National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

الحفاظ على الأمان عبر الإنترنت

لماذا يعد الأمن السيبراني مهمًا بالنسبة لي؟

شبكة الإنترنت ووسائل التواصل الاجتماعي هي منصات رائعة تساعدنا على مشاركة المعلومات والبقاء على تواصل مع الأصدقاء والعائلة.

ومع ذلك، يستخدمها المجرمون والمنظمات غير القانونية الأخرى أيضًا لمحاولة السيطرة على أموالك أو معلوماتك أو لتخويفك.

إذ بإمكانهم العمل من أي مكان في العالم، ويجيدون التحدث بمعظم اللغات بطلاقة وإنشاء مواقع إلكترونية مزيفة سهل عليهم إقناعك بها. سوف يتصلون بك عبر البريد الإلكتروني ووسائل التواصل الاجتماعي والرسائل النصية وسيحاولون جعلك تشعر بالخوف أو القلق، لتشويش أفكارك.

كل هذا يعني أنك بحاجة إلى أن تكون دائما مستعدا ومدركا للحيل التي يستخدمونها.

ما هي بعض المشكلات الشائعة التي قد أواجهها عبر الإنترنت؟

فيما يلي بعضا من المواقف الأكثر شيوعا التي نراها.

- تتلقى رسالة بريد إلكتروني أو رسالة نصية مريبة تطلب منك النقر على رابط فيها.
  - غالبًا ما تؤدي هذه الروابط إلى مواقع إلكترونية مزيفة مصممة لسرقة بيانات تسجيل الدخول أو البيانات المالية الخاصة بك.
- تتلقى مكالمة مريبة يطلبون منك فيها معلوماتك الشخصية.
  - وكما ذكر أعلاه، يتظاهر المتصل بأنه من البنك الذي تتعامل معه ويطلب منك المعلومات.
- تتلقى اتصالاً من شخص يتظاهر بأنه شخص لديه سلطة تؤهله أن يحاول إقناعك بفعل شيء ما.
  - وغالبا ما يلجأ الشخص إلى نوع من أنواع التهديد.
- يتمكن شخص ما من الدخول إلى واحد أو أكثر من حساباتك عبر الإنترنت (على سبيل المثال: البريد الإلكتروني أو وسائل التواصل الاجتماعي).
  - إذا استطاع شخص ما من الدخول إلى حسابك عبر الإنترنت، فيمكنه آنذاك سرقة معلوماتك وإعادة توجيه المدفوعات واستهداف أصدقائك أو عائلتك من خلال انتحال شخصيتك.
- تتم سرقة تفاصيل بطاقة الائتمان الخاصة بك، أو يتم خداعك وسرقة أموالك في عملية بيع أو استثمار مزيفة.
  - يأمل المحتال أن تعجبك الصفقة ويطمح منك بالدفع لها دون تفكير. أو ربما يتم اختراق بيانات موقع إلكتروني حقيقي، وبهذا يتم تسريب تفاصيلك عبر الإنترنت.

هناك المزيد من السيناريوهات هنا:
احصل على المساعدة الآن - تَمَلَّكْ موقعك الإلكتروني

