UNIVERSITY OF TORONTO | Community Safety Office

معلومات منع الاحتيال وخيارات الدعم في جامعة تورنتو.

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

موارد متاحة لمساعدتك:

إذا كنت تشُك بأنك مستهدف من شخص محتال، فنحن نشجعك على تقديم بلاغ إلى Non- ***Campus Safety*** Emergency Lines (أدناه).

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

مكتب أمن المجتمع (***Community Safety Office***) على استعداد للتشاور معك حول أي موقف يسبب لك القلق بشأن سلامتك أو سلامة شخص آخر. يمكنك الوصول إلى الدعم من هذه الخدمة عن طريق الاتصال بالرقم: 1485-978-416 أو community.safety@utoronto.ca.

المزيد من النصائح:

قم بتنزيل تطبيق Campus Safety من جامعة تورونتو

- وصول إلى التنبيهات في الوقت الفعلي على مدار الساعة طوال أيام الأسبوع للحوادث المتعلقة بالسلامة أو إغلاق الحرم الجامعي
- محادثة مباشرة مع Campus Safety، وربط المستخدمين بموظفي السلامة في جامعة تورونتو في الوقت الفعلي
- وصول إلى TravelSafer: السماح لـ Campus Safety بمراقبة مسار المستخدم عند القدوم إلى الحرم الجامعي أو مغادرته حتى الوصول إلى الوجهة
- وصول إلى Mobile Bluelight: عند تفعيله، فإنه يرسل موقع المستخدم داخل الحرم الجامعي إلى الحرم الجامعي
- ميزات إضافية — مثل Friend Walk وخدمات الدعم — مساعدة المستخدمين في أي مكان في العالم.

الطلاب من خارج البلاد:

لمزيد من المعلومات حول مختلف أنواع عمليات الاحتيال والخداع التي غالبًا ما تستهدف الطلاب من خارج البلاد، تفضل بزيارة موقع دائرة الجنسية والهجرة الكندية على الرابط:

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

يتوفر تطبيق Campus Safety من جامعة تورونتو للتنزيل مجانًا على متجر Google Play ومتجر Apple.

نصائح حول الأمان على وسائل التواصل الاجتماعي

أمور يجب مراعاتها إذا كان ملفك الشخصي على وسائل التواصل الاجتماعي عامًا:

يمكن لأي شخص وكل شخص **مشاهدة او حفظ أو التقاط** الصور أو الرسوم أو التعليقات التي تنشرها .يشمل هذا أصحاب العمل، والزملاء، وزملاء الدراسة، وأي شخص لديه نوايا سيئة محتملة.

لا تستخدم اسمك الكامل و/أو صورتك الشخصية على ملفك الشخصي ومعلوماتك التعريفية، **و لا تضع معلومات شخصية** في سيرتك الذاتية.

تجنب نشر أي صور أو مقاطع فيديو للحي الذي تعيش فيه، أو الأماكن التي تتردد عليها، أو المدرسة، أو مكان العمل، وما إلى ذلك، لأن هذه الأماكن يمكن أن تساعد شخص ما على تحديد موقعك. انشر الصور بعد مغادرة الموقع أو الحدث: **#latergram** وحافظ باستمرار على أن يكون التطبيق الذي يحدد **موقعك الجغرافي في وضع إيقاف تشغيل**.

هل من الضروري أن يكون لديك **حساب عام** للتطوير الوظيفي، والمناصرة، والقضايا السياسية، وما إلى ذلك؟
إذن، ضع في اعتبارك امتلاك حساب عام يركز على الغرض منه، وأن يكون منفصلًا عن الحساب الخاص الذي يتيح لك مشاركة حياتك الشخصية.

هل من الضروري أن يكون لديك عدد كبير من المتابعين؟ إذن، ضع في اعتبارك **تحديد حجم المعلومات الشخصية التي تنشرها** وراجع القسم أعلاه في حسابات الملف الشخصي العامة.

