सोशल मीडिया सुरक्षा सुझाव

अगर आपकी सोशल मीडिया प्रोफ़ाइल सार्वजनिक है तो इन बातों का ध्यान रखें:

कोई भी और हर कोई आपके द्वारा पोस्ट की जा रही **तस्वीरों, छवियों या टिप्पणियों को देख सकता है, सहेज सकता है या स्क्रीनशॉट ले सकता है।** इसमें नियोक्ता, सहकर्मी, सहपाठी और संभावित गलत इरादे वाले सभी लोग शामिल होते हैं।

अपने प्रोफ़ाइल चित्र और पहचान के लिए अपना पूरा नाम और/या अपने चेहरे की छवि का उपयोग न करें या बायो डिस्क्रिप्टर पर **व्यक्तिगत जानकारी का खुलासा** न करें।

अपने आस-पड़ोस की तस्वीरें या वीडियो पोस्ट करने से बचें, जहां आप अक्सर आते-जाते हैं, स्कूल, रोज़गार की जगह, आदि क्योंकि इनसे आपको ढूंढ़ने में किसी को मदद मिल सकती है। स्थान या आयोजन छोड़ने के बाद चित्र पोस्ट करना: ***#latergram*** **और अपने जियो-लोकेटर** को बंद रखें।

क्या कॅरियर के विकास, हिमायत, राजनीतिक कारणों, आदि के लिए एक सार्वजनिक अकाउंट होना आवश्यक है? इसके बाद सार्वजनिक अकाउंट रखने पर विचार करें जो अपने उद्देश्य पर केंद्रित हो और ऐसा अकाउंट निजी खाते से अलग हो जहां आप अपना निजी जीवन साझा कर सकें।

क्या यह महत्वपूर्ण है कि आपके कई फ़ॉलोअर्स हों? इसके बाद **आपके द्वारा पोस्ट की जाने वाली व्यक्तिगत जानकारी की मात्रा को सीमित करने** और सार्वजनिक प्रोफ़ाइल वाले अकाउंट पर उपरोक्त खंड की समीक्षा करने पर विचार करें।

यदि आपकी सोशल मीडिया प्रोफ़ाइल निजी है, तो यह विचार करने योग्य बातें हैं:

क्या आप व्यक्तिगत रूप से उन सभी को जानते हैं जो आपको फॉलो करते हैं? क्या आप उन सभी से व्यक्तिगत रूप से मिले हैं? यदि इनमें से किसी भी प्रश्न का उत्तर नहीं में है, तो अपनी सूचियों को अद्यतन करने पर विचार करें और नियमित रूप से उनका पुनरावलोकन करें।

सोशल मीडिया पर किसी को आपको फ़ॉलो करने या आपसे मित्र बनने की अनुमति देने से पहले, इस बात को सत्यापित करने के लिए उनके अकाउंट को देखें कि **कहीं यह नकली तो नहीं है** और यह जांच लें कि क्या आपके मित्र समान हैं।

और सुझाव:

U of T Campus Safety ऐप का डाउनलोड करें

- सुरक्षा से संबंधित घटनाओं या परिसर के बंद होने के लिए 24/7 रियल-टाइम अलर्ट तक पहुंच
- Campus Safety के साथ लाइव चैट करें, यूज़र्स को U of T सेफ्टी स्टाफ़ से रियल-टाइम में कनेक्ट करें
- TravelSafer तक पहुंच: कैंपस सुरक्षा को एक गंतव्य तक पहुंचने तक कैंपस से आने या जाने पर उपयोगकर्ता के मार्ग की निगरानी करने की इजाजत देता है
- Access Mobile Bluelight: सक्रिय होने पर यह उपयोगकर्ता के ऑन-कैंपस स्थान को कैंपस में भेजता है
- अतिरिक्त सुविधाएं (फ़ीचर्स) — जैसे कि फ्रेंड वॉक और सपोर्ट सर्विसेज़ — दुनिया में कहीं भी उपयोगकर्ताओं की सहायता करती हैं।

अंतरराष्ट्रीय छात्र:

विभिन्न प्रकार की धोखाधड़ी और घोटालों के बारे में अधिक जानकारी के लिए जो अक्सर अंतरराष्ट्रीय छात्रों को लक्षित करते हैं, कनाडा सरकार की निम्न आव्रजन वेबसाइट पर जा सकते हैं:

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

U of T Campus Safety ऐप Google Play और Apple Store पर मुफ़्त डाउनलोड के लिए उपलब्ध है।

आपकी सहायता के लिए उपलब्ध संसाधन:

यदि आपको संदेह है कि आप पर कोई धोखेबाज़ नज़र रख रहा है, तो हम आपको ***कैंपस सुरक्षा*** गैर-आपातकालीन लाइन (नीचे दिए अनुसार) को इसके बारे में बताने के लिए प्रोत्साहित करते हैं।

