[FRONTCOVER]

[Start Community Language Document 1]

الوعي السيبراني

نسخة التنسيقات البديلة للمركز الوطني للأمن السيبراني.

تم إنتاج هذا المحتوى بواسطة ليد اسكتلندا Lead Scotland بالاشتراك مع الشركاء وبتمويل من وحدة الصمود السيبراني التابعة للحكومة الاسكتلندية.

يعتمد هذا الدليل على المحتوى المتاح على موقع المركز الوطني للأمن السيبراني

تم تقسيم المعلومات إلى 7 وثائق بلغات مجتمعاتية وهي:

- هذا المستند ، الذي يتضمن مقدمة ونظرة عامة على 6 إجراءات يمكنك القيام بها لتحسين أمنك عبر الإنترنت.
- ثم وثائق مفصلة فردية عن الإجراءات الستة التي يمكنك القيام بها.
- يمكن الولوج إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على:

https://www.ncsc.gov.uk/cyberaware/

6 طرق لتحسين أمنك على الإنترنت

بسبب فيروس كورونا ، يقضي الناس وقتًا أطول على الإنترنت هذا العام.

وهذا يعني أنه هناك المزيد من الفرص للقراصنة للقيام بالهجمات الإلكترونية. يفعلون ذلك غالبًا عن طريق استهداف الأشخاص والشركات باستخدام:

- عمليات الاحتيال عبر البريد الإلكتروني والموقع الإلكتروني.
- البرامج الضارة - وهي برامج يمكنها إتلاف جهازك أو السماح لأحد المخترقين بالدخول.

إذا دخل المخترقون إلى جهازك أو حساباتك ، فيمكنهم الوصول إلى أموالك أو معلوماتك الشخصية أو معلومات حول عملك.

يمكنك تحسين الأمن السيبراني الخاص بك عن طريق اتخاذ ستة إجراءات:

الإجراء 1 - استخدم كلمة مرور قوية ومنفصلة عن كلمة مرور بريدك الإلكتروني.

الإجراء 2 - أنشئ كلمات مرور قوية باستخدام 3 كلمات عشوائية.

الإجراء 3 - احفظ كلمات المرور الخاصة بك في متصفحك.

الإجراء 4 - قم بتشغيل المصادقة الثنائية (2FA)

الإجراء 5 - قم بتحديث أجهزتك.

الإجراء 6 - قم بالحفاظ بنسخة احتياطية من بياناتك

[End Community Language Document 1]
[Start Community Language Document 2]

الإجراء 1 - استخدم كلمة مرور قوية ومنفصلة لبريدك الإلكتروني

إذا وصل أحد المخترقين إلى بريدك الإلكتروني ، فيمكنه إعادة تعيين كلمات مرور حساباتك الأخرى والوصول إلى المعلومات التي قمت بحفظها عنك أو عن عملك.

يجب أن تكون كلمة مرور بريدك الإلكتروني قوية ومختلفة عن جميع كلمات المرور الأخرى. وهو ما سيجعل من الصعب ايجادها أو التخمين فيها.

يعد استخدام ثلاث كلمات عشوائية ، طريقة جيدة لإنشاء كلمة مرور قوية وفريدة من الممكن لك تتذكرها. سننظر في ذلك بمزيد من التفاصيل في الوثيقة التالية.

يجب عليك أيضًا حماية حساباتك المهمة الأخرى ، مثل البنوك أو وسائل التواصل الاجتماعي.

مالسبب في أهمية البريد الإلكتروني؟

البريد الإلكتروني هو أحد أهم حساباتك. ولكن لماذا يهتم المخترقون برسائل البريد الإلكتروني الخاصة بك؟

تخيل لو وصل أحد المخترقين إلى بريدك الإلكتروني

يمكنهم الآن الوصول إلى المعلومات التي قمت بحفظها عن نفسك أو الاتصال بأشخاص وهم يتظاهرون بأنهم أنت لكن الأسوأ من ذلك كله ، أنه يمكنهم عزلك عن أي من حساباتك على الإنترنت

يمكنهم القيام بذلك عن طريق الذهاب إلى أي من حساباتك واستخدام ميزة "نسيت كلمة المرور"

