٤.

احم أشياءَك الافتراضية القيمة

تمامًا مثلما تهتم بأشيائك الثمينة في المنزل، كذلك يجب أن تفعل بالنسبة للمعلومات التي تخزنها افتراضيًا، سواء كان ذلك سجلات مالية، أم صور جواز سفرك، أو حتى عنوانك أو رقم هاتفك، إن الأمر يستحق التفكير: أين تخزّن بياناتك الشخصية الأكثر أهمية؟ و كيف يمكنك حمايتها؟

إن أداء عملية تنظيف كاملة أمر رائع إذا أردتَ القيام ببعض التحسينات الخاطفة في أثناء احتسائك كوبًا من القهوة. ابحث عن معلومات محددة موجودة في بريدك الإلكتروني أو حساباتك الأخرى واحذفها؛ صور هويتك، تفاصيلك البنكية أو معلومات تأمينك الصحي، على سبيل المثال لا الحصر. وفي حال كنت ستحتاج إليها في المستقبل، فيمكنك تحميلها على جهازك أو طباعتها قبل حذفها من بريدك الإلكتروني.

أما إجراء عملية تنظيف عميقة فهي أكثر شمولية، ومن الجيد أن تقوم بها مرة في السنة، أرشِف كل شيء في بريدك الإلكتروني أو حسابك على مواقع التواصل الاجتماعي، حمّله على كمبيوترك واحذف محتوى الحساب من أجل بداية جديدة.

ويعود الأمر إليك إذا كنت تريد أن تحتفظ بنسخة احتياطية لأرشيفك ومستنداتك على السحابة، أو حفظها على قرص صلب خارجي أو فلاشة. في كل الأحوال، تأكد من عدم فقدانها، وأن كلمة المرور قوية ومنطقية بالنسبة لك.

٥.

مرِّرها

لئن كان النسيان سهلًا، فإن وراء تسمية "الشبكة العنكبوتية" سبب وجيه. نحن جميعًا متصلون عبر الإنترنت من خلال عدة شبكات، ليس فقط "كأصدقاء" على مواقع التواصل الاجتماعي، بل كذلك عبر قائمة الأسماء على حسابات الإيميلات والصور التي نشاركها على الإنترنت.

عندما تؤمِّن حساباتك، وتقوّي كلمات المرور، وتنظّف بياناتك، فإنك لست المستفيد الأوحد من ذلك، فكل شخص أنت على اتصال به يصبح في أمان أكبر بفضل جهودك.

عندما تنظف قوم بتنظيف بريدك الإلكتروني وحساباتك على مواقع التواصل الاجتماعي، فكر بالأشياء الأخرى التي تستطيع تحميلها على جهازك وحذفها التي تساعد أصدقاءك وزملاءك في العمل: : التفاصيل البنكية الخاصة بشقيقتك، رمز مفتاح الدخول إلى مكتبك، أو صورة عن الجواز السفر الخاص بابنك، هذهي فقط بعض السجلات التي يمكن أن تسبب المتاعب إذا ما وقعت في الأيدي الخطأ.

منتج لصالح
TACTICAL TECH
مدعوم من قبل
GOETHE INSTITUT
Firefox

datadetoxkit.org/ar/home
#datadetox

DATA DETOX KIT

غيّر إعداداتك

لتأمين بياناتك

إذا كان الإنترنت فقط مكانًا لمشاركة صور كلاب ترتدي زي ديناصورات، فلن تكون هناك حاجة ماسة لكلمات المرور.

إلا أنه من خلال الإنترنت، فإنك أيضًا تدفع فواتيرك، وتعيد شراء وصفاتك الطبية، وتسجّل بياناتك للتصويت.

عندما تفكر في جميع "أشيائك الافتراضية الثمينة" التي تشاركها عبر الإنترنت، والتي تخزّن على أجهزتك، تسأل: لماذا لا تُبقي عليها في مأمن تمامًا مثل محفظتك ومفاتيحك؟

هناك طريقة بسيطة لجعل وصول الآخرين إلى أشيائك الافتراضية الثمينة مهمة أصعب: لا تجعل تكهنهم بكلمات المرور أمرًا سهلاً، لا يحتاج أغلب الناس إلى مهارات تقنية متخصصة للدخول إلى حساباتك، إذ يمكنهم الدخول إليها عبر القيام ببعض التكهنات لكلمات المرور أو بتشغيل برنامج مؤتمت.

وحالما يتمكنون من الدخول إلى حساب واحد، يمكنهم تجريب كلمة المرور المكشوفة هذه للدخول إلى حسابات أخرى، وتجميع معلومات عنك وعن عاداتك، والاستيلاء على الحسابات التي تملكها، أو حتى استخدام هويتك الرقمية.

