ENSURING YOUR DIGITAL PRIVACY

INTERACTIVE RESOURCE GUIDE

SSST | SAFER SCHOOLS TOGETHER

ICDTA®
International Center for Digital Threat Assessment

TABLE OF CONTENTS

INTRODUCTION

Law enforcement officers and school staff (teachers, administrators) can be targets or subjects of threat-related behavior. This Interactive Resource Guide and accompanying Micro Module will provide participants with tools and knowledge to ensure their digital privacy and safety.

Advances in technology and today's digital economy have made it difficult to distinguish between the information that should be freely shared online and information that should be kept private. Are you inadvertently giving away more information about yourself or your family than you should be? When almost every aspect of our lives is touched by some form of technology, the best approach to ensuring your digital privacy is to increase your digital literacy.

Safer Schools Together (SST) has seen an increase in personal information being used in harmful ways, specifically for those in the education sector. Since the onset of the COVID-19 pandemic, teachers and educators have had to pivot to a new teaching style. The transition to remote learning brought with it new platforms such as Zoom and Teams. This experience has been a stark reminder of how important it is to ensure you know what you are sharing online and who can view it.

Protecting sensitive information is becoming increasingly difficult as private information is exposed more frequently. When private information is shared on a public platform, it's usually exposed by someone with the intent of ruining the victim's life or subjecting them to embarrassment, harassment, and/or threats.

The act of gathering an individual's personal information (such as name, address, phone number, etc.) and publishing that information online is known as "doxing". The name derives from the word "document". According to an article from Wired magazine, doxing is "compiling and releasing a dossier of personal information on someone. The word dox is the modern, abbreviated form of 'dropping dox,' an old-school revenge tactic that emerged from hacker culture in 1990s." [1] The term first came into use in the 1990s to describe humiliating or intimidating someone by linking online personas to sensitive personal information.

[1] https://www.wired.com/2014/03/doxing/

Photo courtesy of Smarty DNS.

While doxing is an older trend, the laws are quite clear about what is legal and what isn't. Technically, it's not against the law to find someone's publicly available information and re-post it elsewhere online. However, there are two instances where this conduct could be considered illegal. First, if the information was obtained through illegal methods, such as hacking, the publication of this information becomes illegal. Second, if the information is posted with the intent of harassment; intimidation; invasion of privacy; assault; or instruction to carry out any of the preceding actions toward the victim, the publication of the information is against the law. It is possible for doxing to be prosecuted as assault if the intent was to intimidate someone or threaten them with violent conduct.

Doxing is usually seen as a form of cyberbullying. When it comes to doxing organizations, it usually plays out in the form of blackmail. An example of this was the Ashley Madison data breach where private data was collected by hacking methods and shared online when the demands of the attackers were not met.

Photo courtesy of HUFFPOST UK.

Researchers at the New York University Tandon School of Engineering and the University of Illinois at Chicago, conducted the first large-scale study to find out who is most likely to get doxed and why.[2] The results showed that although women experience more online harassment in general, doxing specifically is targeted mostly towards men. Men are more commonly doxed because the most frequent types of users to get doxed are gamers and hackers, which are mostly male-dominated. The researchers also looked at the motivation of doxers where they found that justice and revenge were the two most common motivations, followed by competitive or political reasonings.

Although protecting ourselves online can seem intimidating, it's important to be educated on the potential dangers of personal information being shared online, as well as the benefits of digital privacy.

[2] https://pmc.ncbi.nlm.nih.gov/articles/PMC6352099/

HISTORY OF DOXING

For many regular internet users, doxing is now common household terminology. Some of us have probably seen doxing without even realizing it. Whenever we see on the internet that someone said or did something that was deemed unacceptable, there were probably comments or other posts that included where the person worked, where they lived, where they went to school, or a combination of all three. Let's explore some high-profile doxing attacks that shaped how we understand doxing today:

Fake Messaging BC Teacher

Falsely accused teacher files lawsuit in sexual abuse case

TRACY SHERLOCK

SHARE

ADJUST

[redacted] teacher who an arbitrator found was falsely accused of sexually abusing a student has filed a lawsuit in the Supreme Court of British Columbia seeking damages against an investigator into the accusations.

A student had accused the teacher of raping her repeatedly from the time she was in Grade 5 to the time she was in Grade 8. She said he

We have seen doxing enter our schools on multiple occasions. One case was when a teacher was falsely accused of sexual abuse. The most significant piece of evidence against him was multiple screenshots of Facebook direct messages between him and the student. They included very harsh language, like the scenes described in the article. When interviewed, the student claimed she was brought over to the teacher's house on multiple occasions. She was able to describe what the house looked like, what paintings were on the walls, and where the bedroom was. While working with the district, she shared copies of the direct messages. The student had originally claimed she had deleted them and only had screenshots. Upon reviewing the screenshots, our threat analysts noticed that some of the colors appeared different and the icons were in different places. After re-creating the chats through Facebook, they found that they looked different, and after searching the internet, they found that the chats might have been falsified and created with a social media post generator. Moreover, upon using Boolean Search Operators to search the teacher's name, our analysts found that his house was up for sale on a real-estate website, which included a "virtual walkthrough" of the house. This walkthrough included what the house looked like, what paintings were on the walls, and where the bedroom was. When presented with the findings, the student confessed to falsifying the claim.

Unfortunately, this isn't an isolated case. When an educator or anyone with a large social media footprint becomes the subject of public scrutiny, there will always be those willing to dig up personal information using all of the techniques we are showing.

Boston Marathon Bombing

On April 15th, 2013, two bombs went off near the finish line during the Boston Marathon. Later that evening, grainy photos of two male suspects aired on live television.

The Reddit community, which proved to be helpful in uncovering information during the Aurora, Colorado movie theatre shooting, started a thread regarding the suspects. Members began hunting for similar-looking suspects online, trying to find answers from the comfort of their computer chairs.

Within minutes, brands worn by the bombers were correctly identified on Reddit and 4chan. One user stumbled upon the Tripathi family's Facebook page for Sunil Tripathi, a student missing from Brown University. Sunil's photo was copied and pasted next to a photo of the youngest bombing suspect and posted to Reddit. Misinformation and speculation spiraled out of control. The Reddit and 4chan communities believed the rumors that Sunil was responsible for the bombing. Nasty comments continued to invade Sunil's Facebook page and later that night when an MIT police officer was shot and killed by the real bombing suspects (Dzhokhar and Tamerlan Tsarnaev), the messages became too much for the Tripathi family. They took down the page, which only added fuel to the Reddit, 4chan, and X (Formerly known as Twitter) fire.

Photo courtesy of Smarty DNS.

According to the New York Times article, "Should Reddit Be Blamed for the Spreading of a Smear" by Jay Caspian Kang,[3] this was the sequence of events:

"At midnight, [BuzzFeed Senior Sportswriter Erik] Malinowski, whose [X] following includes a number of journalists, tweeted: 'FYI: a Facebook group dedicated to finding Sunil Tripathi, the missing Brown student, was deleted this evening.' Roughly 300 [X] users retweeted Malinowski's post, including the pop-culture blogger Perez Hilton, who

[3] https://www.nytimes.com/2013/07/28/magazine/should-reddit-be-blamed-for-the-spreading-of-a-smear.html

sent Sunil Tripathi's name out to his more than six million followers.

…The next multiplier came from Andrew Kaczynski, another journalist at BuzzFeed, who sent out the police-scanner misinformation to his 90,000 followers and quickly followed up with: "Wow Reddit was right about the missing Brown student per the police scanner. Suspect identified as Sunil Tripathi."

…The Internet fate of Sunil Tripathi was finally sealed minutes later when @YourAnonNews, a Twitter news feed connected to the hacker collective Anonymous, tweeted out Tripathi's name to the hundreds of thousands of people who follow the account. By 3 a.m., in many heavily trafficked corners of the Internet, it was accepted that Sunil Tripathi was Suspect No. 2, and Reddit had got there first.

It was a long evening for the Tripathi family. NBC's Pete Williams helped clear Sunil's name when he confirmed that the missing boy was not one of the two suspects at 5:16 AM. But the damage had already been done. Sunil's sister was called 58 times between 3 and 4:15 AM that day, Kang reports. The family told Kang it received "hundreds of threatening and anti-Islamic messages (though they are not Muslim)." Groups that had been working with the Tripathi family to find their son shied away, thinking he might still be one of the Boston bombers."

HOW DOES DOXING HAPPEN?

If we want to best ensure our digital privacy, we must understand that there are many ways to retrieve personal information online. An individual may not realize how many clues they give away when posting about their life, work, and leisure activities. Social media profiles that are open to the public are goldmines of data. Third-party data collectors, such as White Pages, also have a wealth of information which could include things like relatives, and past and current addresses.

If a person uses the same username and password on all the sites they access and one of those accounts gets compromised, that means all accounts connected to that person are compromised. These compromised accounts sit in many different databases that get passed around hacking communities. This makes it possible to break into personal accounts and obtain more knowledge. That's why using different strong passwords is critical – including the use of Two-Factor Authentication (2FA).

SWATTING

It's important to know that things like bomb threats have been around since the 1970s.[4] However, because technology has changed the way we communicate, it also changes how we deal with threats.

One of the more dangerous acts that pair with doxing is called "swatting". Swatting occurs when a call to 911 is made under false pretenses, such as hostage situations, bomb threats, or murders, to generate a response from emergency services like the SWAT team. Most swatting calls are made to another person's address and are done as a criminal harassment tactic.

One of the highest-profile swatting attacks occurred in 2017. This incident originated over a $1.50 wagered match in a Call of Duty game between two men named Casey Viner and Shane Gaskill. The two involved in the match took to X to air out their dispute. Gaskill provided his address to Viner in their DM's and said he "would be waiting". Viner took the address and paid a known swatter to fake a 911 call to the house. Unfortunately, Gaskill purposely gave out a different address. When the team arrived at the address, the man who stepped out was mistaken to be holding a gun. The man was shot once by officers and later pronounced dead at the hospital. The man who was killed was an innocent party who had no part in the initial dispute.[5]

While it is a rare occurrence, swatting is a dangerous and illegal practice that still occurs to this day.

