Social Media Safety Tips

Things to consider if your social media profile is public:

Anyone and everyone can **see, save or screenshot the pictures**, images or comments that you are posting. This includes employers, colleagues, classmates, and anyone with possible ill intentions.

Don't use your full name and/or an image of your face for your profile picture and identification or include **revealing personal information** on the bio descriptor.

Avoid posting any pictures or videos of your neighborhood, places you frequent, school, place of employment, etc. as these can help someone to locate you. Post images after you have left the location or event: ***#latergram*** and **keep your geo-locator off**.

Is it necessary to have a **public account** for career growth, advocacy, political reasons, etc.?
Then consider having a public account that is focused on its purpose and separate from a private account where you can share your personal life.

Is it important that you have many followers?
Then consider **limiting the amount of personal information that you post** and review the above section on public profile accounts.

Things to consider if your social media profile is private:

Do you personally know everyone who follows you? **Have you met all of them in person**? If the answer is no to any one of these questions, then consider updating your lists and review them regularly.

Before allowing someone to follow you or to befriend you on social media, take look at their account to **verify that it is not fake** and to check whether you have friends in common.

More Tips:

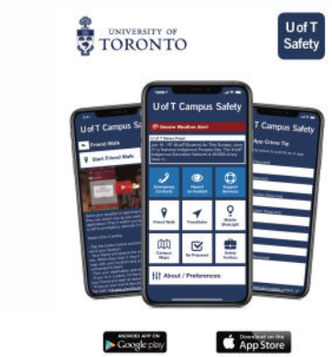
Download the U of T Campus Safety App

- 24/7 access to real-time alerts for safety-related incidents or campus closures
- Live chat with Campus Safety, connecting users with U of T safety staff in real-time
- Access TravelSafer: allowing Campus Safety to monitor a user's route when coming to or leaving from campus until reaching a destination
- Access Mobile Bluelight: when activated it sends the user's on-campus location to Campus
- Additional features — such as Friend Walk and Support Services — assist users anywhere in the world.

International Students:

For more information about different types of frauds and scams that often target international students, visit the Government of Canada's immigration website at:

https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html



The U of T Campus Safety App is available for free download at Google Play and the Apple Store.

Resources Available to Help You:

If you suspect that you have been targeted by a fraudster we encourage your to make a report to the ***Campus Safety*** Non-Emergency Lines (below).

- **UTM Campus Safety** - 905-828-5200
- **UTSC Campus Safety** - 416-287-7398
- **UTSG Campus Safety** - 416-978-2323

The ***Community Safety Office*** is available to consult with you on any situation that is causing you to be concerned for your safety or the safety of someone else. You can access support from this service by contacting: 416-978-1485 or community.safety@utoronto.ca.

UNIVERSITY OF TORONTO | Community Safety Office

Fraud Prevention Information & Support Options at U of T

www.communitysafety.utoronto.ca
community.safety@utoronto.ca
416-978-1485

Types of Fraud

Fraud Scheme 1: "Return to Sender"

1. The Victim receives an automated call from a delivery company about a package. It connects to a person claiming to work for a delivery company.
2. The Victim is "transferred" to the police and is then told a package addressed to them, containing illegal goods, has been intercepted.
3. The Victim is told they face arrest and deportation for their involvement. The Victim is told that they have an opportunity to pay a fine to avoid jail/ deportation.

Fraud Scheme 2: "Laundry Card"

1. The Victim receives a call from a person claiming to work for police.
2. The Victim is told that their bank card has been used in a money laundering scheme and their accounts are going to be locked.
3. The Victim is told they must help with the investigation to clear their name and are told to withdraw the money from their accounts and deposit it to a "secure system" via Bitcoin while the investigation continues.
4. The Victim is told this money will be returned at the end of the investigation.

Fraud Scheme 3: "Sextortion"

1. The Victim engages in seemingly harmless encounters over social media or through dating sites.
2. Eventually the perpetrator will coerce the victim into sending explicit images, getting naked on camera, or performing sexual acts while on camera.
3. The Victim is told the images will be shared (online, with family members, etc.) unless they send money to the perpetrator (or in some cases unless they send more images).
4. In some cases the Victim is coerced into going into hiding under threat of the images being shared and the Victim's family is contacted for "ransom".

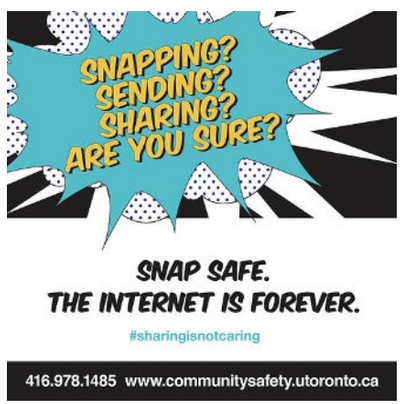
Other Scenarios?

- A call/email from someone posing as the legal department of Service Canada saying that there are charges that have been brought against you.
- A call/email from someone posing as a Service Canada representative indicating that your Social Insurance Number (SIN) has been blocked, compromised or suspended.
- Threats from a caller indicating that a warrant for your arrest is outstanding and will be executed if payment is not made immediately.
- Threats from a caller indicating that you will lose your visa or status or be deported from the country if payment is not made immediately.
- A call/email saying that your computer has been infected with a virus. The caller or sender will offer to remove the virus from your computer. The person will try to get your computer passwords and other private information
- A call/email saying that you won something, but you did not enter a contest. Do not enter any information and delete the text. If the text tells you to text "STOP" or "NO" so you don't get more texts, delete it. Do not reply. Scam artists do this to confirm they have a real phone number.

What Does Fraud Look Like? What Should I Do?

What if I am being contacted by someone trying to defraud me?

- Don't always trust your caller ID/call display on your phone. Scammers have ways to change call display to say things like "Police", when in fact they are not legitimate.
- Canadian Government Officials WILL NOT contact you directly and demand money in exchange for securing your Canadian status.
- The Canada Revenue Agency (CRA) or Service Canada will NEVER request a payment by e-transfer, online currency such as bitcoin or pre-paid credit cards.
- Government Officials won't ask you to secure your money by transferring it to them via online currency like bitcoin.
- If the CRA is sending you money it will be by direct deposit or by cheque in the mail.
- The Canadian Government DOES NOT accept payments via Western Union, Money transfer, prepaid Credit Cards or through wire transfers to a foreign country.
- The CRA or Government Officials will NEVER use aggressive language or threaten you with arrest or sending the Police.



Here is what to do when you receive these types of calls or contact:

- Be suspicious of anyone asking for money or personal information.
- DO NOT make a payment or provide your personal information. If you are suspicious, ask the caller for an employee number and hang up the phone. Look up the company online (e.g. CRA or IRCC) and call them to confirm whether the employee number provided by the caller and request is legitimate.
- Call Campus Safety to get support confirming the legitimacy of the caller.
- Report the incident to the Canadian Anti-Fraud Centre (https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm), Campus Safety or Toronto Police Services .

What if someone is threatening to publish or share intimate images of you?

- Do not be embarrassed. Consider making an appointment with the Community Safety Office to discuss your options.
- Consider making a report to Campus Safety or to Toronto Police Services.
- Regardless of whether you know the person who is threatening you or not – take a screenshot of their URL/Name/Email Address/handle.
- Save and copy all messages that have been sent to you. You may need this information when making a report to the police.
- Do not continue to respond or engage with the other person.
- Consider changing the password of your social media account and/or temporarily disabling or deactivating your account.