrestricted access

[1] How long does the average user stay on their device?

and social media algorithms.

Before the use of algorithms, users saw posts of the people they followed in reverse chronological order. Then, Facebook determined that users didn't need to see their friends' posts in this specific order. They could keep users engaged longer if they showed users the posts with the most engagements or likes.

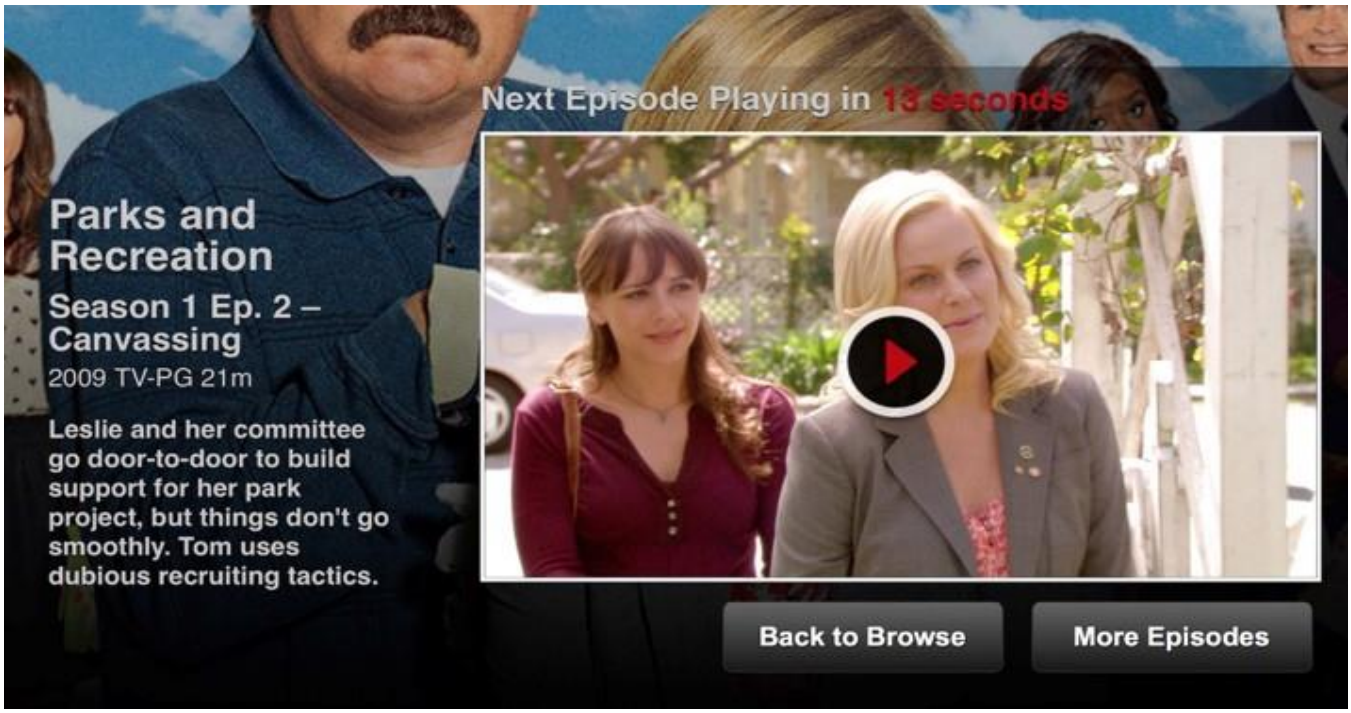


Social media companies are constantly changing. Facebook didn't incorporate hashtags until June 2013. Considering how widely used hashtags are, these features that are part of our regular everyday lives are not that old. Instagram "Reels" only went live in 2020 to compete with TikTok, which rebranded from Musical.ly in 2018. The ability to "go live" started on one social media app, and others followed their lead.

When observing the data and considering the timelines of certain features on social media platforms, it's easy to see that these companies are competing for our attention. It's important to remember why social media companies want us hooked in the first place. Unfortunately, the platforms are free to use because we are not the customers - we are the product. This product includes our data, interactions with the app, what we like, what we share, who we follow, and our search history. We readily sell our data to advertisers when we accept social media companies' terms of use.

Filmmaker Tristan Harris worked at Google as a data ethicist. Concerned by the direction that Google was heading and the amount of information they had on individuals, he left and created the Center for Humane Technology to give more insight into the personal information apps are gathering about us. Click here to watch the Netflix documentary (The Social Dilemma) to explore the dangerous impact of social networking.

Even Netflix itself has some big competitors that work to keep our attention. Companies such as Hulu, Disney+, and HBO are among some of the most popular streaming networks. However, many are surprised to hear that the biggest competitor Netflix has is actually YouTube. Netflix identified YouTube as its biggest competitor when YouTube launched the Autoplay feature that forces algorithm-recommended videos to automatically play when a video ends.



With so much content online, algorithms generate content and advertisements based on our behaviors – sometimes suggesting things before we even know we want them. Algorithms are very personal, and no two algorithms will be the same. Two people may have the same friend group and follow the same people, but their main feeds may look completely different. If we rarely check the app, the algorithm will mainly show us the posts with the most likes and interactions; if we engage with the same group of users, we'll be more likely to be shown their photos. Whether we are catching up on Instagram, TikTok, Reddit, or X, everyone's main feed will look different because they are determined by a combination of all our behaviors online.

The best example of this is Snapchat's gamification of its app – specifically, the Snapstreaks feature ("Snaps"). Streaks are the number of consecutive days two users have messaged each other without a 24-hour break. They are important to understand within the context of threat assessment and overall school safety. Who else can provide better insight into how an SOC's baseline has changed than someone who has the highest streak count with them? This is someone SS/TA Teams can interview to ensure accurate assessments of level of risk or in the development of a comprehensive intervention strategy. We can only access Streaks when we have access to the device of the subject, unless we ask their friends if they know with whom the subject has the highest Snapstreak with. That is someone we can now consider for an interview. For some youth, keeping that Streak alive is more important than school or anything else – so much so that it can lead to students giving their passwords to their friends while away on a camping trip or while they are grounded to continue the Streak if they are unable to.

SOCIAL MEDIA DATA REQUESTS

Have you ever wondered why our smartphones put that red badge beside the notification count? Red means "Alert!"; it's an important color and creates a sense of urgency. Every piece of design for social media is crafted with purpose.

Our phones and the apps we use also take advantage of our inherent social impulses and anxieties, including our fear of missing out (FOMO) and the impression that we need to reciprocate when we feel someone has done something for us. The clearest outcome of these notifications is that they keep us engaged with our devices. Many neuroscientists and psychologists are worried about the negative effects of this technology — from the way smartphones appear to affect our ability to concentrate, to the potential correlation with rising rates of mental illness and suicide in teens. There's also a fair amount of research detailing how notifications themselves distract users and cause stress.

Such purposeful design is why we are seeing an increase in social media usage; the apps are experts and are purposely convincing us to spend more time on their platforms. What we choose to share online provides insight into our thoughts, feelings, and behaviors. We can use information on social media activity to inform our threat assessments. Social media profiles and activity provides further insight into an SOC's digital behavioral baseline.

Following the Cambridge Analytica Scandal, revealing that Facebook was selling our personal data (including how we lean politically), there were many privacy laws and views that needed to be changed across all major social media platforms. Now, we can request our data from whichever social media site we choose. If you are interested in doing this, you can Google how to request your data from any given platform that you are actively using; all you need is a verified email, as this is where the data will be sent.

What does this data include?

- Our device information
- Account login dates, locations, and devices
- Login history
- IP address
- Latest location or top locations
- Search history
- Password changes
- Former email addresses
- Former usernames
- Privacy changes
- Date of birth
- Full names

This information is required when signing up for a social media platform. However, data requests can show us what Instagram, X, Facebook, Snapchat, or TikTok has identified as our interests based on the ways we interact with the app. Some may even show us the ads it plans to target to us.