[4] https://web.archive.org/web/20170202005754/https://www.ncjrs.gov/pdffiles1/Digitization/28883NCJRS.pdf

[5] https://www.justice.gov/usao-ks/pr/ohio-gamer-sentenced-deadly-swatting-case

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 chances of anything getting through would be minimized.

When you create passwords with combinations of letters and numbers that are unique for every one of your online accounts, you'll make it more difficult to unlock your identity – keeping your information safe and secure.

You should password-protect all your devices: computer, laptop, tablet, smartphone, etc. Anything that acts as a gateway between you and your personal information should have some sort of password.

What makes a strong password?

To protect your passwords online, 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 information (online banking, etc.).
- Do not share your passwords (however, it's important that parents know their child's passwords).
- Use a password manager such as keepassxc.org or lastpass.com.

Many people choose a password that's easy to remember such as an address, pet name, or special date. They then use it repeatedly for each account they create. This is not a digitally responsible practice as attackers try these first because they're pieces of information that are typically easy to obtain. Think for a moment… if someone was looking at your social media, could they guess your password?

We all know the challenge of trying to remember our password for a website or an app and it's easy to fall into habits 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 a child's name and their birthday.

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

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

- Password
- 12345
- 123456789
- qwerty
- qwertyuiop
- letmein
- abc123
- 111111

- welcome
- football

PASSWORD MANAGERS

The strongest passwords are often the hardest to remember — that's why things like password managers have been created. A password manager is a secure web-based, cloud-based, or app-based product on our devices that enables us to store passwords, making it easier to log in to our accounts by just remembering one. Some password managers store other sensitive information such as credit card information, addresses, and more.

iPhones have a password manager built-in called Passwords. The Password App can be accessed by Face ID or Touch ID to enter and save login information. This can be a great alternative to password managers.

Photo provided by 9to5Mac.

We often receive questions about password managers in web browsers like Safari or Google Chrome. Browser password managers are only as secure as the physical devices on which they exist. If the password on our computer is 12345 (tip: it shouldn't be!), then whoever is logged in can see the browser-stored passwords without any additional authentication.

Paid password managers also exist. Apps such as Dashlane and LastPass give us the ability to store passwords on the cloud. When passwords are stored on the cloud, you can still access the login information even if it is accessed on a different device.

TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) is a security process in which users provide two different authentication factors to verify themselves before they can log in. 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 a person's devices or online accounts because knowing the victim's password alone is not enough to pass the authentication check.

The user enters their username and password.	An authentication code is sent to the user's mobile device or email.	The user enters their authentication code to log into the application.

DOXING PRACTICES

It is surprising how easily an individual can dig up information on another individual. The larger the digital footprint, the easier it is to find information. Maybe you mention that you are traveling to Europe for the first time. A hacker now knows you don't live on that continent. You may make another post saying you've never visited Asia. Now this same hacker can determine that you don't live in Asia, either.

Someone may complain online about the high property taxes in their county. A hacker can now pinpoint the county they live in. If you think of your online activity as a trail of breadcrumbs, determined hackers can follow that trail until they know where you live, your age, gender, and race. Armed with this information, they can slowly determine your identity and follow your digital footprint.

PACKET SNIFFING

Experienced hackers rely on technology to glean clues about our identity. They may turn to a strategy known as packet sniffing. In this method, a doxer intercepts our internet data, looking for everything from passwords, credit card numbers, and bank account information to old emails that may contain personal information or contacts. Doxers accomplish this by connecting to an online network, cracking its security measures, and then snagging the data flowing in and out of the network. This method is typically used when you are accessing public Wi-Fi networks such as at a Starbucks, airport, library, etc. A quick way to check if the website we are visiting is secure is to find the icon to the immediate left of the URL — it should look like a lock. Once clicked, if it says "connection is secure," we can be sure that no one is intercepting our data. If it does not say "connection is secure" it does not necessarily mean that someone is looking at what we type. However, be careful what you are typing on the site just in case.

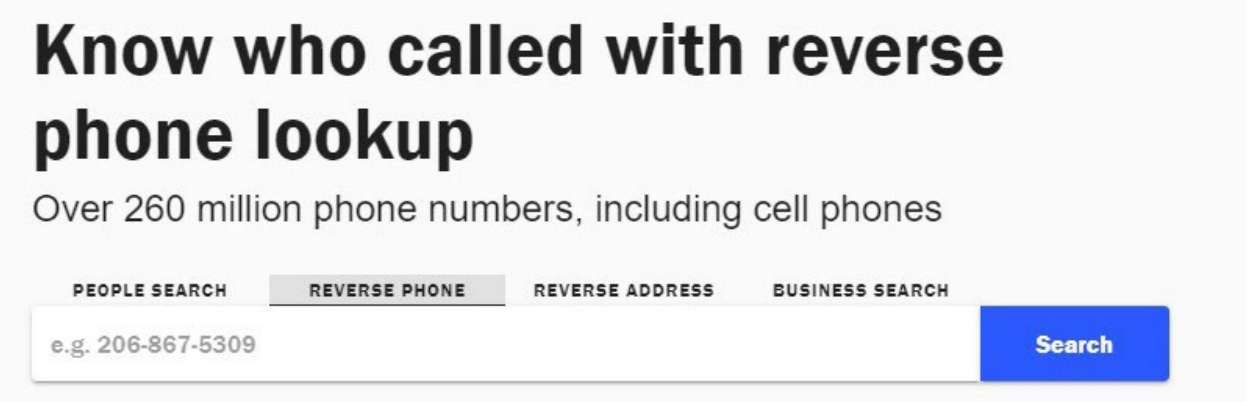
You can protect yourself from packet sniffing by using a Virtual Private Network (VPN). A VPN is an online tool that hides your IP address and encrypts your traffic.

IP LOGGING

Another way that doxers can grab personal information like location data is called IP logging. IP loggers attach a code–one that victims can't see–to an email message or link. Once victims open these emails, the code tracks their IP address and sends them back to the IP logger. From there, they can search the IP address to get a geolocation. This is often used as a tactic to scare individuals into giving up more personal information. The threat-maker will use either the city or location where someone lives, as a way to coax out more information from the victim.

REVERSE CELL PHONE LOOKUP

What can hackers learn about you if they have your cell phone number? Plenty. These reverse phone lookup services let you type in a cell phone number – or any telephone number – to uncover the identity of the person who owns the number. It's not just our names that people can discover from such a service: A search on White Pages may also turn up our current and previous addresses associated with our phone number. Doxers can also use a reverse phone lookup to search criminal and traffic records, financial records, and properties that someone may have owned.



Sites such as White Pages charge fees to provide anything beyond the city and state associated with a cell phone number. However, those willing to pay up can find plenty of personal information from a cell phone number. Be careful with your phone number. Do not post your phone number on social media sites, forums, or message boards.

SOCIAL MEDIA STALKING

Many doxers will look at multiple social media platforms to find private information about their targets. Not only do people willingly share personal information on sites such as X, Facebook, and Instagram (such as vacations, new jobs, and moves), but they also provide plenty of key factors about themselves when signing up for these sites – information that determined doxers may uncover. Consider Facebook: When you sign up for the site, you have the option to provide everything from your date of birth to your high school and college. You don't have to fill in these fields, in fact, you can leave them blank.

Another important thing to keep in mind is that you could have the most secure and private social media pages. However, you might have a friend/family member/co-worker who has all of their information set to public. If someone were to do a basic search of your name and see any of those related names and go to their social media, all of the posts and photos they have tagged you in are now visible.

PHISHING SCAMS

Phishing is one of the most common methods of cyber-crime. Despite how much we think scam emails are common knowledge, people still frequently fall victim.

Action Fraud reports receiving over 32 million reports of phishing emails, showing a rise of 44% from 2022 to 2023.[6] Email attacks are extremely common for the workplace. Here are some ways to identify if an email might be a phishing scam:

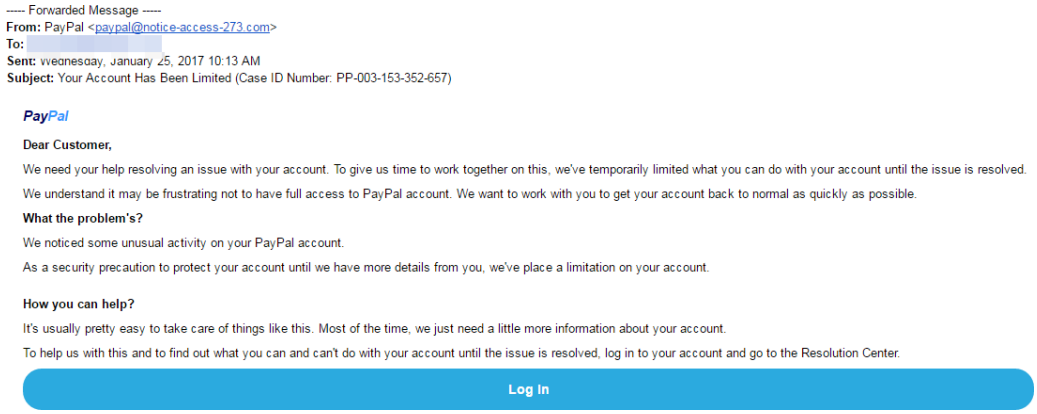
- The message is sent from a public email domain: Except for some smaller businesses, no organization will send emails from an address that ends in '@gmail.com'. Not even Google! For example, emails from Google will come from '@google.com' or Safer Schools Together will read '@saferschoolstogether.com'. If

[6] https://www.darkreading.com/endpoint-security/mimecast-redefines-phish-testing-and-training-with-safe-phish

the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. The best way to check an organization's domain name is to type the company's name into a search engine like Google.

Many of us don't ever look at the email address that a message has come from. Our email inbox displays a name, such as "Customer Support" and the subject line. When you open the email, you already know (or think you already know) who the message is from and jump straight into the content. When scammers create their fake email addresses, they often have the choice to select the display name, which doesn't have to relate to the email address at all. They can use a random email address that will turn up in your inbox with the display name "Google".

