تيلاس وايز

الأمان الرقمي ونصائح حول الخصوصية.

يعد تيلاس وايز® برنامجًا تعليميًا مجانيًا يقوم بدعم الكنديين من أجل الحفاظ على سلامتهم في عالمنا الرقمي.

أمان الانترنت

1. احم نفسك: استخدام مضاد الفيروسات، ومضاد برامج التجسس، وحلول السلامة عن طريق جدار الحماية المعروف باسم «الفاير وول» لإنشاء نسخة احتياطية من بياناتك بشكل منتظم.
2. ابق على البرامج، وأنظمة التشغيل والمتصفحات كاملة التحديث بحيث تكون محمي دائمًا من أحدث التهديدات.
3. ضع كلمة مرور قوية وقم بتغييرها من حين إلى آخر. يمكنك أن تجعل كلمة المرور الخاصة بك أقوى وذلك باستخدام الأحرف الأولى من جملة، بدلًا من كلمة ما. مثال: 2ICARMP* من جملة "I can always remember my password 2*". وبإمكانك حتى أن تستخدم جملة مرور وأن تشغل التصريح عن طريق عاملين من أجل حماية إضافية.
4. تفحص بريدك الإلكتروني: تكون المرفقات/الروابط المشبوهة، طلبات المعلومات الشخصية، والأخطاء الإملائية والنحوية علامة سديدة على رسالة إلكترونية يحتمل أن تتسبب في ضرر ما.

سلامة وسائل التواصل الاجتماعي

1. راقب إعدادات التصريحات والخصوصية:
   - إعدادات التصريحات تتحكم فيما يمكن الوصول إليها وما لا يمكن الوصول إليه وتشاركه فيما يخصك (مثل قائمة الأشخاص الموجودين لديك، الصور، معلومات الصفحة الشخصية).
   - إعدادات الخصوصية تتحكم في من الذي يمكنه مشاهدة صفحتك الشخصية ومنشوراتك ومن لا يمكنه.
2. قم بإنشاء «منبه قوقل»: قم بإعداد منبه قوقل على صفحة google.com/alerts بحيث يتم إخطارك عبر البريد الإلكتروني عندما يظهر اسمك على الانترنت.
3. قم بتقليص ما تقوم بتشاركه: إن تشارك الكثير من المعلومات مثل تاريخ ميلادك، وعنوانك، وتفاصيل إجازاتك قد يزيد من تعرضك للخطر.
4. فكر مليًا قبل التواصل: تواصل فقط عبر الانترنت مع الأشخاص الذين تعرفهم وجهًا إلى وجه.
5. احترس عندما تنقر: لا تنقر على عروض قد تبدو غير معقولة وغير واقعية.
6. قم بغلق خاصية الإشارة الجغرافية: تشمل الصورة الملتقطة بواسطة غالبية الهواتف الذكية «إشارة جغرافية» (التفاصيل الدقيقة للموقع الذي تم فيه التقاط الصورة). أغلق هذه الخاصية لتغزيز خصوصيتك عند تشارك الصور عبر الانترنت.
7. لا تنس تسجيل الخروج: إن ترك حسابات وسائل التواصل الاجتماعي أو البرامج أو الألعاب مفتوحًا في أثناء عدم استخدامها يجعلك معرضًا لمخاطر تمس الأمان والخصوصية.
8. حافظ على نظافة منزلك الرقمي: اضبط وقتًا على رزنامتك (التقويم الخاص بك) كل ثلاثة إلى ستة أشهر لتفحص إعدادات الخصوصية والتصريحات الخاصة بك، وتغيير كلمات المرور، واستعراض قوائم «الأصدقاء» والتحقق منهم، وإيقاف نشاط الحسابات التي لم تعد تستخدمها.

سلامة الهاتف الذكي والجهاز اللوحي «التابلت»

1. أغلق هاتفك: برمج هاتفك بحيث يغلق بشكل تلقائي بعد فترة من عدم النشاط.
   لا تنس تحديد كلمة مرور وتعديلها بشكل منتظم.
2. برنامج الغلق والتعقب والمسح: استخدم برنامجًا يقوم بغلق أو تعقب أو المسح عن بعد للمعلومات على هاتفك في حال أن تم فقده أو تمت سرقته، على سبيل المثال، «Find my phone» بالنسبة لهواتف الآيفون، أو «Find my Device» بالنسبة لبعض هواتف الأندرويد. تذكر مسح كل شيء من جهازك قبل أن تقوم ببيعه أو إعادة تدويره.
3. قم بتحديث برنامج التشغيل الخاص بك بشكل منتظم لحمايته ضد أحدث التهديدات.
4. قم بإدارة إعدادات الموقع: امنح الإطلاع على موقعك فقط للبرامج التي تحتاج إلى معرفة موقعك، مثل برنامج تحديد المواقع GPS أو الخرائط. يمكن لوسائل التواصل الاجتماعي والعديد من البرامج الأخرى أن تعمل من دون معلومات الموقع.
5. تنبه إلى عمليات الاحتيال: مثل الرسائل الإلكترونية المزيفة، تحاول هذه الرسائل النصية المزيفة أن تجعل الأشخاص ينقرون على روابط ضارة و/أو تقديم معلومات خاصة.
6. ابحث عن معلومات حول البرامج قبل تنزليها لتجنب تنزيل البرامج الضارة على جهازك.
7. احذر من شبكات الواي فاي المجانية: اقصر نشاطاتك على التصفح فقط. لا تقم أبدًا بتشارك معلومات شخصية أو مالية عبر شبكة واي فاي عامة.
8. احذر من مخاطر البلوتوث: يمكن لمتسللي الشبكات الوصول إلى معلومات على الجهاز التي بها خاصية البلوتوث مفعلة. قم بالسماح فقط للاتصالات مع الأجهزة الموثوقة و/أو أغلق البلوتوث إذا لم يكن مطلوبًا.