OVERVIEW OF THE MOST POPULAR SOCIAL MEDIA PLATFORMS

TikTok

TikTok is a social network created for sharing user-generated videos. You can learn more about TikTok in the TikTok Micro Module.

- Users create and upload their own videos (3 seconds - 60 minutes long) where they sing, dance, or just talk. You can also browse and interact with other users' content, which covers a wide range of topics, songs, and styles.
- Users sign up with a phone number, email address, and a Facebook or Instagram account. Once logged in, you can search popular creators, categories (comedy, animals, sports, etc.), and hashtags to find videos. You can also use your phone contacts or social media followers to find friends already on the app.
- Youth on TikTok enjoy creating and sharing videos. However, others primarily use the app to watch videos and follow content creators. You are not required to log in to watch videos, however, other aspects of the app will be limited until you log in.

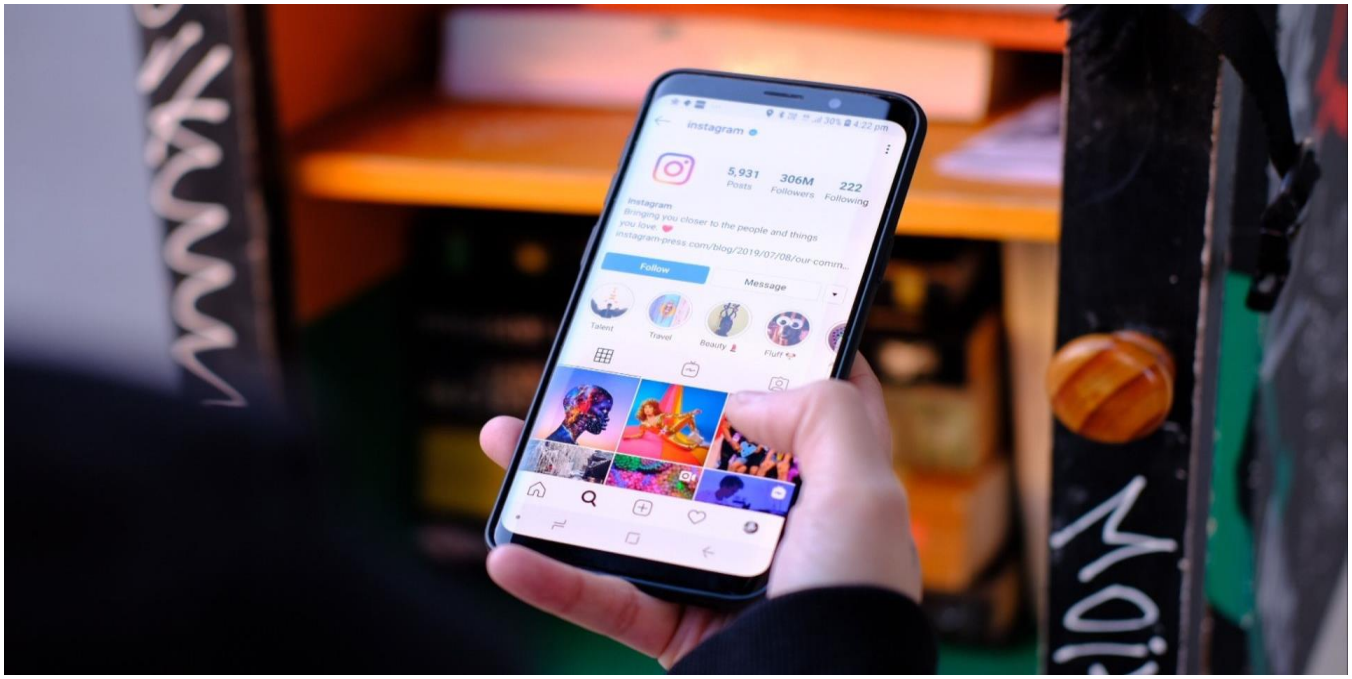
Instagram

Owned by Meta, Instagram is a popular photo-sharing app that has over 2 billion active monthly users.[2] You can learn more about Instagram in the Instagram Micro Module.

If you see a youth scrolling up with their thumb on their smartphone looking at photos, then chances are they are looking at Instagram. Hashtags (#) are used often on this platform: This gives people a way to be introduced to and follow other users with similar interests.

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

- **Stories/Highlights**: Allow 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 sending photos and videos), share content and links, and respond privately to stories.
- **Reels**: A feature on Instagram where users can share short videos; similar to the platform of TikTok.



[2] How many users are on Instagram?

Snapchat

Snapchat is designed for users to share instant messages, photos, or video messages that are set to expire after a certain amount of time. You can learn more about Snapchat in the Snapchat Micro Module.

Snapchat has grown well beyond message transmission and now includes features such as:

- **Snap Map**: Where users can see real-time geographical locations of their friends.
- **Public Stories (aka Our Story)**: A way to share content to the masses. Users do not have to be friends to view Public Stories.
- **Footsteps**: A way for users to see everywhere they have traveled in the last 24 hours.
- **My Eyes Only**: A vault application secured behind a passcode. A place to store images or short videos so others who pick up your phone don't accidentally encounter them.

Although the amount of information social media collects from us can seem alarming, it's important to know exactly what our personal social media use looks like and have a better understanding of why/how our youth spend so much time on social media. This is where we get the blend of current behavioral threat/risk assessments and DTA®.

We cannot understand the overall level of risk without establishing the SOC's digital behavioral baseline. Digital data can impact our threat/risk assessments, school safety plans, and our immediate risk-reducing interventions. This is why we need to apply a DTA® lens.

What social media platform is pictured below?

Answer: Both are from Snapchat.

There's a reason why two images are included – one is older and one is more recent. There's a lot to think about when working with the fast-paced evolution of social media platforms, including key things we need to look out for when dealing with different aspects of social media.

When opening a social media platform, the first step is recognizing the app we are working with. The photos above are vertical, which is usually what we see with photos from Snapchat. The most telltale sign of this image being from Snapchat is the grey text bar with the white text on it. This font and style won't be seen on any other social media platform that has the Stories functionality unless it was reposted from an original Snapchat photo. This grey text bar is unique to Snapchat.

Snapchat photos used to also include the countdown timer in the top right-hand corner. This timer showed how

long you can view the image for before it disappears. Note that there's no timer on the second photo because Snapchat has since been updated and removed this timer on the screen.

Another thing that differentiates the two photos is found in the top left corner of the second photo. It is a character known as a Bitmoji (a digital avatar), which is specific to Snapchat. Snapchat also allows users to change the overall appearance of their Bitmoji to reflect how they see themselves, an important piece of information when conducting a Digital Threat Assessment®.

Specifically with Snapchat, it's important to know the difference between usernames and vanity names. Notice that there is no actual information in the photos above, because 'Draids' is not the username. School districts and other community partners will often find or share the SOC's vanity name — but it's important that we identify the username instead. Vanity names are not unique to a social media profile, meanwhile a username is.

Many of the threats that we see frequently are individuals making statements such as "don't come to school tomorrow" with a photo of a weapon. The good news is that the majority of these threats are what we would consider low-level threats. This is based on a number of threat assessment considerations such as language, specificity of threat, access to the means, the digital behavioral baseline, and target and site selection.

Outside of identifying the app, we can use what's in the background of these photos to gather more information – anything that helps uncover who the subject of concern is (e.g., the color of the walls, the type of door, the TV). As we can see, there is so much information that SS/TA Teams can uncover from just a single Snapchat image.