Let's look at this example of a phishing email mimicking PayPal:



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

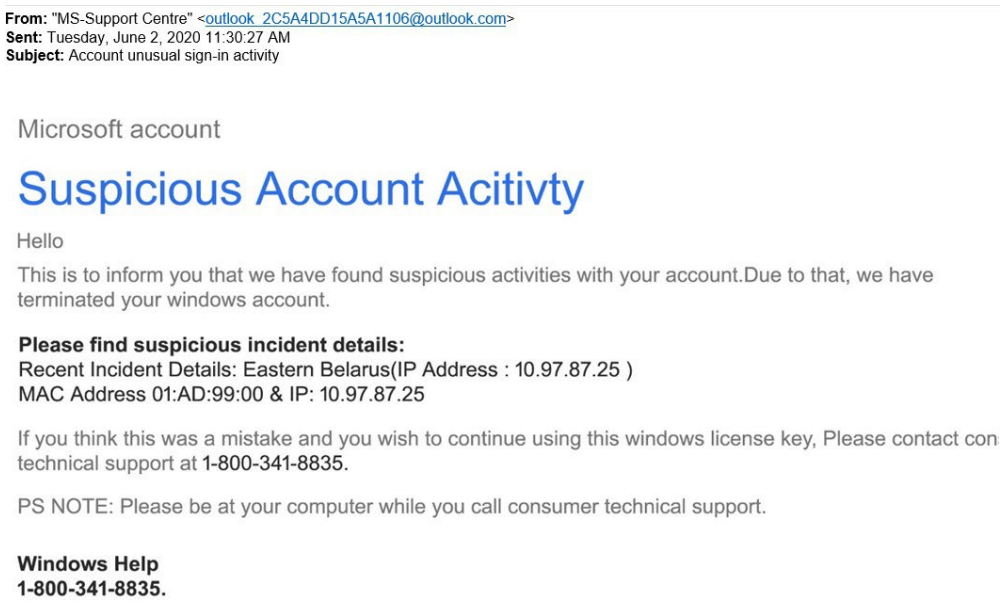
Log In

If we didn't already know this was a scam email, it would probably fool a lot of us. It uses PayPal's logo at the top of the message and is styled professionally.

As much as it tries to be a real email from PayPal, there's one huge red flag: the sender's email address is 'paypal@notice-access-273.com'. A real email from PayPal would have the organization's name in the domain name. The fact that PayPal isn't in the domain name is proof that this is a scam. Unfortunately, simply including PayPal anywhere in the message is often enough to trick people. They may glance at the company name in the email address and be satisfied or not catch onto the fact that the domain is different from the display name.

- The domain name is misspelled: there's another clue hidden in domain names that provide a strong indication of phishing. The problem is that anyone can buy a domain name. Although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed. Some scammers will buy domains of companies with slightly different spellings. For example, if the word "media" is in the domain, a scammer might buy "rnedia". At a quick glance, the r and n together look like an m.

  The email is poorly written: you can often tell if an email is a scam if it contains poor spelling and grammar. It is believed that these errors are made on purpose as part of a "filtering system". The theory is that if someone ignores clues about the way the message is written, they're less likely to pick up clues during the scammer's endgame.



From: "MS-Support Centre" <outlook_2C5A4DD15A5A1106@outlook.com>
Sent: Tuesday, June 2, 2020 11:30:27 AM
Subject: Account unusual sign-in activity

Microsoft account

Suspicious Account Acitivty

Hello

This is to inform you that we have found suspicious activities with your account.Due to that, we have terminated your windows account.

Please find suspicious incident details:
Recent Incident Details: Eastern Belarus(IP Address : 10.97.87.25)
MAC Address 01:AD:99:00 & IP: 10.97.87.25

If you think this was a mistake and you wish to continue using this windows license key, Please contact con technical support at 1-800-341-8835.

PS NOTE: Please be at your computer while you call consumer technical support.

Windows Help
1-800-341-8835.

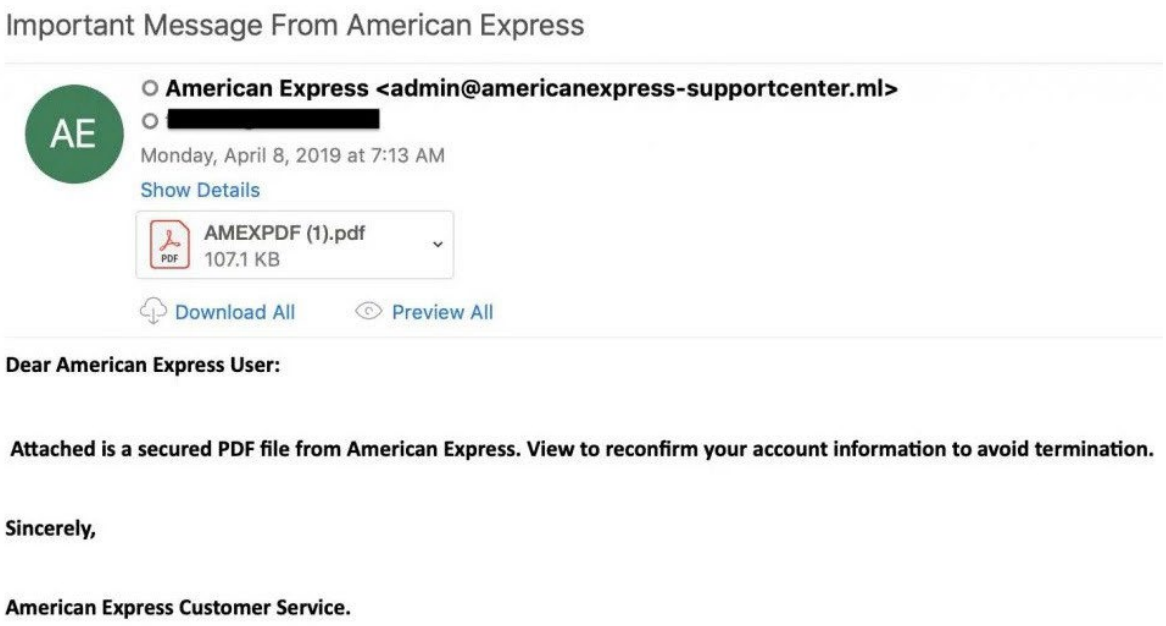
In this example, we can immediately see that the word “Acitivty” is misspelled in the header of the email. If you look closer, the email body is full of grammatical errors such as “...your account.Due to that, we...”. There is also a randomly capitalized word in the final paragraph.

Any supposedly official message that’s written this way is almost certainly a scam. With that being said, that’s not to say any email with a mistake in it is a scam. Everyone makes typos from time to time, especially when they’re in a hurry. It’s our responsibility to look at the context of the error and determine whether it’s a simple mistake or a potential scam. You can do this by asking:

- Is it a common sign of a typo?
- Is this email a template which should have been edited before being sent out?
- Is it consistent with previous messages you have received from this person?

If you are in any doubt, look for other clues listed here or contact the sender using another line of communication, whether that’s in person, by phone, via their website, an alternative email address, or through an instant message client.

- It includes suspicious attachments or links: phishing scams come in many forms – not just emails. Phishing scams can also come in the form of text messages, phone calls, or social media posts. No matter how phishing scams are delivered, some of them will contain a payload. This will either be an infected attachment that you are asked to download or a link to a fake website that does the same thing. The purpose of these payloads is to capture sensitive information such as login credentials, credit card details, phone numbers, and account numbers.



An infected attachment is a seemingly benign document that contains malware. In a typical example (such as the one above), the phisher claims to be sending an invoice. It doesn't matter whether the recipient expects to receive an invoice from this person or not because in most cases they won't be sure what the message pertains to until they open the attachment. When they open the attachment, they'll see that the invoice isn't intended for them, but it will be too late once opened, the document unleashes malware on the victim's computer, which could perform any number of nefarious activities. We advise never to open an attachment unless there is full confidence that the message is from a legitimate party.

For example, if you receive a pop-up warning about the file's legitimacy or the application asks you to adjust your settings, don't proceed. Contact the sender through an alternative means of communication and ask them to verify that it's legitimate.

- **The message creates a sense of urgency:** Scammers know that most of us procrastinate. You receive an email giving us important news and you decide you'll deal with it later. The longer you think about something, the more likely you are to notice things that don't seem right. Maybe you realize that the organization doesn't usually contact you by that email address, or you speak to a colleague and learn that they didn't send you a document. Even if you don't get that 'a-ha' moment, coming back to the message with a fresh set of eyes may help reveal its true nature. That's why so many scams request that you act now or else it will be "too late".

  PayPal, Microsoft, Apple, and Netflix all provide services that are regularly used, and any problems with those accounts could cause immediate inconveniences to the average person. The manufactured sense of urgency is equally effective in workplace scams. Scammers know that you're likely to drop everything if your boss emails you with a vital request, especially when other senior colleagues are supposedly waiting on you.

QUICK RESPOND?

TC

Theresa Campbell <sssmark797@gmail.com>

To Jackie Cao

You forwarded this message on 2021-07-27 10:36 AM.

--

Hello Jackie

I need you to handle a short but urgent task, Reply with your whatsapp number .
Regards.

Sent from my Ipad.

Phishing scams like this are particularly dangerous because even if the recipient did suspect foul play, they may be too afraid to confront their boss. After all, if they are wrong, they're essentially implying that there was something unprofessional about the boss's request. Looking at this example, this is a scam email sent to our newest employee at the time from the CEO of Safer Schools Together. Thankfully, the email was deleted and we did not reply. Organizations that value cyber security would accept that it's better to be safe than sorry.

OVERSHARING

Though the result is the same, people overshare on social media in various ways — such as:

- Posting intimate details about your relationships, friendships, family matters, or personal drama.
- Using social media as a soapbox or a way to vent.
- Posting photos or videos of things meant to be private.
- Posting embarrassing photos or videos of yourself or others.
- Regularly posting meals.
- "Checking In" to everywhere you go.
- Posting about whatever you are doing at a given moment, multiple times a day.
- Sharing too much information and photos of your children.