أمور يجب مراعاتها إذا كان ملفك الشخصي على وسائل التواصل الاجتماعي خاصًا:

هل تعرف شخصيًا كل من يتابعك؟ **هل قابلتهم جميعًا وجهًا لوجه؟** إذا كانت الإجابة "لا" على أي من هذه الأسئلة، ففكّر في تحديث قوائمك ومراجعتها بانتظام.

قبل السماح لشخص ما بمتابعتك أو قبوله صديقًا على وسائل التواصل الاجتماعي، تحقق من حسابه **للتأكد من أنه ليس مزيفًا** وأنه يوجد صداقات مشتركة بينكما.

كيف يبدو الاحتيال؟ ماذا يجب عليّ أن أفعل؟

ماذا لو تم الاتصال بي من قبل شخص يحاول الاحتيال علي؟

- لا تثق دائمًا في هوية/مكالمة المتصل التي تُعرض على هاتفك. يمتلك المحتالون طرقًا لتغيير عرض المكالمات لقول أشياء مثل "الشرطة"، في حين أنها في الواقع غير مشروعة.
- لن يتصل بك أي موظف في الحكومة الكندية مباشرة ليطلب منك مبلغًا من المال مقابل تأمين وضع إقامتك في كندا.
- لن تطلب منك CRA أو Service Canada أبدًا الدفع عن طريق التحويل الإلكتروني أو العملة المشفرة مثل بيتكوين أو بطاقات الائتمان مسبقة الدفع.
- لن يطلب منك أي موظف حكومي تأمين أموالك عن طريق تحويلها إليه عبر عملة مشفرة مثل بيتكوين.
- إذا أرادت CRA أن ترسل إليك مبلغًا من المال، فسيتم ذلك عن طريق الإيداع المباشر أو عن طريق شيك في البريد العادي.
- لا تقبل الحكومة الكندية المدفوعات عبر Western Union أو تحويل الأموال نقدًا أو عبر بطاقات الائتمان مسبقة الدفع أو من خلال التحويلات البنكية إلى بلد أجنبي.
- لن يستخدم موظفو CRA أو موظفو الحكومة أبدًا لغة عدوانية أو التهديد باعتقالك أو تبليغ الشرطة.

التقط بأمان
الانترنت للأبد

#sharingisnotcaring

416.978.1485 www.communitysafety.utoronto.ca

ما الذي يجب عليك فعله عندما تتلقى هذه الأنواع من المكالمات أو جهات الاتصال؟

- لا تأمن جانب أي شخص يطلب منك المال أو معلومات شخصية.
- لا تدفع ولا تقدم معلوماتك الشخصية. إذا كنت تشك في الأمر، اطلب من المُتصل رقم الموظف وأغلق الهاتف. ابحث عن الشركة عبر الإنترنت (مثل CRA أو IRCC) واتصل بهم للتحقق من صحة رقم الموظف والطلب الذي عرضه المُتصل.
- اتصل برقم Campus Safety (416-978-2323) للحصول على دعم يؤكد شرعية المُتصل.
- أبلغ عن الحادث إلى مركز مكافحة الاحتيال الكندي (https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm) أو Campus Safety (416-978-2323) أو شرطة تورونتو (416-808-2222).

ماذا لو هدَّدك شخص ما بنشر أو مشاركة صور حميمة لك؟

- لا تشعر بالحَرَج. فكِّر في تحديد موعد مع مكتب سلامة المجتمع (416-978-1485) لمناقشة خياراتك.
- فكِّر في تقديم بلاغ إلى Campus Safety (416-978-2323) أو إلى شرطة تورنتو (416-808-2222).
- بغض النظر عما إذا كنت تعرف الشخص الذي يهددك أم لا - التقط صورة مصغرة لشاشة عنوان URL / الاسم / عنوان البريد الإلكتروني / العنوان.
- احفظ وانسخ جميع الرسائل التي تم إرسالها إليك. قد تحتاج إلى هذه المعلومات عند تقديم بلاغ للشرطة.
- لا تستمر في الرد أو التعامل مع الشخص الآخر.
- فكِّر في تغيير كلمة مرور حساب الوسائط الاجتماعية الخاص بك و/أو تعطيل حسابك أو إلغاء تنشيطه مؤقتًا.