- **UTM कैंपस सुरक्षा** - 905-828-5200
- **UTSC कैंपस सुरक्षा** - 416-287-7398
- **UTSG कैंपस सुरक्षा** - 416-978-2323

Community Safety Office ऐसी किसी भी स्थिति पर आपसे परामर्श करने के लिए उपलब्ध है जिसके कारण आप अपनी सुरक्षा या किसी और की सुरक्षा के लिए चिंतित हैं। आप इस सेवा से सहायता प्राप्त करने के लिए: 416-978-1485 पर फ़ोन करके या Community.safety@utoronto.ca पर ईमेल करके संपर्क कर सकते हैं।

UNIVERSITY OF TORONTO | Community Safety Office

U of T पर धोखाधड़ी रोकथाम सूचना और सहायता विकल्प

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

धोखाधड़ी के प्रकार

धोखाधड़ी योजना 1: "प्रेषक पर वापस आएं"

1. पीड़ित को किसी डिलीवरी कंपनी से एक पैकेज के बारे में एक स्वचालित कॉल मिलती है। यह एक डिलीवरी कंपनी के लिए काम करने का दावा करने वाले व्यक्ति से साथ जुड़ता है।
2. पीड़ित को पुलिस को "हस्तांतरित" कर दिया जाता है और फिर उसे बताया जाता है कि उसे संबोधित एक पैकेज, जिसमें अवैध सामान था, को इंटरसेप्ट किया गया है।
3. पीड़ित को बताया जाता है कि उनकी संलिप्तता के लिए उन्हें गिरफ्तारी और निर्वासन का सामना करना पड़ रहा है। पीड़ित को बताया जाता है कि उनके पास जेल/निर्वासन से बचने के लिए जुर्माना भरने का अवसर है।

धोखाधड़ी योजना 2: "लॉन्ड्री कार्ड"

1. पीड़ित को पुलिस में काम करने का दावा करने वाले एक व्यक्ति का फ़ोन आता है।
2. पीड़ित को बताया जाता है कि उनके बैंक कार्ड का इस्तेमाल मनी लॉन्ड्रिंग योजना में किया गया है और उनके खाते लॉक होने जा रहे हैं।
3. पीड़ित से कहा जाता है कि उन्हें अपना नाम हटाने के लिए जांच में मदद करनी चाहिए और कहा जाता है कि वे अपने खातों से पैसे निकाल लें और जांच जारी रहने के दौरान बिटकॉइन के माध्यम से इसे "सुरक्षित प्रणाली" में जमा करें।
4. पीड़ित को बताया जाता है कि जांच के अंत में यह पैसा वापस कर दिया जाएगा।

धोखाधड़ी योजना 3: "सेक्सटॉर्शन"

1. पीड़ित सोशल मीडिया या डेटिंग साइटों के माध्यम से हानिरहित लगने वाली घटनाओं में शामिल होता है।
2. अंततः अपराधी पीड़ित को अश्लील तस्वीरें भेजने, कैमरे पर नग्न होने, या कैमरे पर यौन क्रिया करने के लिए मज़बूर करेगा।
3. पीड़ित को बताया जाता है कि तस्वीरें साझा की जाएंगी (ऑनलाइन, परिवार के सदस्यों के साथ, आदि) जब तक वे अपराधी को पैसे नहीं भेजते (या कुछ मामलों में जब तक कि वे अधिक चित्र नहीं भेजते)।
4. कुछ मामलों में छवियों को साझा किए जाने की धमकी के तहत पीड़ित को छिपने के लिए मज़बूर किया जाता है और पीड़ित के परिवार से "फिरौती" के लिए संपर्क किया जाता है।

अन्य परिदृश्य?

- Service Canada के कानूनी विभाग के भेष में किसी व्यक्ति का कॉल/ईमेल आता है जिसमें यह कहा जाता है कि आपके खिलाफ़ आरोप लगाए गए हैं।
- Service Canada के प्रतिनिधि के रूप में किसी व्यक्ति का कॉल/ईमेल यह दर्शाता है कि आपके सामाजिक बीमा नंबर (SIN) को अवरुद्ध कर दिया गया है, इससे छेड़छाड़ की गई है या निलंबित कर दिया गया है।
- कॉल करने वाले की ओर से धमकी जिसमें यह संकेत दिया गया है कि आपकी गिरफ़्तारी का वारंट शेष है और अगर तुरंत भुगतान नहीं किया गया तो उसे निष्पादित कर दिया जाएगा।
- कॉल करने वाले की ओर से धमकी जिसमें यह संकेत दिया गया है कि यदि भुगतान तुरंत नहीं किया जाता है तो आप अपना वीज़ा या स्टेटस खो देंगे या देश से निर्वासित कर दिए जाएंगे।
- एक कॉल/ईमेल जिसमें कहा जाता है कि आपका कंप्यूटर वायरस से संक्रमित हो गया है। कॉल करने वाला या प्रेषक आपके कंप्यूटर से वायरस को हटाने की पेशकश करेगा। वह व्यक्ति आपके कंप्यूटर के पासवर्ड और अन्य निजी जानकारी लेने का प्रयास करेगा
- एक कॉल/ईमेल में कहा जा रहा है कि आपने कुछ जीता है, लेकिन आपने प्रतियोगिता में प्रवेश नहीं किया है। कोई भी जानकारी दर्ज न करें और टेक्स्ट को मिटा दें। यदि टेक्स्ट आपको "रुकें" या "नहीं" टेक्स्ट करने के लिए कहता है, तो आपको और टेक्स्ट नहीं मिलते हैं, इसे हटा दें। जवाब न दें। स्कैम कलाकार इसे यह पुष्टि करने के लिए करते हैं कि उनके पास कोई वास्तविक फ़ोन नंबर है।