Why do we overshare? Social media encourages it. Social media sites invite users to share everything about their personal lives. It's easy to post a status update, a photo, an event, or a "check-in" with the click of a button. Unfortunately, this can lead to an anxious feeling called "FOMO" (fear of missing out) because of how addicting it is to share information with others online. FOMO is a lingering feeling that people are doing things without you or that things are passing you by. Social media profiles can give the impression that other people's lives are much better than yours. Online platforms let you in on the intimate details of others' lives. You may login and see a friend's vacation photos and wonder why your life is so boring in comparison. This can lead to insecurities in your own life. Some may be tempted to share their own "highlights" whenever they can to one-up their peers and look "interesting".

By oversharing, you are allowing yourself to become your own biggest security risk. You are willingly giving people on the internet information about you — which could lead to a cyber-attack or a real-life physical attack.

REMOTE LEARNING

Nearly 49% of students have taken some form of online learning.[7] It's important to know that personal information in your remote learning environments, including (but not limited to) your workspaces, backgrounds, and family members, can become pieces of information that you may not realize you are giving out.

[7] Online Learning Statistics That You Must Know in 2024

GOOGLE SEARCHING

Have you ever searched your name on Google? How about your address? Your phone number? Your social media handles? You're either nodding your head yes, saying something along the lines of, "of course I've Googled myself before, I want to know what is out there about me!", or you're shaking your head no, thinking something along the lines of, "I've never thought about doing that - why would I do that?". Either way, finding out information that is available to the world-wide web about yourself is an important step in ensuring your digital privacy. By using Google search techniques, you can uncover information about yourself that you may not have known exists. It's important to be aware of what the Internet knows about you.

How to Google Yourself Using Boolean Search Operators

Enter your first and last name into the Google search bar. You will see thousands, or potentially millions of results. You need to utilize Boolean Search Operators in order to narrow your search.

Boolean Search Operator Method #1 - Quotation Marks:

Quotation marks are used when you are searching for a specific word combination or an exact phrase. In Boolean searches, use quotation marks whenever your keyword consists of more than a single word. Return to your search result from above and add quotation marks around your first and last name; this will tell Google to only pull results that contain your first name and last name together. You should now see your search results narrowed down.

Not only is this method simple and effective for searching your first and last name, but quotation marks can be utilized for other searches such as phone numbers, addresses, and social media usernames.

Conducting a Google background check on yourself can be helpful in ensuring your digital privacy and safety. Furthermore, if you conduct searches on your spouse or children, you could also ensure their digital privacy by unveiling potential additional information about yourselves.

Boolean Search Operator Method #2 - NOT:

How can you narrow down your searches even further? The second Boolean Search Operator we will introduce you to is the “NOT” operator, which is reflected by the minus symbol on your keyboard. Although Google may be pulling the right information, if you find there are still too many results, you can include the NOT operator.

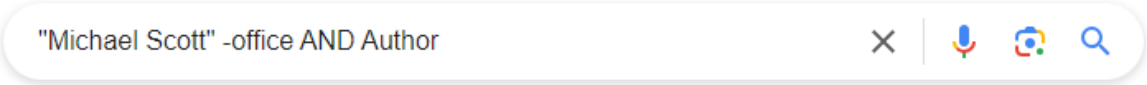
Perhaps in your results, you see there is someone with the same name as you who is a lawyer or a hockey player. To exclude the results related to them, you can go back to the search string and type in -lawyer or -hockey. This will tell Google to exclude any search results that contain the words “lawyer” and/or “hockey”.

If you Google yourself and find that someone with the same name has a different profession or lives in a different area, you can exclude that word from the search by using the NOT operator to ensure it doesn’t show up in your search results.

Boolean Search Operator Method #3 - AND:

The “AND” Boolean Search Operator, is used to tell the search engine to pull records containing all the terms, or specific terms, used in your search. For example, if you worked for Safer Schools Together, you could include that information in your search by adding AND ”Safer Schools Together”. Since Safer Schools Together consists of multiple words, you must add the quotation marks around it in order to group the words together. Otherwise, if you only searched AND Safer Schools Together, Google would read that only as adding the term ‘Safer’.

This can be a very powerful search tool to narrow down your search results. Take some time to utilize this operator and find out what search string works best for you. Try searching your name with your city, school, spouse’s name, etc., and take note of what works best.



GOOGLE ALERTS

Google Alerts can help keep you up to date by alerting you via email if/when new results regarding your search arise. The good news is that any one of our Boolean search operators will work as a Google Alert. That way, you only need to initiate one search and Google will send you any new updates.

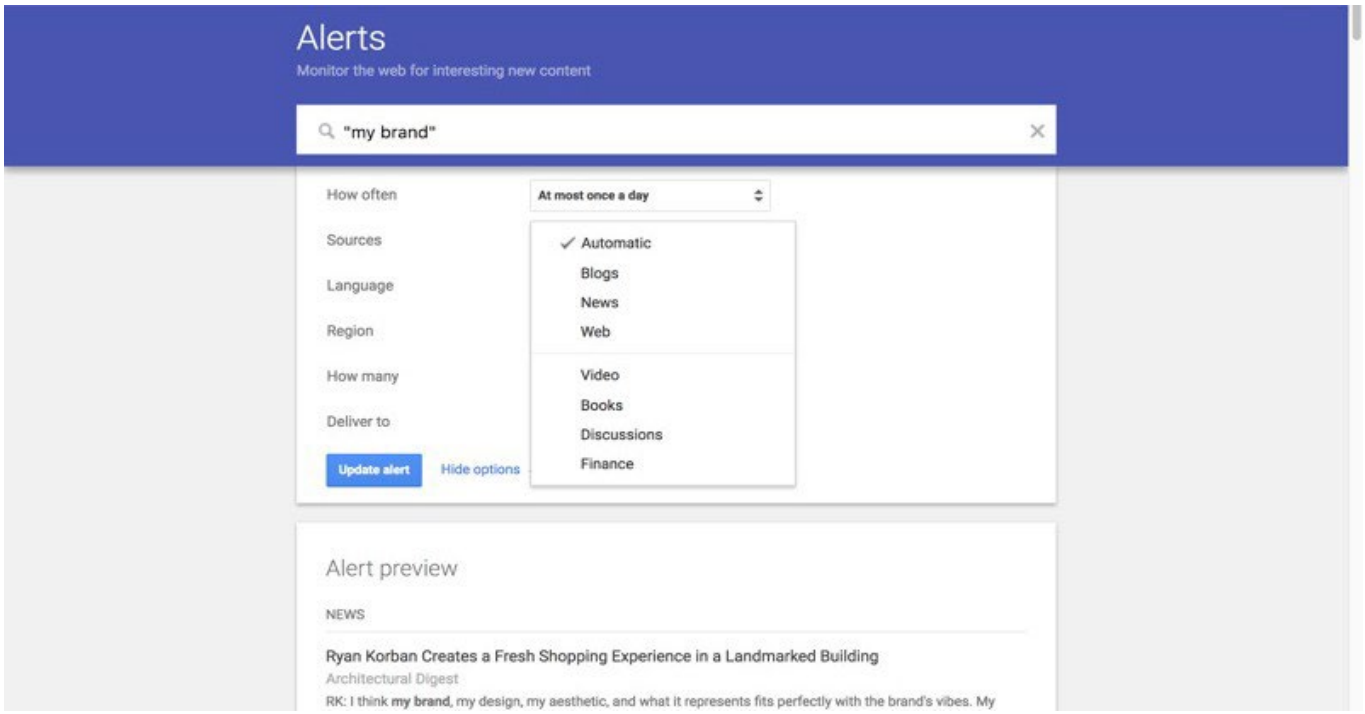


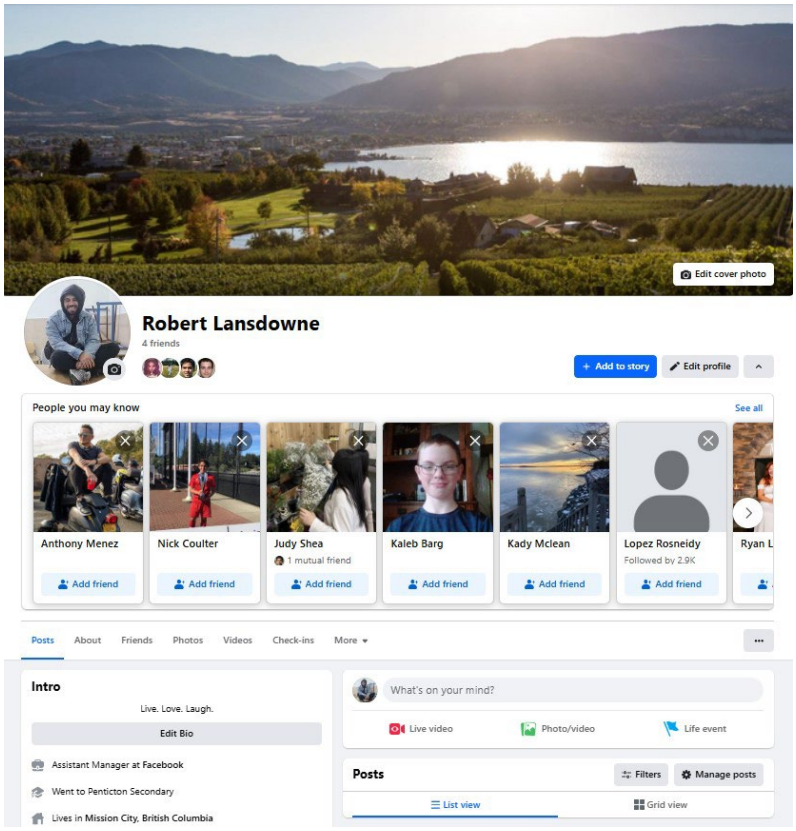
Photo courtesy of Mention.com.