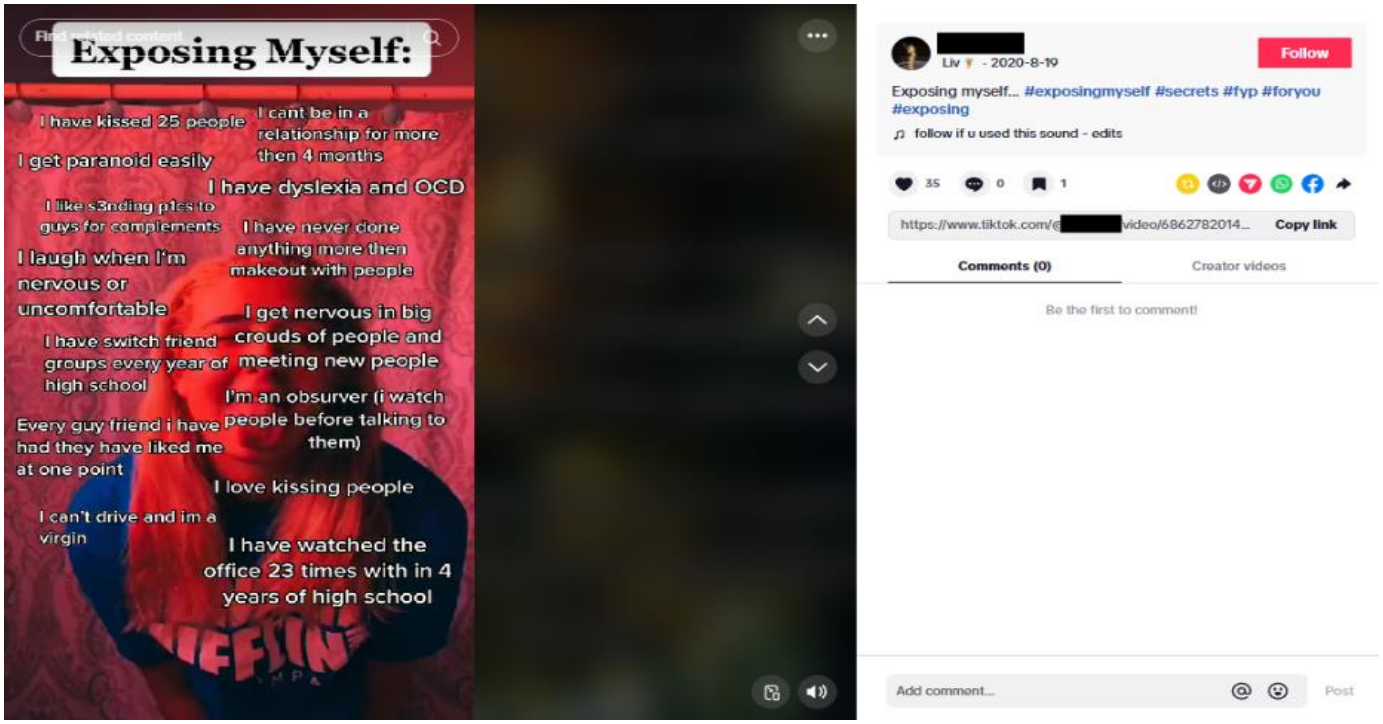
LEAKAGE

Another key term that will be referenced in DTA® is leakage. Pre-incident leakage can occur through daily journal entries, assignments, or graffiti tags; however, a major component of leakage that is missed occurs on social media. This does not have to be from public social media posts. It can occur in direct messaging conversations with friends. One-to-one communication apps are important, especially with social media platforms like Discord and Snapchat that are designed for private communication and group chats. That's why we can't just rely on our teams to capture all worrisome posts. Youth having access to an anonymous reporting tool, such as PSST World, can help them report any concerning behaviors they see outside the school, in the school, or through social media.

Why is DTA® necessary? Think back to Parkland, Florida, and the Marjory Stoneman Douglas High School tragedy in 2018 or any other case over the past few years. It is almost certain that each of them had some sort of social media or digital leakage. It was all there and present for us to find prior to the tragedy and before their SS/TA Teams were activated. They followed a threat assessment model; however, the digital data was not considered as part of their threat assessment. Unfortunately, this piece was missed. The killer did engage in behaviors that were consistent with the threat, had access to the means, and had perceived grievances towards the target and site (which in this case was the school).

This is why DTA® is the missing link for SS/TA Teams. It provides SS/TA Teams with the tools to find additional data we probably wouldn't find when we rely on traditional behavioral threat assessment models alone. Behavioral threat assessment relies on interviews with staff, students, and parents, but there are plenty of questions we can answer in two hours or less by looking at social media. Before a School Resource Officer or any other member of the SS/TA Team considers who they will interview, the online data from the publicly available open-source social media can inform additional questions we need to ask, who needs to be interviewed, and in what order. Remember that no two cases are the same.

There is so much data we can find by looking at social media. Have a look at the post on the following page and try to determine which social media platform it is:



Answer: This is a TikTok post – which is always going to be a video.

We now have the information to form a hypothesis based on what a student is posting about; those are things that inform us of our next steps.

The above screenshot is an example of a trend on TikTok that has been very popular, called "Exposing Myself":

These videos include positive and negative things said to the SOC. There is a wealth of information available in this one post alone. However, it's important to look further and establish the SOC's digital behavioral baseline and read every post and comment made. Information can often be found in one or two other posts as well.

What's the purpose of this exercise? It allows us to change our mindset from just looking at social media for entertainment, to analyzing the content to form an initial hypothesis around the subject's potential risk enhancers. This is the first step in intervention planning.

Questions To Think About

- What would be the hypothesized risk enhancers for this SOC? What would be some perceived injustices for this SOC?
- What are some initial thoughts about intervention plans for this SOC and what other agencies may need to be involved?
- Are the posts about peers who are possibly on the pathway to violence? To self-harm or suicide?
- In terms of perceived injustices, are they talking about bullying behavior? Are they mentioning any peers by name who are perceived to have bullied them in the past?
- Are they talking about perceived injustices with staff? Do they have problems with a certain staff member? What are these perceived injustices, and more importantly, what are some of the protective factors for the SOC? Do they mention any? Do they talk about positive relationship(s) with a counselor, staff member, teacher, or friend?

After collecting this initial information, it's time to test our hypotheses. This is where our SS/TA Teams can get together and conduct interviews based on what they have seen through publicly available social media — whether it's through one TikTok post or looking at their full digital behavioral baseline.

THREAT ASSESSMENT REVIEW

When we look at the characteristics of school killers, unfortunately, there is no clear profile as no two killers or threat makers are the same. What is clear is that they were all on the pathway to violence. This is why multidisciplinary Behavioral Threat Assessment and DTA® training is crucial for early identification.

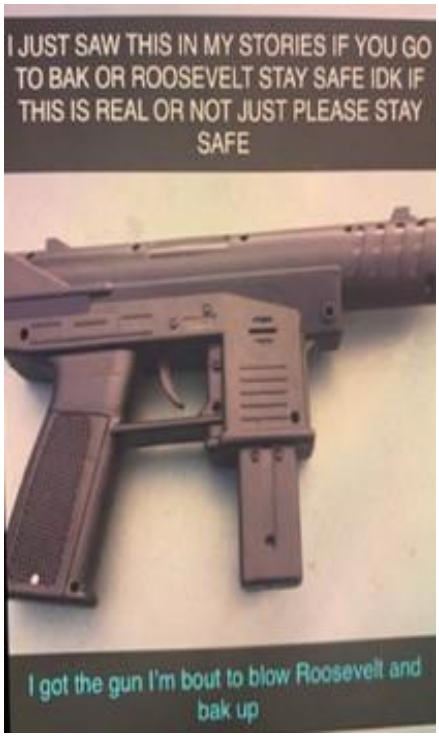
There are two critical principles to understand for a threat assessment or any school safety concern. The first is that all threat makers and threats are not equal. The second is that most threat makers are unlikely to carry out their threats based on language used. Regardless, all threats must be taken seriously and evaluated in the event that they are, in fact, expressions of intent to commit harm or act out violently against someone or something.