حيث يتم إرسال بريدًا إلكترونيًا يحتوي على رابط لإعادة تعيين كلمة المرور الخاصة بك والتي يمكن للمخترق استخدامها لحجبك من حسابك

بمجرد إعادة تعيين كلمة مرور واحدة ، يمكنهم الاستمرار في إعادة تعيين كلمات المرور لحساباتك الأخرى أيضًا

إذن ، كيف يمكنك حماية بريدك الإلكتروني والمساعدة في إبعاد المخترقين عن جميع حساباتك على الإنترنت؟

استخدم كلمة مرور قوية لبريدك الإلكتروني وتأكد من أن كلمة مرور بريدك الإلكتروني مختلفة عن جميع كلمات المرور الأخرى التي تستخدمها

هذا يعني أنه إذا اخترق شخص ما كلمة مرورك لحساب آخر ، فلن يتمكن من استخدام ذلك للوصول إلى بريدك الإلكتروني

تذكر أن بريدك الإلكتروني هو أحد أهم حساباتك. فتأكد من أنه آمن

كيفية تغيير كلمة مرور البريد الإلكتروني الخاص بك

كيفية تغيير كلمة المرور الخاصة بك في:

- جيميل
- ياهو!
- آوتلوك.
- بي تي.
- آي أو أل.

إذا لم يكن بريدك الإلكتروني مدرجًا هنا ، فيجب عليك البحث عبر الإنترنت للحصول على نصيحة من مزود الخدمة الخاص بك حول كيفية تغيير كلمة مرور بريدك الإلكتروني.

نصائح حول كلمات المرور للمتداولين الحصريين والشركات الصغيرة

إذا كنت صاحب عمل ، فقد تتضمن حساباتك معلومات حساسة عن عملائك أو عملك أو أموالك.

إذا لم تكن حساباتك آمنة ، فقد يكون عملك أكثر عرضة لخطر وقوع حادث سيبراني. قد يعرض ذلك عملك لمخاطر قانونية أو مالية ، وخطر انتهاك اللائحة العامة لحماية البيانات.(GDPR)

إذا كان لشركتك موظفين ، فعليك التأكد من عدم تخزين كلمات المرور الخاصة بهم بجوار أجهزتهم ، وأن الأجهزة مقفلة أو متوقفة عن التشغيل عندما لا تكون قيد الاستخدام.

لمزيد من المعلومات ، راجع دليل الشركات الصغيرة للمركز الوطني للأمن السيبراني.

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 2]

[Start Community Language Document 3]

الإجراء 2 إنشاء كلمات مرور قوية باستخدام ثلاث كلمات عشوائية

عندما تستخدم كلمات مرور مختلفة لحساباتك المهمة ، قد يكون من الصعب تذكرها جميعًا.

يعد استخدام ثلاث كلمات عشوائية طريقة جيدة لإنشاء كلمات مرور قوية يسهل تذكرها.

لا تستخدم كلمات يمكن التخمين فيها (مثل اسم حيوانك الأليف). يمكنك تضمين الأرقام والرموز إذا كنت بحاجة إلى ذلك. على سبيل المثال: RedPantsTree4!

سيساعدك حفظ كلمات المرور الخاصة بك في متصفحك على إدارتها ، وسننظر في ذلك بمزيد من التفصيل في المستند التالي.

اختبر معرفتك لإنشاء كلمة مرور قوية

هل تعرف ماهي كلمة المرور التي لا تظهر في كلمات المرور الـ 100000 التي يمكن اختراقها أكثر؟

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!
- 2011977

الجواب هو: RedPantsTree.

يشارك المخترقون قوائم على الإنترنت تحتوي على ملايين كلمات المرور المخترقة.

3 كلمات عشوائية هي طريقة أسهل لإنشاء كلمات مرور جديدة من المرجح أن تكون فريدة بالنسبة لك وأقل عرضة للتخمين فيها

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 3]

[Start Community Language Document 4]

الإجراء 3 احفظ كلمات المرور الخاصة بك في متصفحك

يعني حفظ كلمة مرورك في متصفحك السماح لمتصفح الويب مثل كروم Chrome أو سفاري Safari أوإيدج Edge بتذكر كلمة مرورك نيابةً عنك.