PRIVACY SETTINGS

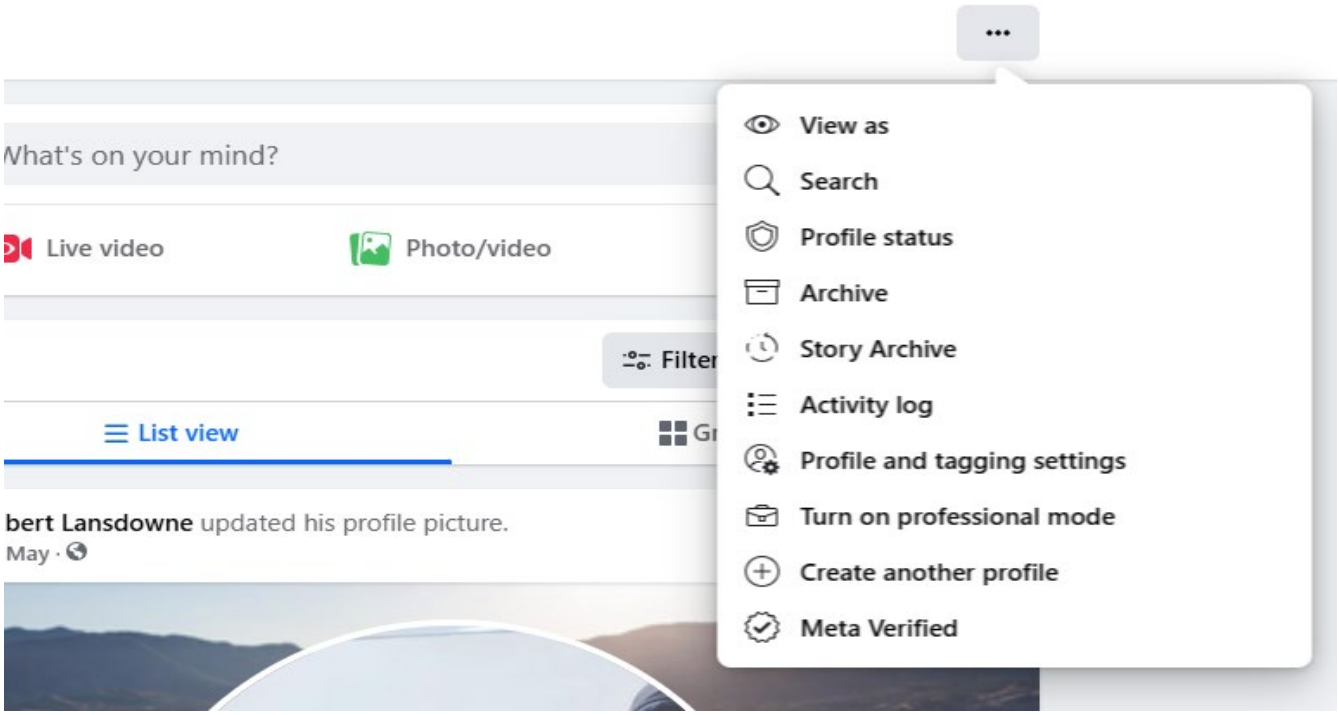
The privacy settings in your social media accounts that determine who can see your posts, like or comment on your photos, and send you friend requests are all commonly overlooked when setting up new accounts on social media. The good news is that you can still take control of those privacy settings at a later time, regardless of when you created your accounts.

Facebook

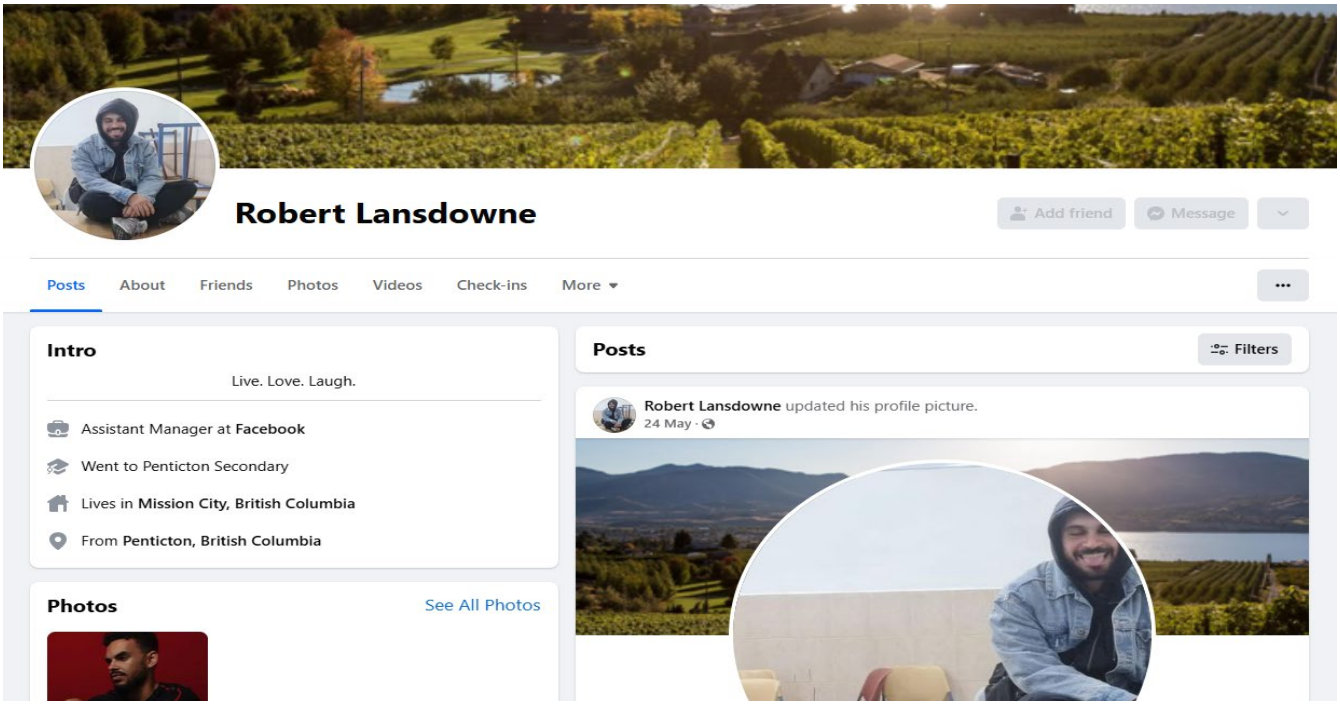
Here is an example of a Facebook page from the view of the account owner:



On this Facebook profile page, there is visibility of friends, posts, statuses, likes, and more. However, this is not necessarily what the account looks like to others who aren't friends of the account owner. To see what the account looks like as someone who is not a friend of the account owner, click the three dots "…" and then click the button 'View As'.



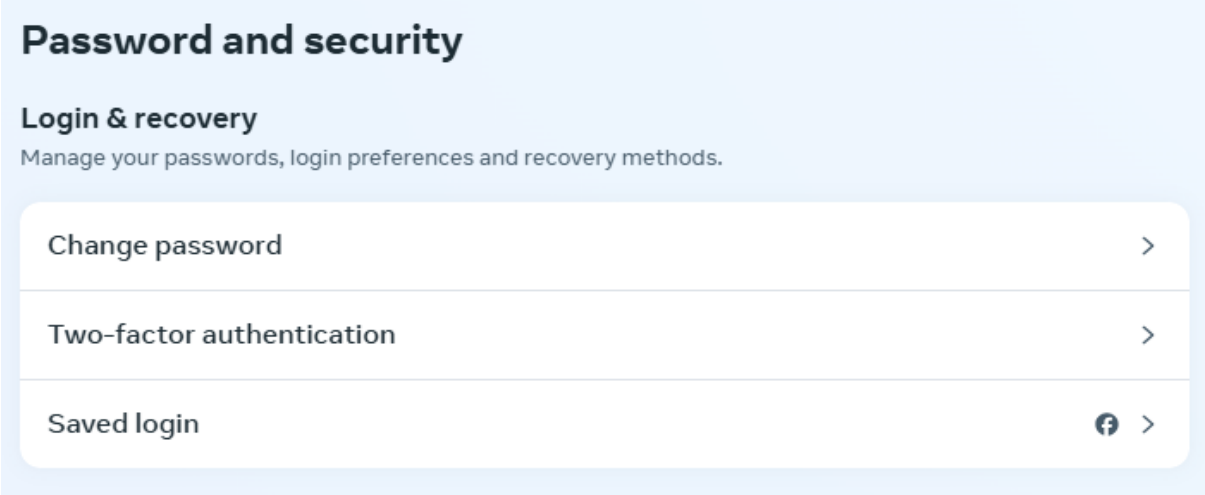
Now, you are able to view the profile as if you are someone who is not on your friends list on Facebook.