Below are some examples of different types of threats that have arisen in schools, according to the FBI and the US Secret Service. These are the kinds of threats we deal with on a weekly basis, especially in the world of social media:

- A direct threat identifies a specific act against a specific target and is delivered in a straightforward and explicit manner. For example: “I’m going to stab Jason in the cafeteria at lunch.”
- An indirect threat is one that tends to be vague, unclear, and often ambiguous. For example: “I could kill everyone at this school.”
- A veiled threat strongly implies but does not explicitly threaten violence. For example: “My life would be better if you weren’t around anymore.”
- A conditional threat warns of a violent act that will happen unless certain demands and terms are met. For example: “If you don’t give me the money you owe me, I’m going to shoot you.”

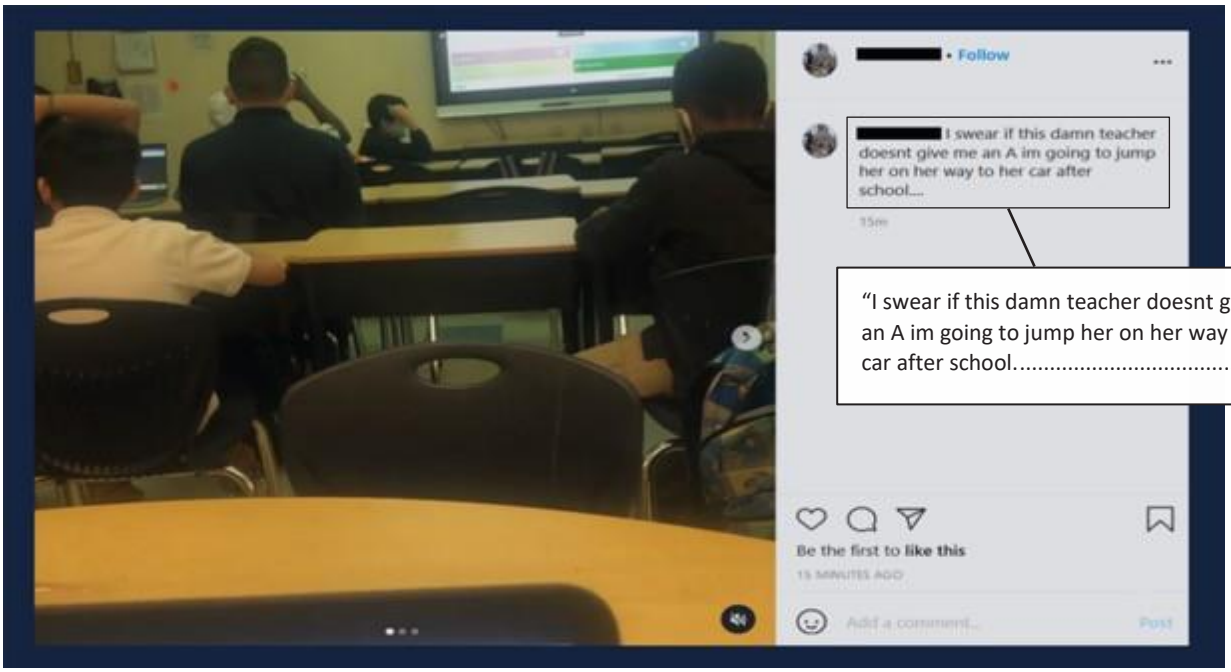
If there is a direct threat that is a criminal offence and the police are involved, SS/TA Teams need to be cautious when they consider who to interview and in what order. It’s important to communicate with local law enforcement prior to conducting interviews to ensure we don’t contaminate the criminal investigation.

Here are some examples from Snapchat that show the different types of threats we see:



One of the things that we talk about in DTA® training is the importance of determining if an image is real or not. Tools like the reverse image search allow us to determine if the photo is unique to the subject or if the photo has been shared and passed around Internet communities from another source. Based on this, we can determine the initial level of risk. Even if there is a fake photo of a gun, the threat could still be very real: Therefore, it should be taken seriously.

Let's examine this next example of a threat:



"I swear if this damn teacher doesn't give me an A, I'm going to jump her on the way to her car after school". As we can see, this conditional threat was made on Instagram, specifically, the desktop view of the site. There are a couple different ways that we can identify the platform: the profile picture next to the username, the username next to the comment's text, the date it was posted, and the like, comment, and share icons. These are all specific to Instagram.

Threat assessment is the process of determining if an SOC actually poses a risk to the target(s). The initial threat assessment can usually be carried out in two hours or less, during which our SS/TA Teams engage in the data collection process. Someone may be looking at the social media data while someone else conducts interviews. Ultimately, we have different individuals from different agencies coming together to plan the immediate risk-reducing interventions.

If someone posts or sends a photo of a gun with text saying not to come to school tomorrow, we want to get the police and our School Resource Officer(s) involved. If it turns out to be a real and/or unique image of a firearm, we must ask multiple questions:

- If we know who this person is, where are they now?
- Does the threat maker have access to that gun?
- Is it their firearm or does it belong to someone else?
- How can we make sure we eliminate the access to that weapon?

Threat assessment is designed to identify and assess risks in a deliberate and data-driven approach. In determining response strategies to mitigate risk, it is helpful to clarify threats by level. Based on the information collected, the SS/TA Team will determine the level of risk by looking at publicly available open-source social media surrounding threats.

Concern level:	Concern Rating Grid
LOWER	There was no true threat (no evidence was found that a threat was made), and/or behaviours were taken out of context, and/or threat is vague, indirect, inconsistent, implausible, and/or SOC lacks developmental understanding or intent. The student can be managed through existing resources and programming, but the individual should be observed for changes that could increase their risk level. Supports and resources may be recommended.
MEDIUM	Threat is plausible but lacks specificity or intent. No clear indication that the student has taken preparatory steps. Has the capacity and means to carry out an act of violence if stressors/contributing factors cannot be mitigated. Some grievances and/or indications of a potential plan but does not view situation as hopeless, helpless, and/or desperate; willing to consider non-violent alternatives and some protective factors present. An intervention and management plan must be developed with increased monitoring, supervision, and interventions established. Progress monitoring and ongoing team reviews are to occur.
HIGHER	Has intent, means, and capacity. A highly directive and intensive intervention and management plan must be developed. Student may not to be at school in the short term in order to receive interventions and supports. All risk reducing interventions, monitoring, and supports must be explored and closely monitored with frequent progress monitoring and team reviews. A return-to school plan may also need to be developed.
IMMINENT	Risk is very serious. Immediate containment is needed from law enforcement (i.e., taken into custody) or an emergency mental health hold is necessary to assure safety.

When SS/TA Teams are conducting a threat assessment, it is important to break down the language of these threats as this will assist in determining the level of risk a threat may carry. When identifying a threat, there are different levels in which these threats can be made:

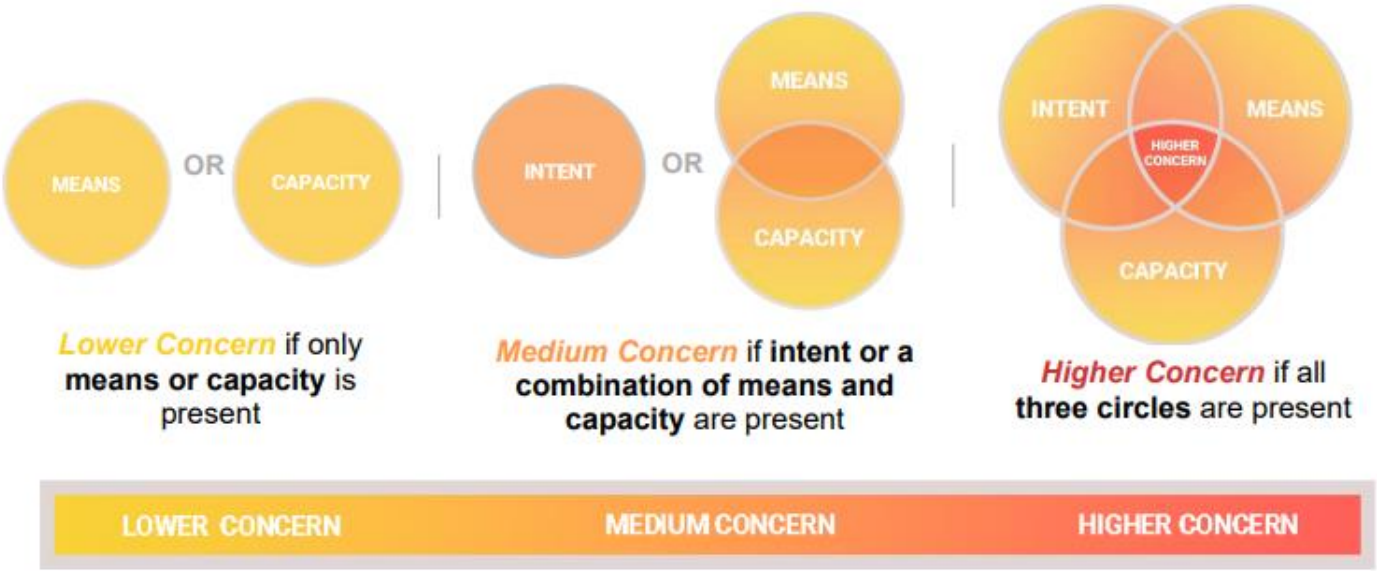
- **Direct:** A threat that identifies a specific act against a specific target and is delivered in a straightforward, clear, and explicit manner. “I am going to stab Jason in the cafeteria at lunch.”
- **Indirect:** A threat that tends to be vague, unclear, and ambiguous. “I could kill you; I could 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.”

Beyond determining the type of threat that is being made, SS/TA Teams must be asking these additional questions below which again support the implementation of those immediate risk-reducing interventions

- **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?

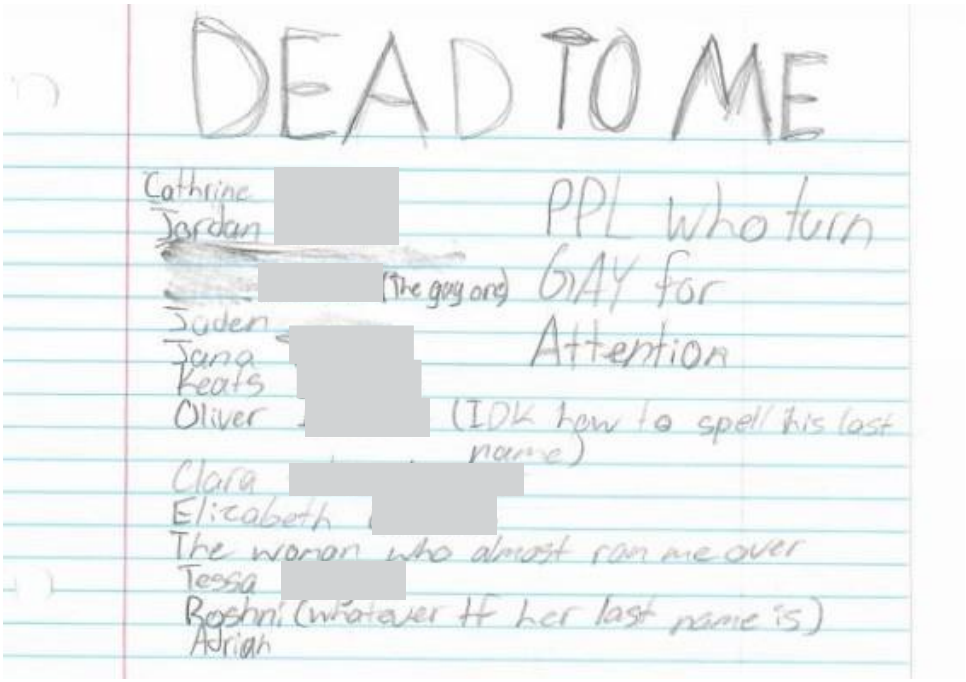


"Low categorization of risk does not imply no risk."

It is also important that we examine the exact language of the threat(s). In a specific case example from SST's Threat Analyst Team, a student came forward to the school with a gun in a plastic bag. The student walked into the school's office and told the principal, "I found this gun stashed behind the urinal. Here you go." First, the SS/TA Team checked the cameras and did not see anyone entering that washroom prior to that student in the early morning which caused confusion as to when the weapon was put in the restroom. They interviewed many peers who were at school around that time but couldn't identify anyone, so they reached out to SST.

SST's first question was, "When that student brought the gun forward, what was their exact language?" The response was, "He said he found it stashed behind the urinal." A lot of the time, urinals in men's rooms are attached to the wall, so nothing can be stashed behind it. That was the first clue, but one of the other important pieces is considering everyone involved. We asked the school about the student that found the gun to get a sense of their baseline behavior. According to the school, this student had no prior history; he was, however, changing schools the next week because his parents had divorced and were now moving a significant distance away. This was important information and SST suggested the team re-interview the student. In the second interview, the SS/TA Team discovered that the SOC wanted to leave school on a "high note" (being seen as a hero), so he placed the gun there himself. When the SS/TA Team searched his locker, they found a suicide note which would suggest that him bringing that firearm to the office was a "Cry for Help".

Another common thing we come across are "hit lists", "kill lists" or "shit lists" where SOCs make a list of those they feel have wronged them. SST has dealt with many of these incidents and 90-95% of the time, the author has included their name on the list. That is why interviewing all those involved is crucial when dealing with an SS/TA issue.



What would constitute a high-risk threat? It's one where an individual or situation appears to pose a threat of violence and where the threat maker exhibits behaviors that indicate both a continuing intent to harm and efforts to carry out that plan. The subject may also exhibit some concerning behaviors that would require immediate intervention: Being categorized as "high-risk" indicates an imminent risk of violence and an immediate need for interventions. This is a direct, specific, or plausible threat.

With a high-risk threat maker, we're going to notice significant shifts in their behavioral or digital baselines and it's still important to look at how frequently they post, the intensity of their posts, and the recency of their posts. There's almost certainly an extensive history of warning signs and possible acts of violence, including leakage.

This type of threat suggests that some concrete steps have been taken towards carrying out the threat, which denotes a level of commitment. It is imperative that we check for posts about weapons. These are behaviors that are consistent with the threat and it appears they have the means to carry out that threat. Other data that can be concerning could be diary entries or floorplans of the school. Some of the high-risk cases that SST has handled have involved the SOC having detailed plans — even down to the exact time they would conduct that act of violence. One journal chose 8:32 am as the time, since most students would still be groggy. This is very specific and therefore denotes a high level of risk. They also had access to the means and had made a detailed plan.

As SS/TA Teams, we need to prioritize data-driven intervention planning to be successful at redirecting the path the SOC is on.

SOCIAL MEDIA ACCOUNTS FOR SCHOOL SAFETY / THREAT ASSESSMENT

Two things we need to understand when we explore the world of DTA® is why we are searching, and more importantly, how we are searching. When we understand how social media algorithms work, we can get a better understanding of why we need to create an account(s) specifically for searching when dealing with a SS/TA issue. If we use our personal accounts for searching, there are some potential issues that can arise.

It is imperative we do not use personal accounts when collecting data for SS/TA. Here is a scenario of why it's not best practice to use personal accounts:

You've been scrolling through someone's Instagram page and you've gone pretty far back in their post history. Just then, you accidentally double tap a picture — liking it. Our concern now is that the SOC will receive a notification that their post from a year ago was just liked by you. It could be embarrassing for them and could significantly impact the threat assessment process. It is important to avoid this when we are gathering an SOC's digital behavioral baseline. This could also lead the SOC to deleting or hiding all their public posts or even their entire profile.