धोखाधड़ी कैसी दिखती है? मुझे क्या करना चाहिए?

यदि मुझे धोखा देने की कोशिश करते हुए मुझसे संपर्क किया जा रहा हो तो क्या होगा?

- अपने फ़ोन पर आने वाले अपने कॉलर आईडी/कॉल डिस्प्ले पर हमेशा भरोसा न करें। स्कैमर्स के पास "पुलिस" जैसी बातें कहने के लिए कॉल डिस्प्ले को बदलने के तरीके होते हैं, जबकि वास्तव में वे वैध नहीं होते हैं।
- कनाडा सरकार के अधिकारी आपसे सीधे संपर्क नहीं करेंगे और आपकी कनाडियन स्टेटस हासिल करने के बदले पैसे की मांग नहीं करेंगे।
- CRA या Service Canada कभी भी ई-ट्रांसफर, बिटकॉइन या प्री-पेड क्रेडिट कार्ड जैसी ऑनलाइन मुद्रा द्वारा भुगतान का अनुरोध नहीं करेगा।
- सरकारी अधिकारी आपको बिटकॉइन जैसी ऑनलाइन मुद्रा के माध्यम से अपने पैसे को उन्हें ट्रांसफर करके सुरक्षित करने के लिए नहीं कहेंगे।
- यदि CRA आपको पैसा भेज रहा है तो यह सीधे जमा या डाक में चेक द्वारा होगा।
- कनाडा सरकार Western Union, Money transfer, प्रीपेड क्रेडिट कार्ड या किसी विदेशी देश में वायर ट्रांसफर के माध्यम से भुगतान स्वीकार नहीं करती है।
- CRA या सरकारी अधिकारी कभी भी आक्रामक भाषा का प्रयोग नहीं करेंगे या आपको गिरफ़्तार करने या पुलिस को भेजने की धमकी नहीं देंगे।

आप के द्वारा इस प्रकार के कॉल या संपर्क प्राप्त करने पर क्या करना चाहिए, यहां बताया गया है:

- पैसे या व्यक्तिगत जानकारी मांगने वाले किसी भी व्यक्ति पर संदेह करें।
- भुगतान न करें या अपनी व्यक्तिगत जानकारी न दें। यदि आपको संदेह है, तो कॉल करने वाले से कर्मचारी का नंबर मांगें और फ़ोन काट दें। कंपनी को ऑनलाइन देखें (उदाहरण के लिए, CRA या IRCC) और यह पुष्टि करने के लिए उन्हें कॉल करें कि क्या कॉल करने वाला व्यक्ति और अनुरोध किया गया कर्मचारी नंबर वैध है।
- कॉल करने वाले की वैधता की पुष्टि करने के लिए सहायता प्राप्त करने के लिए कैंपस सुरक्षा (Campus Safety) (416-978-2323) पर कॉल करें।
- कनाडा के जालसाजी रोधी केंद्र (https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm), Campus Safety (416-978-2323) या Toronto Police Services (416-808-2222) को घटना के बारे में बताएं।

अगर कोई व्यक्ति आपकी अंतरंग छवियों को प्रकाशित करने या साझा करने की धमकी दे रहा है तो क्या होगा

- शर्मिंदा न हों। अपने विकल्पों पर चर्चा करने के लिए Community Safety Office (416-978-1485) के साथ अपॉइंटमेंट लेने पर विचार करें।
- Campus Safety (416-978-2323) या टोरंटो पुलिस (416-808-2222) को बताने पर विचार करें।
- भले ही आप उस व्यक्ति को जानते हों जो आपको धमकी दे रहा है या नहीं जानते हों - उनके URL/नाम/ईमेल पता/हैंडल का स्क्रीनशॉट लें।
- आपको भेजे गए सभी संदेशों को सहेजें और कॉपी करें। पुलिस को बताते समय आपको इस जानकारी की आवश्यकता हो सकती है।
- जवाब देना या दूसरे व्यक्ति के साथ जुड़ना जारी न रखें।
- अपने सोशल मीडिया अकाउंट का पासवर्ड बदलने और/या अस्थायी रूप से अपने खाते को अक्षम या निष्क्रिय करने पर विचार करें।