Clicking ‘View As’ can reveal things that you would prefer not to share. Here are the Facebook settings utilized to control and hide the information that you would like to keep private:

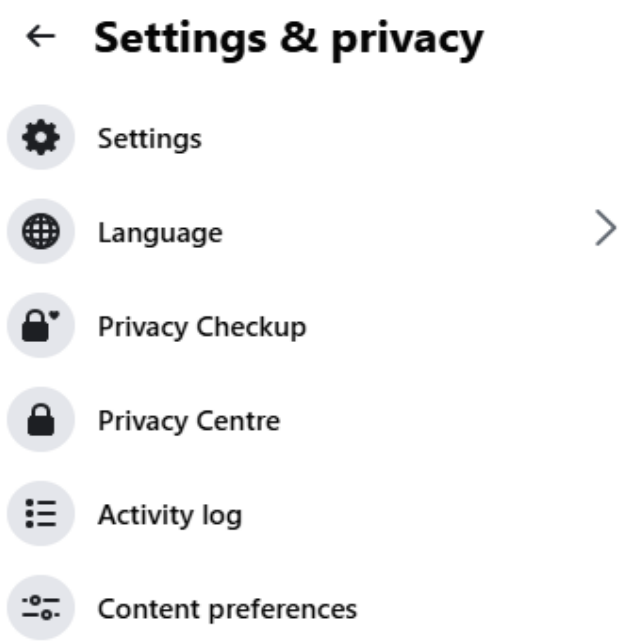
Security and Login

- Enable 2-Factor Authentication



Privacy

- Privacy Shortcuts
- Who Can See What You Share
- How To Keep Your Account Secure
- How People Can Find You On Facebook[8]
- Your Data Settings
- Your Ad Preferences

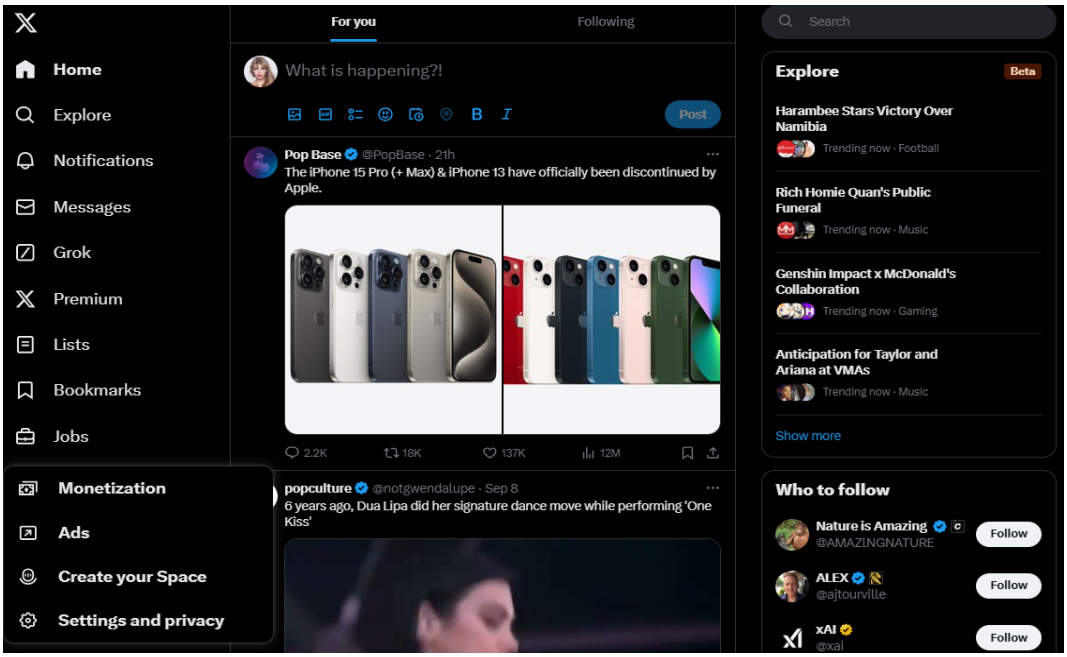


[8] This setting is often overlooked and very important. You can choose how people look you up on Facebook. Using the search bar, users can search your phone number or your email to find your account based on those pieces of information. You can control this setting by turning it off, so that people can only look up your profile by the name on your Facebook page.

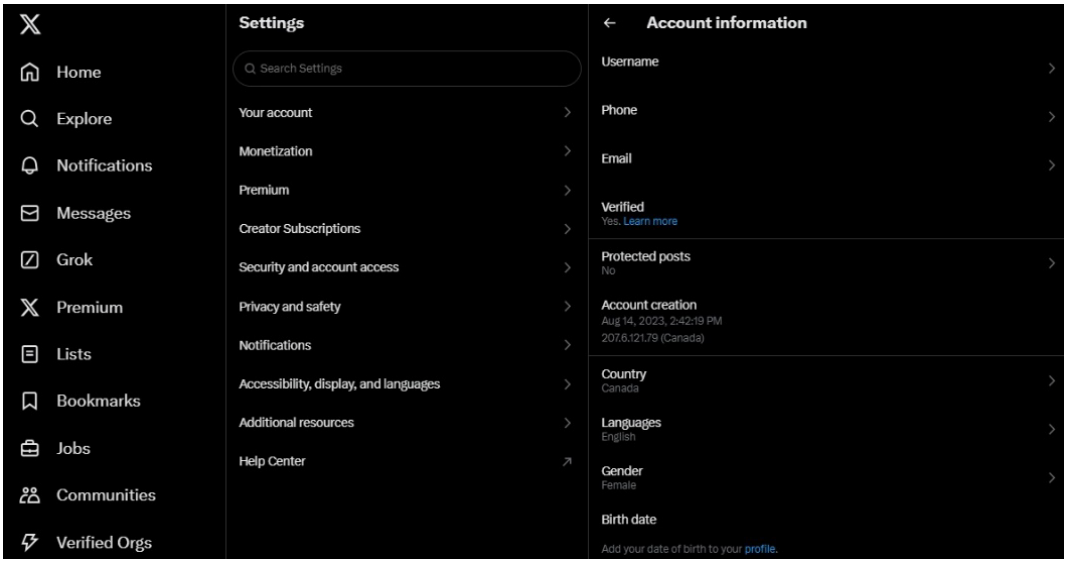
X (Formerly Known as Twitter)

X (Formerly known as Twitter) is a commonly used social media platform among educators. It is a great way for educators to communicate with each other, share ideas, and send information out publicly. The idea behind X is to share less personal information, but ask questions, and share ideas publicly. Because of this, there are settings that help ensure digital privacy beyond just making your accounts private:

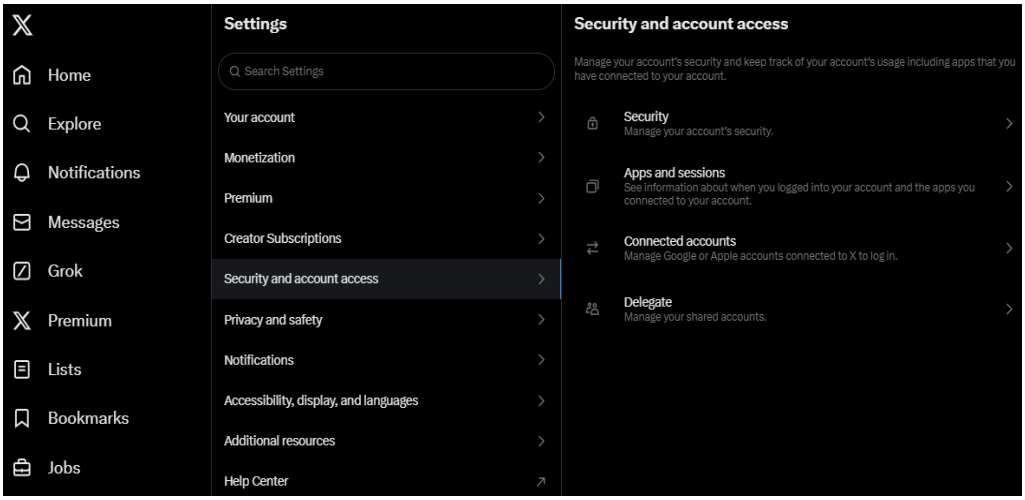
Settings and Privacy



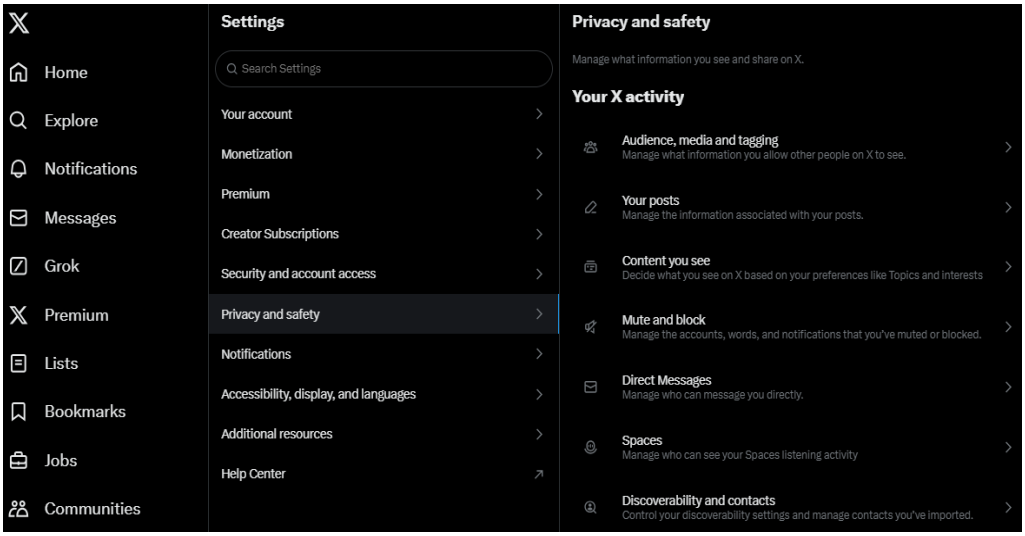
Your Account > Account Information > Protected Tweets