وهو ما قد يساعد في:

- التأكد من عدم فقدان كلمات المرور الخاصة بك أو نسيانها.
- حمايتك من بعض الجرائم الإلكترونية ، مثل المواقع المزيفة.

وهو ما يعتبر أكثر أمانًا من استخدام كلمات مرور ضعيفة أو استخدام نفس كلمة المرور في أكثر من مكان.

تأكد من حماية كلمات المرور المحفوظة في حالة فقد جهازك أو سرقته.

كيف تحمي كلمات مرورك المحفوظة

قد يتمكن الشخص الذي يمكنه الوصول إلى جهازك من استخدام كلمات المرور المحفوظة للوصول إلى حساباتك.

هذا النوع من الجرائم السيبرانية أقل شيوعًا من الهجمات عن بُعد عبر الإنترنت ، حيث يتم اختراق كلمات المرور باستخدام برامج معينة.

للتأكد من أنك محمي ، يجب عليك:

- ايقاف تشغيل جهازك أو قفله عند عدم استخدامه.
- استخدم كلمة مرور قوية لحماية جهازك.
- قم بتشغيل المصادقة الثنائية لجميع أجهزتك وحساباتك.
- قم بتشغيل القياسات الحيوية (معرف الوجه أو التعرف على بصمات الأصابع) إذا كان جهازك يدعم ذلك.

يجب عليك أيضًا حفظ نسخ احتياطية لبياناتك بانتظام. بحيث سيساعدك ذلك في استعادة معلوماتك المهمة في حالة فقد جهازك أو سرقته.

كيفية حفظ كلمات المرور الخاصة بك في متصفحك تعرف على كيفية حفظ كلمات المرور الخاصة بك في:

- جوجل كروم
- مايكروسوفت إيدج.
- فاير فوكس.
- سفاري.

هل تعرف؟

أنه يمكنك الوصول إلى كلمات المرور المحفوظة الخاصة بك من أي جهاز قمت بتسجيل الدخول فيه في نفس المتصفح.

زد حماية إضافية

بمجرد إعداد كلمات مرور قوية ومنفصلة (الإجراءات من 1 إلى 3) لجميع أجهزتك وخدماتك ، هناك أشياء أخرى يمكنك القيام بها لتقليل خطر التعرض للاختراق (الإجراءات من 4 إلى 6).

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 4]

[Start Community Language Document 5]

الإجراء 4 تشغيل المصادقة الثنائية (2FA)

تساعد المصادقة الثنائية **(2FA)** على منع المخترقين من الدخول إلى حساباتك ، حتى لو كان لديهم كلمة مرورك.

تستخدم بعض الخدمات المصرفية عبر الإنترنت المصادقة الثنائية تلقائيًا. يتم ذلك بطلب مزيد من المعلومات لإثبات هويتك ، مثلا رمز يتم إرساله إلى هاتفك.

كيفية تشغيل المصادقة الثنائية (2FA)

ستحتاج إلى تشغيل المصادقة الثنائية **(2FA)** يدويًا لمعظم حساباتك. لن تقدم كل الحسابات المصادقة الثنائية **.(2FA)**

تستخدم الخدمات المصرفية عبر الإنترنت المصادقة الثنائية تلقائيًا.

تُعرف المصادقة الثنائية **(2FA)** أيضًا باسم التحقق من خلال خطوتين أو المصادقة المتعددة العوامل.

الفيديو: كيف تعمل المصادقة الثنائية

الوصول إلى الفيديو الخاص بكيفية عمل المصادقة الثنائية على موقع اليوتوب

قم بتشغيل المصادقة الثنائية للبريد الإلكتروني

- جيميل
- ياهو!
- آوتلوك
- آي أو أل

قم بتشغيل المصادقة الثنائية للتواصل الاجتماعي

- إنستغرام.
- الفيسبوك.
- تويتر.
- لينكدين.

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 5]

[Start Community Language Document 6]

الإجراء الخامس: قم بتحديث أجهزتك

لدى البرامج والتطبيقات وأنظمة التشغيل القديمة نقاط ضعف. وهو ما يجعلها أسهل للاختراق.