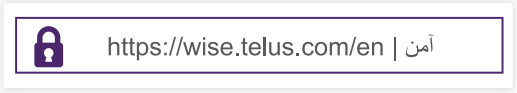
سلامة IoT

يقصد باختصار IoT، أو انترنت الأشياء (بالإنجليزية Internet of Things) إلى الأجهزة الذكية أو المتصلة بالانترنت مثل أنظمة الأمان المنزلي، وشاشات مراقبة الرضع، والهواتف الذكية المتصلة ببعضها عبر الإنترنت. تحدث هذه الأجهزة ثورة في العديد من مناحي حياتنا، لكنها تقوم بجمع ونقل البيانات، لذا من المهم أن نضع في الاعتبار ما يلي:

1. فهم ماهية البيانات التي يتم جمعها وكيف يتم استخدامها.
2. قم بإدارة إعدادات الخصوصية بحيث يمكنك فقط مشاركة ما تود مشاركته وما تشعر بالراحة حياله.
3. أغلق الأجهزة عندما لا تستخدمها (خاصة الأجهزة ذات خواص الكاميرا/الميكروفون).
4. اجعل الأجهزة على شبكة الضيوف «Guest network»، لحماية شبكتك الشخصية في حال حدوث تسلل أو قرصنة.

سلامة التسوق عبر الانترنت

1. تحقق من سمعة البائع: اطلع على بيان الخصوصية، والعنوان الفعلي، ورقم الهاتف وسياسة الإرجاع على الموقع الإلكتروني، واطلع على ردود الفعل الإيجابية من جانب عملاء آخرين.
2. تحقق من الأمان: ابحث عن رمز القفل وحرف «S» في «https» في شريط العنوان.



3. احم معلوماتك: لا تقم بالتسوق من خلال حواسيب عامة أو شبكات واي فاي عامة وارفض دائمًا خيار حفظ معلومات بطاقة البنك.
4. عندما القيام بالسداد المحمول عبر هاتفك أو ساعتك، استخدم فقط برنامج السداد الذي أتى مع الجهاز (مثل Apple Pay أو Android Pay).

قف في مواجهة القيادة المشتتة

إن القيادة المشتتة غير مقبولة اجتماعيًا. ابق يديك على عجلة القيادة وعينيك على الطريق من خلال هذه النصائح:

1. اجعل هاتفك بعيدًا عن ناظريك ولا تشغل بالك به.
2. اجعله صامتًا أو أغلقه.
3. اعتمد على من يجلس إلى جوارك في التعامل مع هاتفك.
4. افحص رسائلك وبرنامج GPS قبل القيادة.
5. اركن سيارتك إلى مكان آمن إذا كان من الضروري استخدام هاتفك.

أوقف التنمر الإلكتروني وترفع عنه من خلال هذه النصائح:

1. توقف عن التشابك واترك المساحة الإلكترونية على الفور؛ إن الرد على الجدال قد يتسبب في تصاعد الموقف.
2. قم بعرقلة وتعطيل جميع الرسائل إن استطعت، وقم بالإبلاغ عن/حظر الشخص عبر منصة التواصل الاجتماعي.
3. سجل الرسائل إن استدعت الحاجة لاحقًا إلى التحقيقات؛ قم بالتقاط صورة للشاشة لحفظ الأدلة.
4. تحدث إلى شخص ما واعقد الأمر حول الإجراء الذي ستتخذه. إذا تعذر عليك إصلاح الموقف أو كنت تشعر بالتهديد ينبغي عليك الاتصال بالهيئة المحلية لإنفاذ القوانين التي تتبع لها.

انضم إلى حركة **#EndBullying** وساعد في العمل على أن تكون المساحة الرقمية مكانًا آمنًا. شارك في تعهد «تيلاس وايز» الرقمي على **telus.com/digitalpledge**

لمعرفة المزيد طالع **telus.com/wise** أو تواصل مع **wise@telus.com** لطلب ورشة عمل. انضم إلى المحادثة عبر الانترنت مع **#TELUSWise**

مصادق عليه من جانب الجمعية الكندية لرؤساء الشرطة،
وصلت تيلاس وايز إلى أكثر من 200,000 كندي
عبر ورش عمل وموارد تعليمية وتثقيفية.

TELUS
the future is friendly®