أنواع الاحتيال

خطة الاحتيال 1: "الإعادة إلى المُرسل"

1. يتلقى الضحية مكالمة آلية من شركة توصيل حول طرد بريدي. ترتبط هذه المكالمة بشخص يدّعي أنه يعمل في شركة توصيل طرود.
2. تتم "إحالة" الضحية إلى الشرطة ثم يتم إبلاغه بأنه تم مصادرة طرد معنون له يحتوي على بضائع غير قانونية.
3. يتم إخبار الضحية بأنه سيتم اعتقاله وترحيله بسبب تورطه في هذا العمل. يتم إخبار الضحية أن لديه فرصة لدفع غرامة لتجنب السجن/الترحيل.

خطة الاحتيال 2: "بطاقة غسيل الأموال"

1. يتلقى الضحية مكالمة من شخص يدّعي العمل مع الشرطة.
2. يتم إخبار الضحية بأن بطاقته المصرفية قد تم استخدامها في مخطط لغسيل الأموال وسيتم إغلاق حساباته.
3. يتم إخبار الضحية بأن من الواجب عليه أن يتعاون مع التحقيق لتبرئة اسمه ويُطلب منه سحب أموال من حساباته وإيداعها في "نظام آمن" عبر العملة المشفرة بيتكوين أثناء مسيرة التحقيق.
4. يتم إخبار الضحية بأن هذه الأموال ستُعاد في نهاية التحقيق.

خطة الاحتيال 3: "الابتزاز الجنسي"

1. يتعرض الضحية لمواقف تبدو غير مؤذية عبر وسائل التواصل الاجتماعي أو من خلال مواقع المواعدة.
2. وفي المحصلة، يُجبر الجاني الضحية على إرسال صور فاضحة، أو التعرّي أمام الكاميرا، أو القيام بأفعال جنسية أثناء التواجد أمام الكاميرا.
3. يتعرض الضحية للتهديد بمشاركة صوره (عبر الإنترنت، مع أفراد الأسرة، وما إلى ذلك) ما لم يرسل مبلغًا من المال إلى الجاني (أو في بعض الحالات ما لم يرسل المزيد من الصور).
4. وفي بعض الحالات، يُجبر الضحية على الاختفاء تحت تهديد مشاركة الصور ويتم الاتصال بأسرة الضحية للحصول على "فدية".

سيناريوهات أخرى؟

- مكالمة/رسالة بريد إلكتروني من شخص ينتحل صفة الإدارة القانونية لـService Canada ليقول إن هناك تهمًا تم توجيهها إليك.
- مكالمة/رسالة بريد إلكتروني من شخص يتظاهر بأنه ممثل عن Service Canada ويشير إلى أن رقم الضمان الاجتماعي (SIN) الخاص بك قد تم حظره أو اختراقه أو تعليقه.
- تهديدات من متصل تشير صدور مذكرة توقيف بحقك وسيتم تنفيذها إذا لم يتم السّداد على الفور.
- تهديدات من متصل تشير إلى أنك ستفقد تأشيرتك أو وضع الإقامة الخاص بك أو سيتم ترحيلك من البلاد إذا لم يتم السّداد على الفور.
- مكالمة/رسالة بريد إلكتروني تشير إلى أن جهاز الكمبيوتر الخاص بك مصاب بفيروس. سيعرض عليك المُتصل أو المُرسل إزالة الفيروس من جهاز الكمبيوتر الخاص بك. سيحاول هذا الشخص الحصول على كلمات مرور من جهاز الكمبيوتر الخاص بك ومعلومات خاصة أخرى.
- مكالمة/رسالة بريد إلكتروني تشير إلى أنك فزت بشيء، لكنك لم تدخل في مسابقة. لا تدخل أي معلومات واحذف النص. إذا أخبرك النص أن ترسل رسالة نصية "STOP" أو "NO" حتى لا تحصل على المزيد من الرسائل النصية، فاحذفها. لا ترد. يقوم محترفو الاحتيال بذلك للتأكد من أن لديهم رقم هاتف حقيقي.