تعمل الشركات على إصلاح نقاط الضعف من خلال إصدار التحديثات. عندما تقوم بتحديث أجهزتك وبرامجك ، فإن ذلك يساعد على إبعاد المخترقين.

قم بتشغيل التحديثات التلقائية للأجهزة والبرامج التي توفرها. هذا يعني أنك لست مضطرًا لتذكر القيام بذلك بنفسك.

تحتاج بعض الأجهزة والبرامج إلى التحديث يدويًا. قد تستلم تذكيرات على هاتفك أو جهاز الكمبيوتر الخاص بك. لا تتجاهل هذه التذكيرات. فسوف يساعد التحديث في الحفاظ على أمنك على الإنترنت.

كيفية تشغيل التحديثات التلقائية

تعرف على كيفية تشغيل التحديثات التلقائية لـ:

- آبل - ماك
- آبل - آيفون وآيباد
- مايكروسوفت 10 - ابحث في ويندوز 10 عن تحديثات
- لم يعد ويندوز 7 مدعومًا. يجب عليك الترقية إلى ويندوز 10
- الهواتف الذكية والأجهزة اللوحية التي تعمل بنظام الآندرويد
- تطبيقات الأندرويد

اختبر معرفتك

سؤال: كيف تصلح الشركات نقاط الضعف في برامجها؟

- تضميد
- تصحيح
- اصلاح

الإجابة: عندما تجد الشركة نقطة ضعف في برامجها ، فإنها تصدر "تصحيحًا" لإصلاحه. يساعد ذلك في الحفاظ على أمان معلوماتك.

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 6]

[Start Community Language Document 7]

الإجراء 6 - قم بالحفاظ على نسخة احتياطية لبياناتك

يعني النسخ الاحتياطي إنشاء نسخة من معلوماتك وحفظها على جهاز آخر أو في التخزين السحابي عبر الإنترنت.

النسخ الاحتياطي بانتظام يعني أنه سيكون لديك دائمًا نسخة حديثة من معلوماتك المحفوظة. سيساعدك ذلك على التعافي بشكل أسرع في حالة فقدان بياناتك أو سرقتها.

يمكنك أيضًا تشغيل النسخ الاحتياطي التلقائي. وسيؤدي ذلك إلى حفظ معلوماتك بانتظام في التخزين السحابي ، دون الحاجة إلى تذكرذلك.

إذا احتفظت بنسخة احتياطية من معلوماتك على الناقل التتابعي المشترك أو محرك القرص الصلب الخارجي ، فافصلها عن جهاز الكمبيوتر عندما لا يكون النسخ الاحتياطي يسير.

هل تعرف؟

يجب عليك دائمًا الحفاظ على نسخة احتياطية لبياناتك قبل تحديث جهازك.

هذا لأن التحديثات يمكن أن تزيل أو تغير الملفات في بعض الأحيان.

كيفية تشغيل حفظ النسخ الاحتياطي التلقائي

كيفية تشغيل النسخ الاحتياطي التلقائي لـ:

- آبل – ماك.
- آبل - آيفون وآيباد.
- آندرويد
- مايكروسوفت ويندووز 10 ووان درايف لويندوز 8

نصائح حول النسخ الاحتياطية للتجار الفرديين والشركات الصغيرة

يعني الاحتفاظ بنسخة احتياطية من بياناتك أنه يمكنك الاستمرار في العمل في حالة وقوع حادث إلكتروني.

ابدأ بتحديد البيانات الأكثر أهمية لعملك. قد تكون هذه المعلومات مالية أو عقد أو معلومات عميل أو مورد. تأكد من نسخها احتياطيًا بانتظام.

يجب أن تعرف أيضًا كيفية استعادة نسخة احتياطية في حالة فقد البيانات.

لمزيد من المعلومات ، راجع دليل الشركات الصغيرة للمركز الوطني للأمن السيبراني.

يمكن الوصول إلى جميع الروابط المذكورة من خلال زيارة موقع المركز الوطني للأمن السيبراني على:
https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document7]

[END OF DOCUMENT]