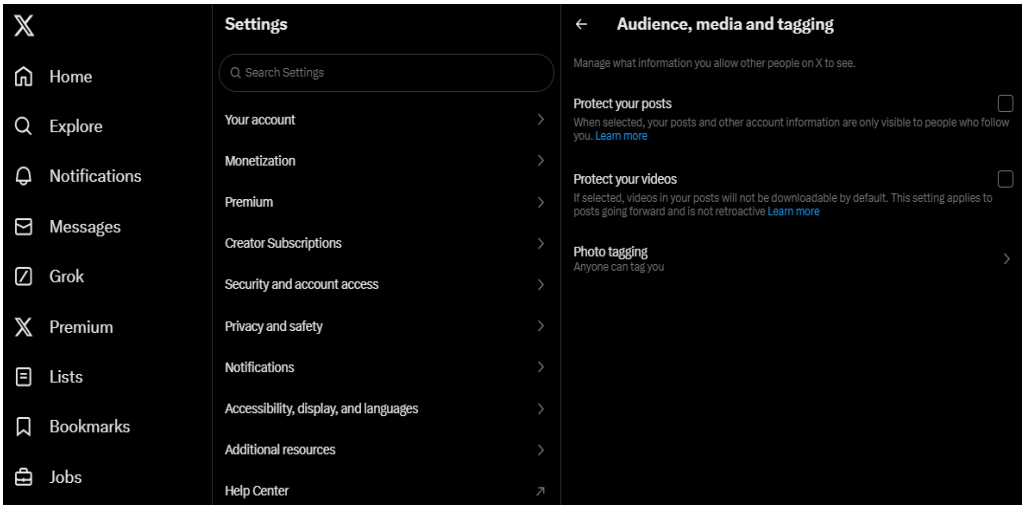
Security and Account Access



Privacy and Safety



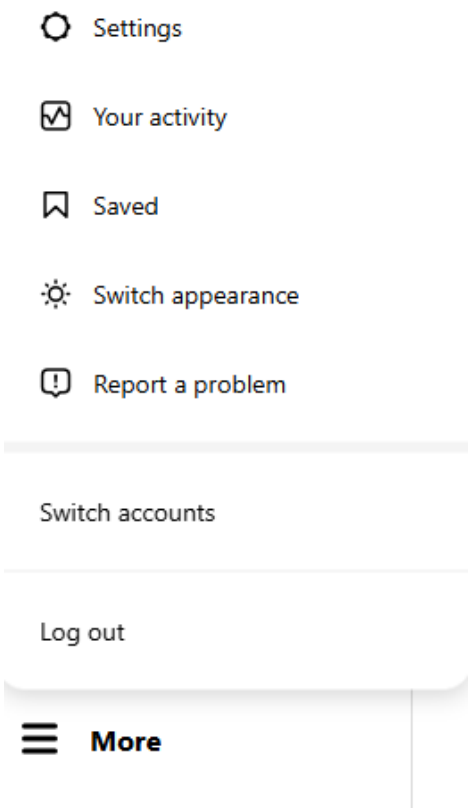
Audience and Tagging



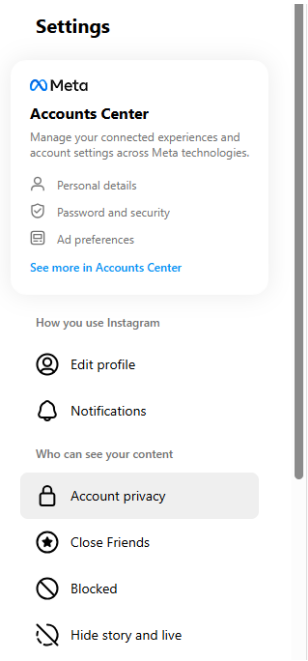
Instagram

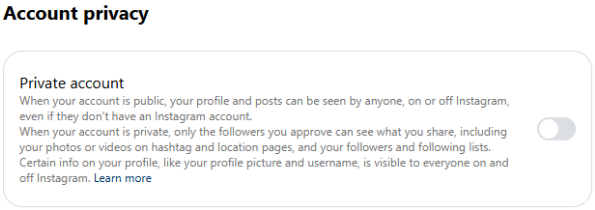
Instagram is a very commonly used social media platform among students. Safer Schools Together recommends students below the 11th grade keep their accounts private, whereas students in the 11th grade through college and their adult life may want to use their Instagram account as a portfolio to showcase their accomplishments to potential post-secondary institution recruiters or employers. Here is how you can make your Instagram accounts more secure:

More > Settings

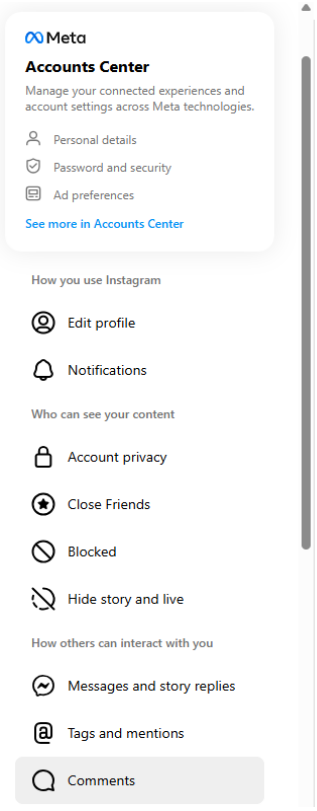


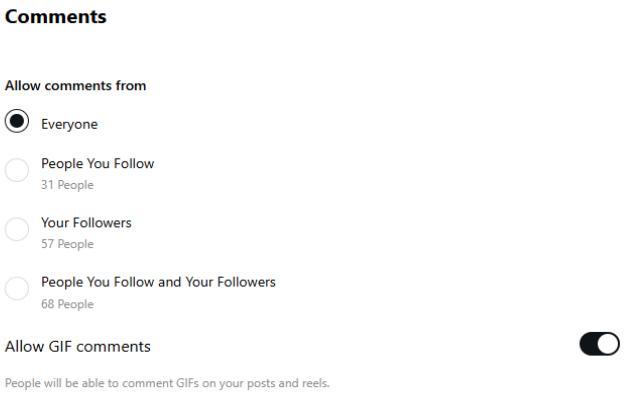
Account Privacy



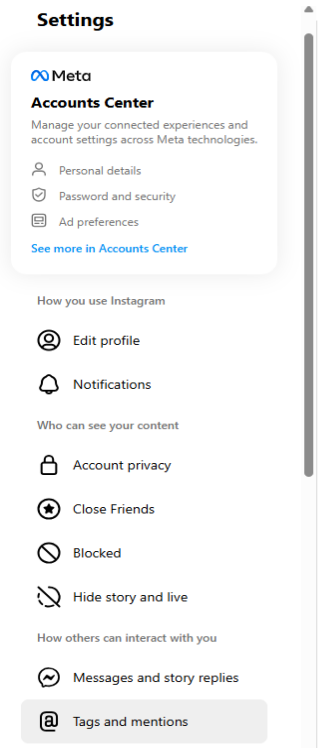


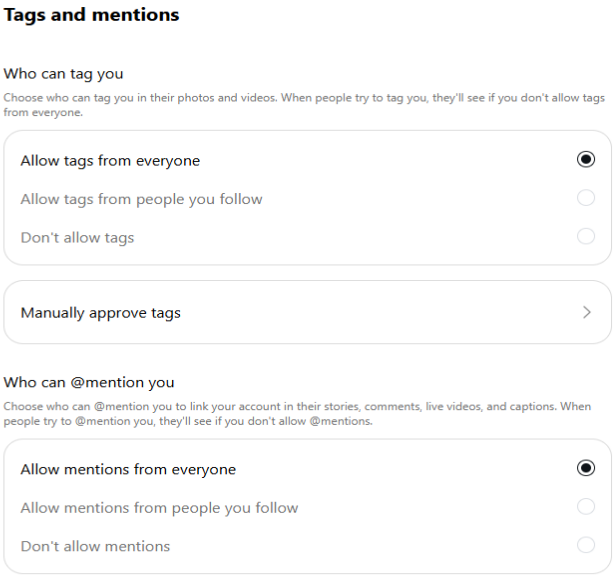
Comments



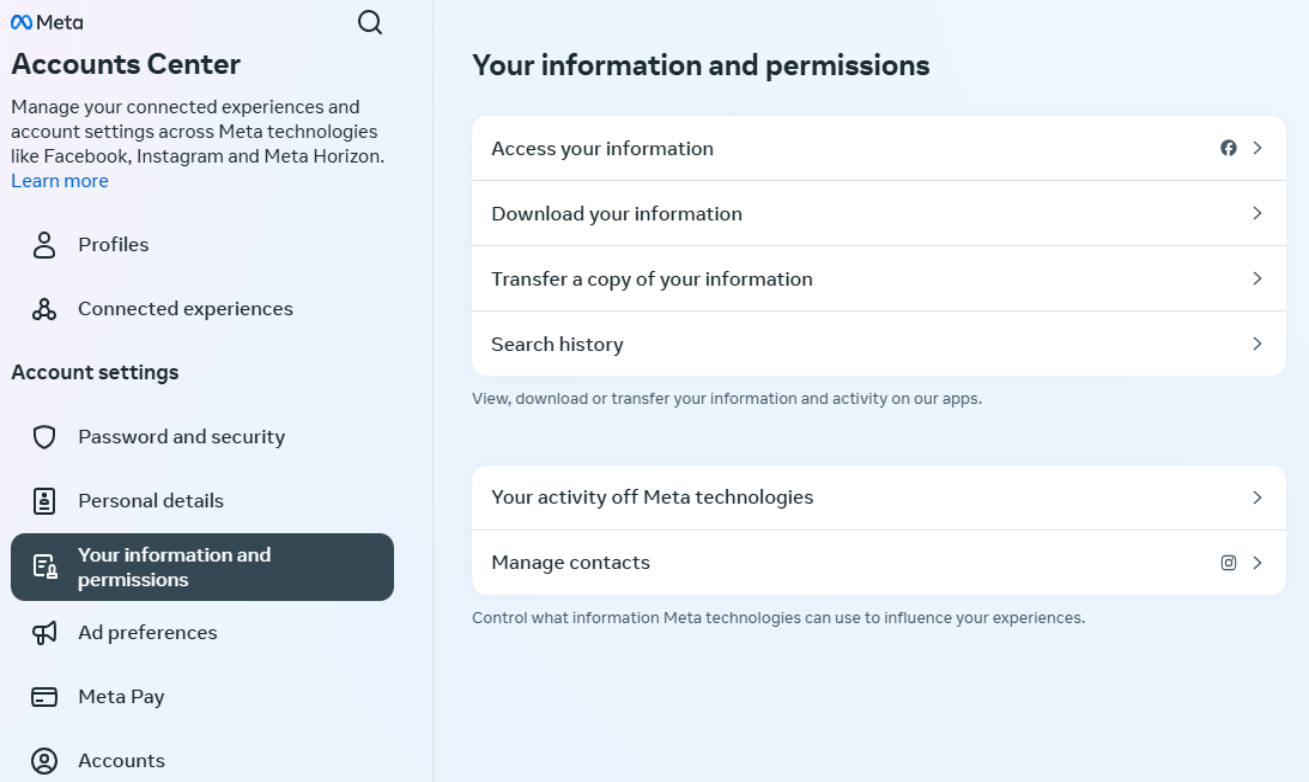


Tags and Mentions





Data Download



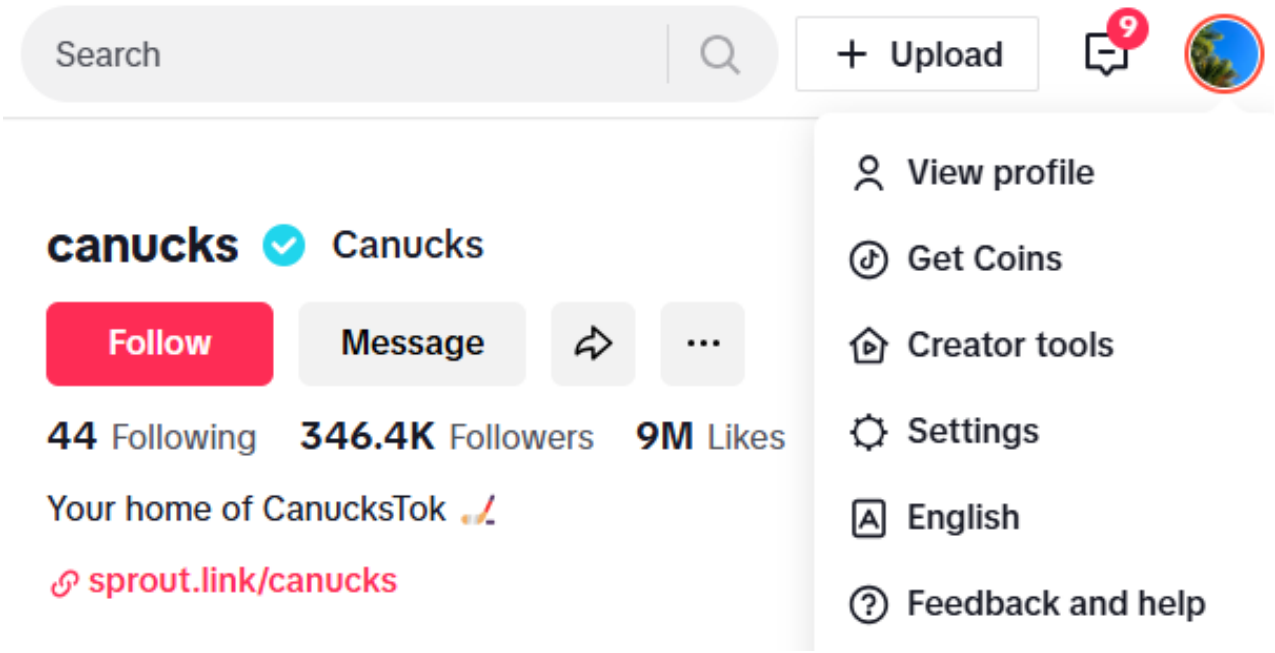
TikTok

You can learn more information regarding TikTok through the SST TikTok Micro Module. When conducting searches using TikTok, it is best practice to use the mobile application rather than the desktop application, as there are more search functions on the mobile version. As a newer platform, here is how you can ensure your TikTok accounts are secure:

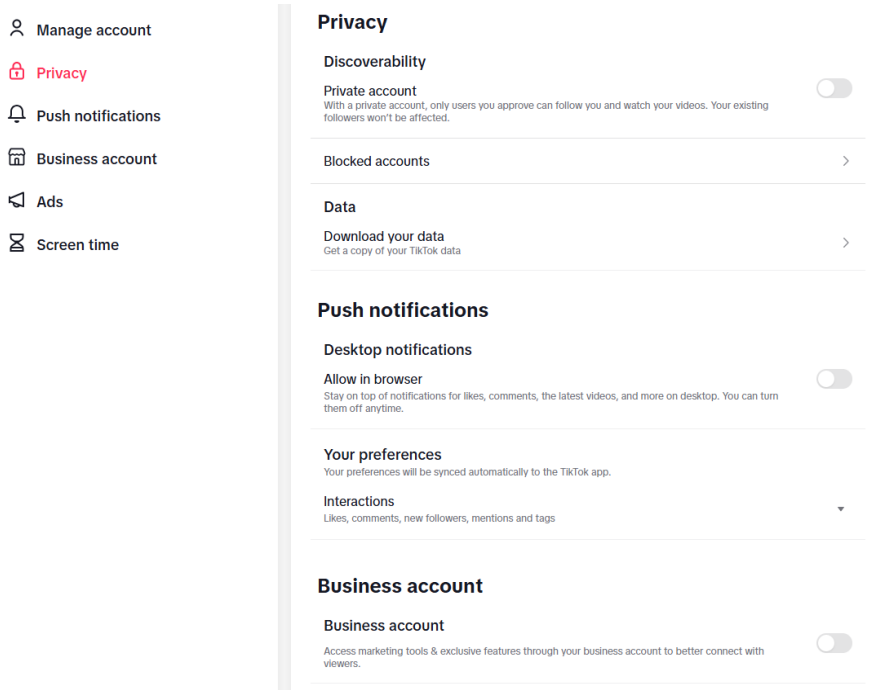
Privacy Settings

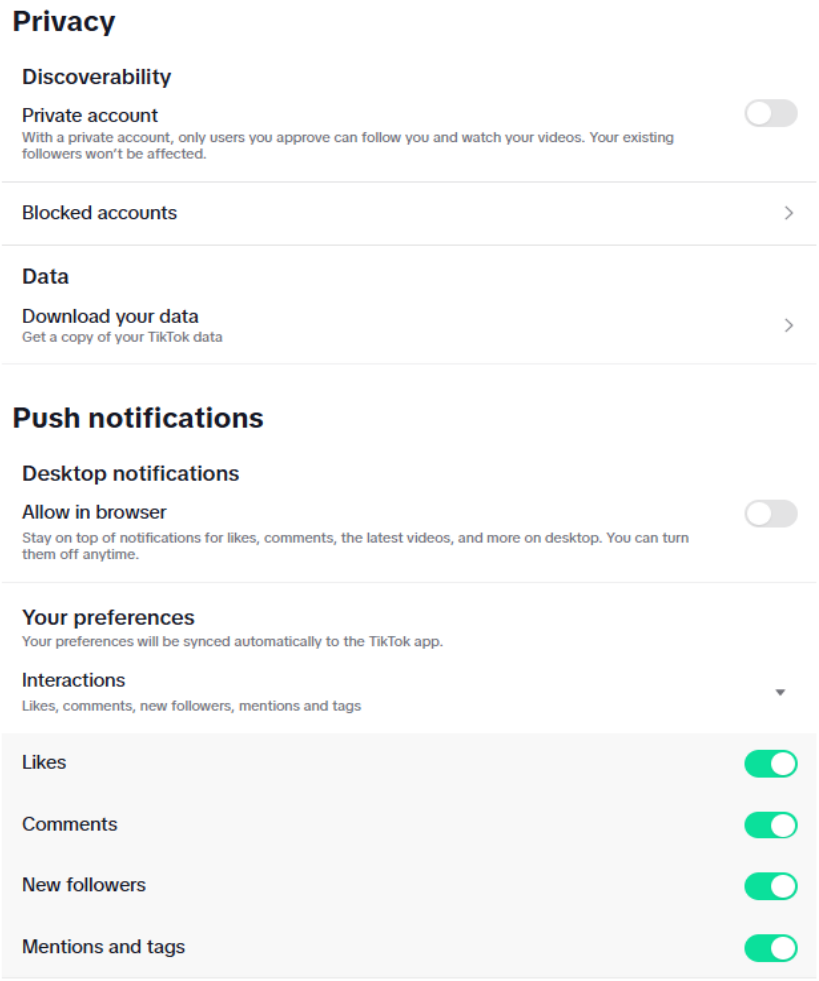
To access the Privacy Settings on mobile, go to your TikTok profile and click on the three lines at the top right. On the desktop version, right-click on your profile picture on the top right of the screen.

Here is where you can access your account and privacy settings similar to other social media platforms. Within your account settings, you have the ability to change and update information such as your phone number, email, and other personal information.



Next, go to the Privacy section, where you have the ability to decide whether or not you want your TikTok account to be private, and if you want TikTok to be able to suggest your account to others.


Manage account
Privacy
Push notifications
Business account
Ads
Screen time
Privacy
Discoverability
Private account
With a private account, only users you approve can follow you and watch your videos. Your existing followers won't be affected.
Blocked accounts
Data
Download your data
Get a copy of your TikTok data
Push notifications
Desktop notifications
Allow in browser
Stay on top of notifications for likes, comments, the latest videos, and more on desktop. You can turn them off anytime.
Your preferences
Your preferences will be synced automatically to the TikTok app.
Interactions
Likes, comments, new followers, mentions and tags
Business account
Business account
Access marketing tools & exclusive features through your business account to better connect with viewers.


Privacy
Discoverability
Private account
With a private account, only users you approve can follow you and watch your videos. Your existing followers won't be affected.
Blocked accounts
Data
Download your data
Get a copy of your TikTok data
Push notifications
Desktop notifications
Allow in browser
Stay on top of notifications for likes, comments, the latest videos, and more on desktop. You can turn them off anytime.
Your preferences
Your preferences will be synced automatically to the TikTok app.
Interactions
Likes, comments, new followers, mentions and tags
Likes
Comments
New followers
Mentions and tags

CONCLUSION

Ensuring your digital privacy is the first step to becoming a responsible digital citizen. Once equipped with the knowledge to keep ourselves safe online, we can help our students, colleagues, friends, and family members keep themselves safe as well.

ADDITIONAL RESOURCES

ICDTA®
International Center for
Digital Threat Assessment

International Center for Digital Threat Assessment® (ICDTA®)

SST | SAFER SCHOOLS TOGETHER

Safer Schools Together

SAFER
SCHOOLS
TOGETHER

International Center for
Digital Threat Assessment