Another issue arises with the sites' algorithms. One of the ways platforms such as Facebook, Instagram, and TikTok suggest friends or 'who to follow' is through our behaviors and our interactions within the app. If we search for an SOC using a personal account and conduct daily check-ins on their baseline, the algorithm is going to suggest us as a potential friend on the SOC's feed. Because of our activity with the SOC, we would most likely be their top friend suggestion because we have looked at their account so many times.

Another reason to avoid using personal accounts for any SS/TA concerns that arise is that in a remote learning environment, it's been more common for teachers and staff to use social media to engage with students. If it's part of the curriculum, this should be done through work-based social media accounts. It becomes an issue, however, if staff members use their personal social media accounts to interact with their class. SST does not recommend friending students from personal accounts (or from their SS/TA accounts). No messages or friend requests should be conducted between staff and students. The SS/TA accounts should be used for the sole purpose of responding to school safety concerns or conducting threat assessments.

Before creating an SS/TA account for the purpose of searching, we must first review when an account should be used. Within a law enforcement environment, adequately trained internet investigators and researchers are allowed to create covert accounts to allow covert investigations to be conducted.

As SS/TA Teams, we only want to create these accounts for the purpose of searching. We should never pretend to be another student, request to follow them if their accounts are set to private, or send any messages. The purpose of these accounts is to collect data that is necessary and relevant to your SS/ TA concerns.

It is crucial that SS/TA Teams keep records of the details (e.g. username, password, etc.) associated with their accounts. Recorded details will provide useful if any social media site restricts access to an account and asks the owner to prove they are the account holder by asking questions based on the information provided. In the event that evidence is taken to court, the team can provide the information used for their SS/TA accounts.

Before you create an SS/TA account, you must know your agency's policies around things like friending and any levels of approval or documentation required.

The process of creating an SS/TA account may seem simple, however, the process in which the account is created is important. Here are some tips to consider when creating an account:

- Do not use a VPN; most IP ranges will be flagged.
- Use a public network (such as a Starbucks or a Public Library). Be aware that you will not be on a secure public network. Do not do anything else except create the account(s) while connected to a public network.
- Clear your cache data before you begin. Click here to learn how to clear your browser cache.

Setup Step 1: Email Creation

Just as we do not use personal accounts to conduct SS/TA searches on social media, we do not use personal email addresses to create these accounts. Instead, we create SS/TA Team-specific emails using Tuta Mail.

Setup Step 2: SS/TA Account Creation

- Create all your accounts at once and tie them in as one profile. This will create intentional cross-correlation.
- Keep notes on your SS/TA accounts. The use of a good password manager is suggested.
- Once the account is created, do not leave it empty. Make it feel real right away by adding a profile picture, a bio, and if applicable, some interests to your profile.

What To Name the Account?

SS/TA Teams should not create fake accounts pretending to be a young student in an attempt to gain access to a private account that is privileged content. However, from the connections we may have with students in the school, it's possible to use those connections to ask students in-person if they will show us the SOC's social media account(s).

When creating your SS/TA account, you will need to come up with an account name. Here are some things to consider when choosing a name for your account:

- Do not impersonate someone else.
- Do not add students as friends.
- Keep the theme of your account school related. Have fun with this! For example, if your school is in Texas and called the "Knights", you could call your account "@txknights".

Where To Find Content to Post on the Account?

It is encouraged that SS/TA Teams get together as a team to create one social media account for each platform that is shared only in the SS/TA Team.

There are some good resources for finding free, high-quality stock photos to use for these profiles, including:

- Pexels
- Unsplash
- Royalty-free Bing or Google Images of large crowds (sporting events or concerts)

It is also a good idea to join groups, such as Facebook public Groups, or public forums, such as Reddit, that are publicly accessible – usually based on celebrities, fan accounts, meme accounts, or sports team networks to get content and get engagement on your profile.

Avoid political chat and comments. Politics and social issues are high on the radar of Facebook due to fake news and voter tampering concerns.

PASSWORDS

The Importance of Secure Passwords/Password Managers

Think of your password as a guard that stands between your personal information and potential online risks. Given the best protective armor, the chance of anything getting through is minimized.

When creating passwords with combinations of letters and numbers that are unique for every online account, it will make it more difficult to unlock our identities – keeping information safe and secure. It is recommended to password-protect all your devices: computer, laptop, tablet, smartphone, etc.

We all know the challenge of trying to remember our password for a website or an app, and it's easy to fall into the habit of using the exact same passwords – easy ones – for all of our logins. This is a dangerous practice, especially if it is something easily guessable such as a dog or child's name and their birthday.

Use different passwords for different sites and build strong ones: a mix of numbers, letters, and special characters (!@#$%^&*).

What Makes a Strong Password?

To increase password strength, follow these tips:

- Minimum length of eight characters
- Include at least one character that isn't a letter or number (such as, !@#$%^&*)
- Use a combination of upper and lower-case letters and at least one number
- Disable automatic sign-in
- Use different passwords for different online accounts, especially those dealing with sensitive or financial information (online banking, etc.)
- Do not share your passwords with those outside your SS/TA Team
- Use a password manager such as Lastpass or Dashlane

These are the most common passwords statistically used around the world (based on data breaches) – if any of these are yours, we recommend changing them:

- 123456
- 123456789
- qwerty
- password
- 12345
- qwerty123
- 1q2w3e
- 12345678
- 111111
- 1234567890

TWO-FACTOR AUTHENTICATION (2FA)

Two-Factor Authentication (2FA) is a security process in which users provide two different authentication factors to verify themselves. 2FA provides a higher level of security than a single-factor authentication (SFA), in which the user provides only one factor, typically just a password.

2FA adds an additional layer of security to the authentication process by making it harder for attackers to gain access to an individual's devices or online accounts. Knowing a password alone is not enough to pass an authentication check.

It is also recommended that SS/TA Teams enable 2FA for their threat assessment accounts.

USERNAMES

It is important that we understand the significance of usernames, especially in the SS/TA world. Essentially, a username is a unique identity created by an account user to distinguish themselves from other users. When we conduct a threat assessment or respond to a school safety concern, we are collecting and recording data. Usernames are one of the most valuable pieces of data that we can collect. We must also understand where to go to find the usernames and how to document and record the information.

Many youth have consistent usernames across multiple platforms (or some kind of variation of a username). We can use this information to find additional accounts they are using — even if we're typing it into a Google search.

With some platforms (mainly Instagram and TikTok), individuals will often have more than one account on the platform. On Instagram specifically, these accounts are called "spam accounts" or "finsta accounts". The main account is used as their highlight reel, with their public posts that are highly curated and edited for the public. These are photos they've meticulously chosen to represent themselves with online, knowing that their posts are viewable to the public. Finsta accounts are commonly private. Accounts owners will only allow close friends to follow. Everything that doesn't make the public page will often show up on spam/finsta accounts. Public finsta accounts, however, give us a better insight into the subject's digital baseline.

SOCs are not always going to use the same username(s) for these spam/finsta accounts. It may be a combination of their regular username plus the word "finsta" or their regular username plus "2.0". Some users may have three or four different usernames/accounts. However, if we look at the baseline of all their posts, we should be able to match them up. Maybe they use the same profile picture, have similar photos, or the same followers. These factors can all help identify when the same person is behind multiple accounts.

HASHTAGS

The word “hashtag” (#) has become part of our everyday vernacular. Hashtags are a means of connecting with others within a specific social media app. If we were to click on the hashtag #travel on Instagram, we would see all of the public posts that are tagged with #travel. They are a helpful tool as they serve almost like a file folder organizing different related posts.