كيف أحافظ على الأمان عبر الإنترنت؟

- **كلمات مرور طويلة وفريدة من نوعها.**

  - كلما طالت كلمة المرور كلما كانت أقوى وأكثر أمانا.
  - قم بإنشاء كلمة مرور يسهل تذكرها مكونة من أكثر من 16 حرفا عن طريق ضم أربع كلمات عشوائية معا (على سبيل المثال: TriangleRhinoOperationShoes) وإضافة الأرقام والأحرف الكبيرة والرموز إذا لزم الأمر (على سبيل المثال: Triangle&"Rhino"Operation2Shoes).
  - الأمر المهم هو عدم تكرار كلمات المرور الخاصة بك بأكثر من حساب. إذا حصل أحد المجرمين على إحدى كلمات المرور الخاصة بك، فسوف يحاول استخدامها على حساباتك الأخرى أيضًا.
  - استخدم أداة مدير كلمات المرور لتذكر كلمات المرور الخاصة بك وإنشاء كلمات مرور جديدة.
  - أنشئ كلمات مرور جيدة - تَمَلَّكْ موقعك الإلكتروني
- **قم بتفعيل المصادقة الثنائية.**
  - وهي معلومة إضافية - عادة ما تكون رمزا على هاتفك - تحتاجها لغرض تسجيل الدخول إلى الموقع الإلكتروني.
  - هذه التقنية قوية للغاية ويمكن أن توقف معظم محاولات الدخول إلى حساباتك.
  - نوصي باستخدام "تطبيق المصادقة"، كلما كان ذلك متوفرا.
  - إعداد المصادقة الثنائية (2FA) - تَمَلَّكْ موقعك الإلكتروني
- **حافظ على خصوصيتك على الإنترنت.**
  - الخيار الأفضل للحفاظ على أمان معلوماتك على وسائل التواصل الاجتماعي هو تشغيل إعدادات الخصوصية الخاصة بك.
  - سيؤدي ذلك إلى منع الأشخاص العشوائيين، بما في ذلك مجرمي الإنترنت، من رؤية رسائلك أو إرسال رسائل إليك.
  - ابق حذرًا دائمًا عند نشرك لمعلومات شخصية عن نفسك أو عائلتك أو أصدقائك.
  - تأكد من أن المتصلين بك هم فعلاً من يدعون بأنهم هم.
  - احذر من طلبات الصداقة المزيفة. كن حذرا من الأشخاص الذين يدعون بأنهم صحفيين أو آخرين ممن لا تعرفهم جيدا.
  - حماية خصوصيتك على الإنترنت - تَمَلَّكْ موقعك الإلكتروني
- **حافظ على تحديث كل شيء.**
  - عندما تقوم بتحديث هاتفك أو حاسوبك أو برنامجك فهذا من شأنه أن يسد أي ثغرات قد تكون موجودة في برنامج الحماية أيضًا.
  - يبحث المجرمون دائمًا عن طرق للدخول والتحديثات هي لإصلاح الثغرات الأمنية.
  - أعد تشغيل أجهزتك بانتظام.
  - واكب التحديثات - تَمَلَّكْ موقعك الإلكتروني
- **ابق متيقظا للاحتيالات.**
  - أفضل نصيحة هي أن تكون متيقظا لهذه الاحتيالات ومراقبتها إذا حاول المجرمون الاتصال بك على أي منصة عبر الإنترنت.
  - إذا بدا لك الأمر مريبا، فلا تتواصل مع الشخص الذي اتصل بك. كن حذرا بشكل خاص إذا طلبوا منك المال، حتى لو بدوا لك إنهم ودودين.

- تنبه لروابط وعناوين البريد الإلكتروني الغريبة (على سبيل المثال: لن يرسل لك البنك الخاص بك بريدًا إلكترونيًا من حساب Gmail).
- احذر من النقر على الروابط المرسلة لك في الرسائل النصية.
- قم بتنزيل التطبيقات على جهازك من متاجر التطبيقات الرسمية فقط.
- إذا ساورتك الشكوك، اتصل بالمنظمة المعنية مباشرة ولا تتبع أي روابط أو أرقام هواتف يتم إرسالها إليك.
- حاول أن تظل على دراية بالمخاطر الأمنية عبر الإنترنت، تلك التي تهددك وتهدد جاليتك أو أي مجموعات تنتمي إليها.

- **احم معلوماتك.**
  - استخدم تطبيقات المراسلة المشفرة، مثل Signal. هذا من شأنه منع أي شخص من قراءة رسائلك.
  - لا تشارك المعلومات مع أي موقع إلكتروني ما لم يكن عنوانه يبدأ بـ HTTPS. يشير الحرف S إلى "آمن" ويعني أن أي معلومات يتم إرسالها بينك وبين ذلك الموقع يتم تشفيرها.
  - ضع في اعتبارك استخدام شبكة افتراضية خاصة (VPN) يمكنها حماية بياناتك وإخفاء موقعك.
  - تحقق من البيانات والرخص التي يمكن لتطبيقاتك الوصول إليها. على سبيل المثال، لا يحتاج تطبيق اللياقة البدنية إلى الوصول إلى جهات الاتصال الخاصة بك.

ماذا أفعل إذا تعرضت للخداع أو ما هو أسوأ؟

هناك العديد من الأماكن التي يمكنك الذهاب إليها للحصول على المساعدة. لن تقوم أي من هذه المنظمات بمشاركة بياناتك مع أي شخص آخر، إلا بعد موافقتك.

- يمكنك الإبلاغ عن الحوادث الإلكترونية إلى المركز الوطني للأمن السيبراني NCSC من خلال بوابة CERT NZ ويمكننا مساعدتك أو التواصل مع وكالة أخرى:
  الإبلاغ عن حادث | CERT NZ
- إذا كنت قد خسرت مبالغ مالية، فيجب عليك الاتصال بالبنك الذي تتعامل معه على الفور.
- يمكن إعادة توجيه الرسائل النصية الاحتيالية مجانًا إلى الرقم 7726، وهي خدمة تديرها وزارة الداخلية.