National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

الحفاظ على أمن وسلامة مؤسستك عند استخدام الإنترنت

لماذا يعد الأمن السيبراني مهما للمجتمعات والمؤسسات؟

تحتوي هذه الصفحة على النصائح وبعض من الخطوات التي يمكنك اتخاذها لحماية جاليتك أو مؤسستك من تهديدات الأمن السيبراني. كما ويوجد أيضا دليل منفصل مخصص للأفراد للحفاظ على سلامتهم عبر الإنترنت.

تستند هذه النصائح على أكثر التهديدات شيوعا وخطورة.

- التحديثات - حافظ على تحديث البرامج الموجودة على أجهزتك لتصحيح أي ثغرات تتعلق بالأمن والسلامة.
  - احرص على تحديث أجهزة جاليتك أو مؤسستك. يشمل ذلك الهواتف وأجهزة الكمبيوتر وأجهزة توجيه WiFi وأي جهاز آخر متصل بالإنترنت - بما في ذلك الأجهزة الذكية.
  - استخدم التحديثات التلقائية إذا أمكن ذلك.
- المصادقة الثنائية (2FA) – من شأنها إضافة مزيد من الأمان إلى حساباتك من خلال طلبها لكلمة مرور وإجراء خطوة أخرى، مثل رمز لتطبيق على هاتفك.
  - ملاحظة: يدعى هذا الإجراء أيضا بالمصادقة متعددة العوامل (MFA)، أوالتحقق بخطوتين (2SV)، والعديد من الأسماء الأخرى.
  - قم بتشغيل المصادقة الثنائية (2FA) على جميع الحسابات التابعة لجاليتك أو مؤسستك.
  - وإذا أمكن، حاول استخدام شكل من أشكال المصادقة الثنائية (2FA) المقاوم للتصيد الاحتيالي، مما يعني أنه لا يمكن خداعك للإفصاح عنه. قد يكون هذا على شكل مفتاح أمان فعلي أو اسلوب آخر مثل بصمة الإصبع أو معرّف الوجه.
- تتبع حساباتك على الإنترنت - تأكد من أن الأعضاء السابقين لا يحتفظون بإمكانية وصولهم إلى الحسابات بعد مغادرة المجموعة أو المؤسسة.
  - إذا كان لديك أكثر من شخص واحد يمكنهم الدخول إلى نفس الحساب، فتأكد من أن لديهم جميعا تسجيلات دخول مختلفة، وأن لجميعهم (2FA) قيد التشغيل.
  - احتفظ بقائمة لكل حسابات المستخدمين وقم بإلغاء تنشيط أي حسابات لا حاجة لها، أي عند مغادرة الموظفين المستخدمين لها.
  - احتفظ بسجل لأي أجهزة قدمتها لأعضاء جاليتك أو لموظفيك وتذكر استعادتها منهم وإعادة ضبطها على إعدادات الْمَصْنَعِ إذا غادر هذا الشخص المؤسسة. قد تحتاج أيضًا إلى تغيير شفرات رموز الدخول إلى المبنى بشكل شخصي.
- تحقق من الأشخاص الذين لديهم حق الوصول إلى حساباتك على الإنترنت - يجب أن يقتصر وصول الأشخاص في جاليتك أو مؤسستك فقط إلى الأشياء التي يحتاجون إليها.
  - إذا تم اختراق حساب شخص ما، فإن هذه الخطوات تحد من الضرر الذي يمكن أن يسببه الشخص الْمُخْتَرِقُ للحساب.
  - تحقق من الأذونات غير الضرورية وإزالتها بشكل منتظم.

- إذا كان لديك حساب "مسؤول" واحد يستخدمه عدة أشخاص، فواظب على مراقبته حرصاً من نشاط غير اعتيادي. حاول الحد من استخدام هذه الأنواع من الحسابات، خاصة للمهام اليومية.
- تنطبق هذه القواعد أيضًا على وصول المسؤول إلى الأجهزة، مثل أجهزة التوجيه للأنترنت.

- راجع عقودك مع مزودي الخدمة - إذا كُنْتَ قَدْ وَظَّفْتَ أي شخص لتشغيل خدمات تكنولوجيا المعلومات نيابة عنك.
  - تأكد من أن لديهم حماية الأمن السيبراني اللازمة لتلبية احتياجات مجموعتك أو مؤسستك.
- تَعَرَّفْ على كيفية عمل حساباتك وأنظمتك جميعها معًا - يساعدك فهم الاتصالات على معرفة المكان الذي يمكن للمُخترِق الدخول منه.
  - راجع الاتصالات بين أنظمتك، على سبيل المثال، البريد الإلكتروني والتخزين السحابي ومنصات المحاسبة.
  - فكر في استخدام شبكة افتراضية خاصة (VPN) لمزيد من الأمان عبر الإنترنت. إن استخدام VPN يساعد في إخفاء نشاطك عبر الإنترنت عن أي شخص قد يحاول تتبعك. وهذا مفيد بشكل خاص إذا كان أي من أعضاء مجموعتك أو مؤسستك يتواصلون عن بعد.
- حافظ على إبقاء موظفيك " يتصرفون بذكاء عبر الإنترنت" - فالأشخاص في مجموعتك أو مؤسستك أكثر عرضة للاستهداف من أنظمتك.
  - قم بتدريب جميع الموظفين على أساسيات الأمن السيبراني. موقع الويب الخاص بك تَمَلَّكْ موقعك الإلكتروني | NCSC تَمَلَّكْ موقعك الإلكتروني يقدم المركز الوطني للأمن السيبراني مجموعة واسعة من النصائح والإرشادات لمساعدتك على الحفاظ على الأمن والسلامة عبر الإنترنت وكيفية اكتشاف عمليات الاحتيال.
  - ذكّرهم بأن هذا الأمر مهم لحساباتهم الشخصية وكذلك الحسابات التي يستخدمونها لمؤسستك.
  - لدينا أيضًا دليل للأفراد من أجل الحفاظ على سلامتهم عبر الإنترنت.
- التخطيط للأحداث - يعد وجود خطة استجابة أمرًا مهمًا لتجنب تعرض الأشخاص للارتباك عند وقوع حادث ما.
  - تحدد خطة الاستجابة للأحداث دور كل شخص أثناء وقوع الحادث. تتوفر النماذج هنا NCSC | إدارة الحوادث
  - قم بتضمين خطة لما يجب فعله في حالة فشل عمل الهواتف، أو أجهزة الكمبيوتر، أو الأنظمة الأخرى. حافظ على تحديث هذه الخطة.
  - احتفظ بتفاصيل الاتصال الخاصة بكل شخص معني وتفاصيل احتياطية إذا كانت الطريقة الرئيسية للاتصال بهم معطلة (مثل البريد الإلكتروني).
  - احتفظ أيضًا بالخطة في مكان ما خارج نظامك، في حالة عدم تمكنك من الوصول إليها من خلاله.