Unfortunately, one of the ways we see hashtags being used is related to self-harm and suicidal behavior/ ideation, such as in the example below:

Don't worry guys. Sadly, I'm still here. I was just grounded for a looooong ass time. (I don't promote anything but easing the pain ✌) **#sad #suicide #suicidal #depressed #depression #ugly #fuckup #fat #useless #worthless #disgusting #pig #stopeating #ana #mia #deb #sue #cut #cutting #lost #unfixable #alone #unloved #unwanted #secretsociety123**

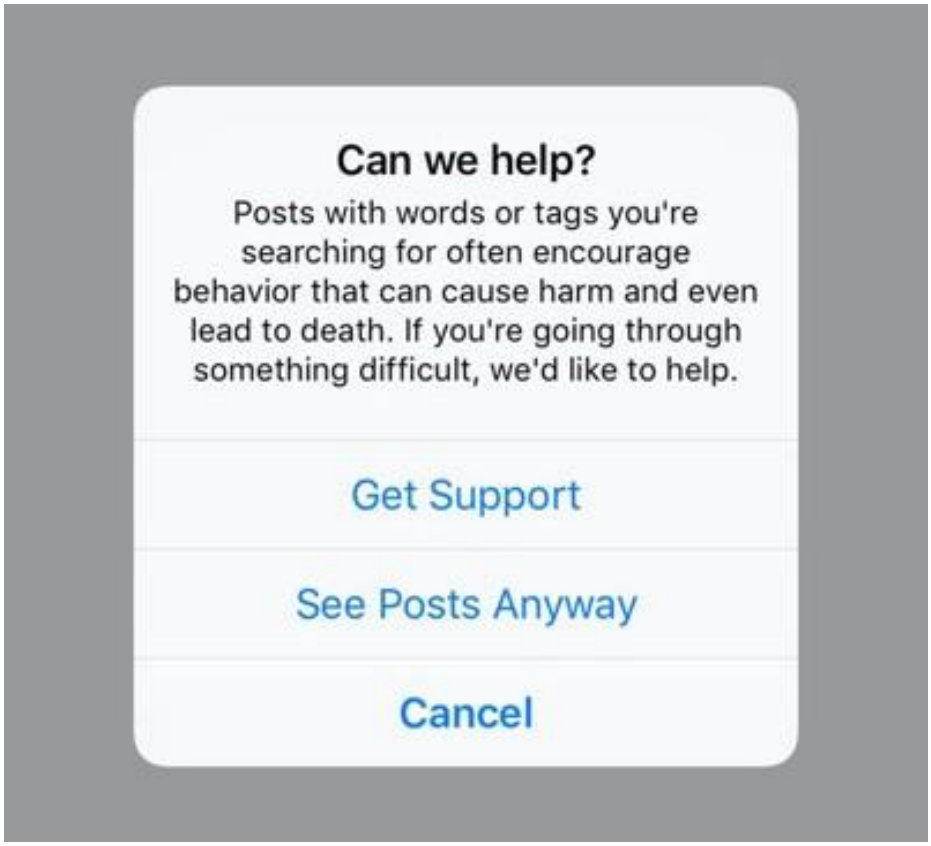
If we read the caption through an SS/TA lens, we find the self-harm posts very troubling. Looking at the caption associated with that post, we see #sad, #suicide, #suicidal, #depressed, #depression, #ugly, #fat, #useless, #ana, #mia, #deb, #sue, #cutting.

Which hashtags in this example would we want further information on? Who is Deb? Who is Sue? Are they peers of the SOC? Are they connected somehow? What is #secretsociety123?

We found through the Journal of Adolescent Health that there is a language of self-harm on Instagram using hashtags associated with mental health issues and eating disorders. #Ana possibly indicates someone is feeling or has engaged in activities associated with anorexia; a male may use #Rex to indicate this. There are male and female associations to each hashtag. #Bri or #Bob possibly indicates someone is feeling or dealing with bipolar disorder, and #EDNOS means "eating disorder not otherwise specified". This is the way that our youth communicate and engage with each other through a secret language online.

This behavior doesn't only happen on Instagram. We see self-harm trends exploding in popularity on TikTok as well, which has become a huge way for our youth to engage and share trends.

Note: if we were to click on some of those worrisome hashtags, such as #Ana, #Mia, or #suicidal, Instagram now has filters that suggest you're about to see graphic content, providing available resources for anyone struggling with mental health.



DOCUMENTATION

Learning how to document properly and take screenshots on different devices is critical for SS/TA Teams when conducting threat assessment and responding to school safety concerns.

Rules of engagement for DTA® involve collecting data from multiple sources to make a well-informed, data-driven assessment of risk. This allows the SS/TA and multi-disciplinary team(s) to structure an appropriate intervention for corrective action and redirection towards a positive, safe, and pro- social outcome. Conversely, DTA® tools should never be utilized to locate information that could be used against a SOC who is causing a significant amount of mischief in the building so that we have grounds to suspend or expel them. A poorly timed suspension or premature disciplinary action can be a contributing risk-enhancer for an SOC who is already at risk. When responding to threat-related behavior, a threat assessment should precede a suspension.

The information being gathered for SS/TA purposes is publicly available information, also known as Open-Source Intelligence (OSINT). OSINT is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term 'open' refers to overt, publicly available sources.

Data doesn't lie. It's important to gather and document. What else might we find if we know what to look for and whom to ask? Consider the following:

- Student name(s)/nickname(s)
- Current school
- Date of birth
- Name of friend(s)/peer(s)
- Phone number
- Email address (both school and personal)
- Any known social media sites/username(s)*

*It is important to know the exact spelling of usernames.

What To Include in Digital Behavioral Baseline Data Collection

- Username(s)
- Vanity Name(s)
- Real Name(s)
- Screenshots
- Preserve Videos
- Bios
- Information on Others Tagged in Posts
- Profile Web Addresses
- Date and Time of Collection
- Date and Time of Concerning Post(s)
- Location of Post, if possible
- IP Address, if possible

When we are examining an SOC's open-source social media posts and when documenting, we must ask when the posts were made and document that information appropriately. With every social media post, you can find the corresponding date it was posted. This gives us the opportunity to take note of things such as frequency, intensity, and recency of their social media posts and behaviors.

OVERSHARING/PRIVACY

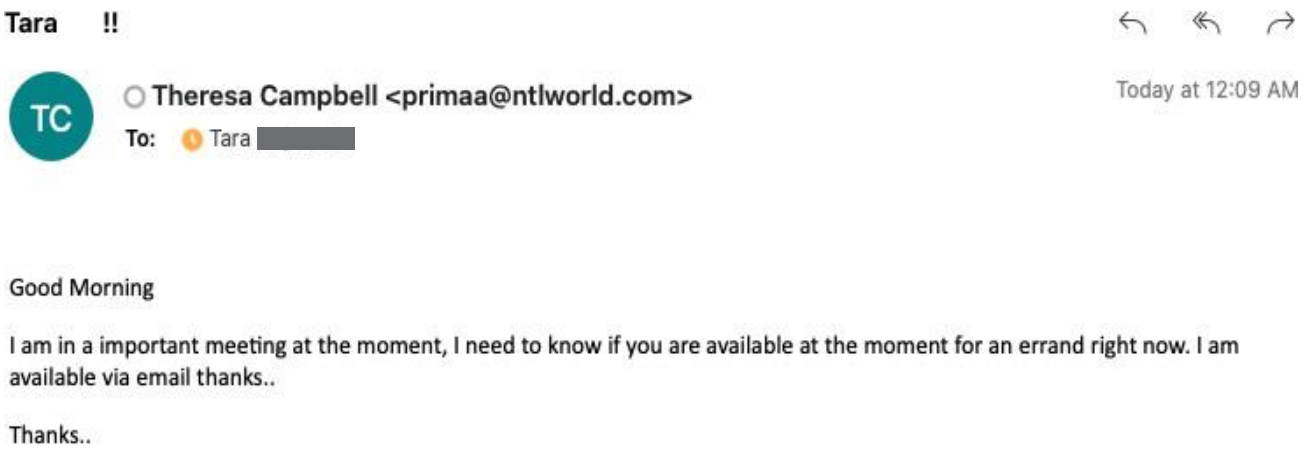
Before social networks were invented, oversharing existed in society. It happened at the gym, at the office, at the dog park…these days, it happens most commonly on social media.

We always need to ensure we're not giving away too much information without even knowing it. For instance, Facebook, we've probably seen this:

Find your Unicorn Name! How fun! Share your name in the comments! All you have to do is publicly post your name and…the month you were born…and the street you grew up on…and the name of your first pet…and your mother's maiden name…and the last 4 digits of your social…you get the point. This may seem like a common and fun activity, but it exposes us to dedicated hackers or people using social engineering tactics to find out information that we would not otherwise be willing to post publicly. Birth months can be valuable pieces of information and can contribute to a stolen identity. It's always important to understand where our information goes and who can see it.

Social engineering is still one of the most common means of cyber-attack — primarily because it's highly efficient. To criminals, the user is the 'weakest link in the security chain'.

Users are normally targeted in two ways: either over the phone or online. By phone, criminals will sometimes pose as employees of a company or organization such as a bank. After going through some typical questions and statements to gain the trust of the potential victim, they will then ask for login credentials and passwords to the potential victim's accounts. No one is safe from this practice, it even recently happened to one of SST's employees:



Tara !!

TC

Theresa Campbell <primaa@ntlworld.com>

Today at 12:09 AM

To: Tara [redacted]

Good Morning

I am in a important meeting at the moment, I need to know if you are available at the moment for an errand right now. I am available via email thanks..

Thanks..

Can you find the discrepancies in this email? What would indicate to Tara that this email isn't actually from Theresa Campbell, CEO of Safer Schools Together? Is it the fact that it didn't come from a @ saferschoolstogether.com domain? Is it the fact that there is no email signature from Theresa? Is it the fact that it was sent at 12 AM and yet started with "Good Morning"? Is it the fact that Theresa would never ask for an errand in such a strange way? These are all important questions to ask when assessing the validity of anything online.

The most common fraud technique on the Internet is "phishing". In this technique, users reveal data because they think they are on a trusted website. Another way that social engineering is used online is by using attachments in emails from people or companies/organizations known to the victim (such as the example from SST above). Malware is used to attack users' address books and send emails with the attacker's file attached to all their contacts.

Falling victim to social engineering can be avoided. First and foremost, to prevent data theft through social engineering, be wary and use common sense. Never reveal passwords or login credentials to anyone. If a legitimate technician needs to access our account or information, they should be able to do this without needing you to give them private details.

We need to be aware of details present in social media posts. What's in the background of the post? Let's look at an example:

What's in the background of this post? We can see this one has cropped out the license plate, which is good practice, but in the background – can you see it? There's a cross street telling us the photo's general location. That's enough information to find the user's house on Google Maps and Street View. Scary!

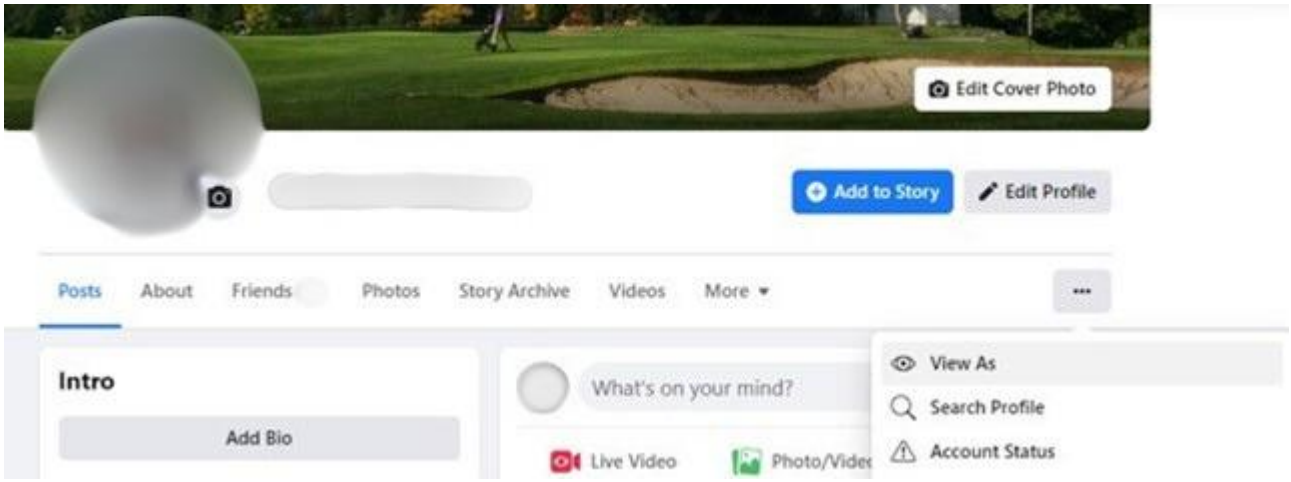
When we post identifying details online, willingly or unknowingly, it becomes publicly available open- source data – which is accessible to anyone. These days, we have parents putting their children's lives on social media before they even have the chance to consent, and students posting pictures of their class schedules and are most likely tagging the school location to those schedules. They post about their teachers and when they have classes, trying to find friends, but also giving away vital information.

Those of us in remote learning or working environments also must guard our personal information. When we work from home, we can inadvertently give away information in the background of our video calls or when we take pictures of our workstations. It's important to understand the amount of information that we don't even realize we're giving up.

PRIVACY SETTINGS

Privacy settings are part of digital responsibility that we need to normalize in both our own social media accounts, our student and children's social media accounts, and our threat assessment accounts. We can learn more about ensuring digital privacy in the Ensuring Your Digital Privacy Micro Module.

When we're logged into our personal social media account, we can see who's posted on our timelines or tagged us in posts/photos, our photos, our friends, and our videos. We're logged into our account, so of course, we have access to everything. If we want to see what our account looks like for people who aren't our friends, there's a button for that; though, it may only be available on desktop computers and not the mobile app version. On Facebook, for example, there's a button at the top of our profile that says, "View As".



Clicking on "View As" shows what our profile looks like to the public or our friends/followers. Try this for yourself on your personal profile.

CONCLUSION

When addressing any school safety concern, it is vitally important to review an SOC's Digital Behavioral Baseline (DBR). Finding the Digital leakage is necessary for school safety and threat assessment teams to identify individuals on the pathway to harm themselves or others and to plan an immediate risk reducing data-driven intervention plan.

Digital Threat Assessment® (DTA) is frequently updated to reflect the changing landscape of social media and the current best practices for School Safety and Threat Assessment teams. SST developed Fundamentals of DTA® to introduce the key concepts of DTA® to school safety and threat assessment professionals. We hope this guide and video module will prove useful as you continue to do the valuable work of keeping our students safe.

ADDITIONAL RESOURCES

Fake Post Generators

- https://zeoob.com/

Finding Meanings of Current Lingo

- http://urbandictionary.com
- https://keywordtool.io/instagram

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://gadwin.com/printscreen/
- https://www.apowersoft.com/free-online-screen-recorder
- https://screenpal.com/
- https://getsharex.com
- https://camstudio.org
- https://support.apple.com/en-ca/102618
- https://www.windowscentral.com/xbox-game-bar
- http://instadp.com

Law Enforcement Guides and Data Requests

- http://www.search.org
- Google – how to request data from…

Other Resources

- Digital Threat Assessment® Training
- TikTok Interactive Resource Guide
- Snapchat Interactive Resource Guide
- Ensuring Digital Privacy Resource Guide

ICDTA®
International Center for Digital Threat Assessment

International Center for Digital Threat Assessment® (ICDTA®)

SST | SAFER SCHOOLS TOGETHER

Safer Schools Together

SAFER
SCHOOLS
TOGETHER

ICDTA®
International Center for
Digital Threat Assessment