باتّباعك عملية تنظيف البيانات هذه، ستتعلم خطوات عملية لزيادة أمنك على شبكة الإنترنت.

فلنبدأ!

١.

أقفل بابك الرقمي

أقفال الشاشة: إن كلمات المرور، أو الأنماط، أو البصمات، أو هوية الوجه التي تستخدمها للدخول إلى جهازك، بعض من أفضل الدفاعات التي تستخدمها ضد من يريد الدخول إلى جهازك. إلا أن هناك كثيرًا من الأنواع المتوافرة وقد يكون من الصعب معرفة أي منها يناسبك.

إن وجود أي قفل على جوالك أو التابلت أو الكمبيوتر يعطيك حماية أفضل من عدم وجود قفل على الإطلاق. وتمامًا كأنواع الأقفال المختلفة التي قد تضعها على أبوابك، فإن بعض أقفال الشاشات أقوى من غيره.

من بين جميع الأقفال المتوافرة، فإن كلمات المرور الطويلة والفريدة هي الأقوى. هذا يعني أنك إذا فتحتَ جهازك بكلمة مرور، فإنها ينبغي أن تتضمن أحرفًا وأرقامًا ورموزًا خاصة.

فلنقل إنكم تستخدمون تمريرًا بسيطًا لفتح جهازكم، باستطاعتكم زيادة أمنكم بإنشاء كلمة مرور طويلة، أو هل تستخدمون نمطًا الآن؟ ما رأيكم بجعل النمط أطول؟ هل تستخدمون 1234 رمزًا للدخول إلى جهازكم؟ ما رأيكم برمي حجر النرد سبع مرات وحفظ ذلك الرمز بدلًا من ذلك؟

إن تغييرًا بسيطًا يمكن أن يسهم بشكل كبير في سيطرتكم على أجهزتكم.

٢.

دع الشخص الصحيح يدخل

إن إنشاء كلمات مرور قوية أمر سهل. كل ما عليك فعله هو اتّباع بعض المبادئ الأساسية. ينبغي أن تكون كلمات المرور التي تنشئها:

طويلة: ينبغي أن تكون كلمة المرور مؤلفة من ثمانية رموز على الأقل، هل تريد أفضل من ذلك؟ 16-20 رمزًا.

فريدة: ينبغي أن تكون كل كلمة مرور تستخدمها -لكل موقع- مختلفة عن الأخرى.

عشوائية: لا ينبغي أن تتبع كلمة المرور نمطًا منطقيًا، أو أن تكون سهلة التخمين، هنا يصبح مدير كلمات المرور مفيدًا جدًا.

إن أقوى كلمات المرور هي تلك التي تجمع بين الأحرف والأرقام والرموز الخاصة. إن هذه النصيحة الأزلية تجعل من كلمة المرور قوية وصعبة التخمين بشكل أكبر، لسوء الحظ، فإن بعض أنظمة كلمات المرور لا تسمح لك باستخدام رموز خاصة (مثل @#$%-=+)، لكن استخدام مزيج طويل بما فيه الكفاية من الأحرف والأرقام، يبقى أفضل من استخدام كلمة مرور قصيرة.

ولأفضل أدا، ينبغي لك استخدام مدير كلمة مرور مخصص لإنشاء جميع كلمات المرور الخاصة بك وتخزينها. إن مديري كلمات المرور مثل 1Password و KeePassXCمما ينصح به خبراء الأمن، وهي تطبيقات هدفها الأوحد حماية بيانات تسجيل الدخول والبيانات الأخرى الحساسة الخاصة بك.

٣.

أضف مفتاحًا ثانيًا

إن إنشاء تحقق ثنائي العامل "2FA أو تحقق متعدد العوامل "(MFA) يعني أنه حتى إذا حصل أحد على كلمة المرور الخاصة بك، فلن يتوافر لديه على الأرجح العامل الإضافي الذي يحتاج إليه للدخول.

ألقِ نظرة على إعدادات الأمن الخاصة بالمواقع والتطبيقات الأكثر استخدامًا، لترى ما إذا كان بإمكانك إنشاء هذا المفتاح الإضافي. ابدأ بالمواقع الأكثر أهمية، أي التطبيقات المالية، أو خدمات مثل البريد الإلكتروني التي تستخدمها لاستعادة حسابات أخرى.

فيس بوك:

القائمة ←
الإعدادات ←
الأمن وتسجيل الدخول ←
استعمل التحقق بخطوتين

جوجل:

سجّل الدخول إلى حسابك
← myaccount.google.com
الأمن ←
2-Step Verification التحقق بخطوتين ←
Get Started ابدأ

ملاحظة: عندما تنشيءتنشئ مرحلة تالية من التحقق، فسيترتب عليك اختيار طريقة ثانية للتحقق من هويتك. حاول تجنب استخدام الرسائل النصية المرسلة إلى رقم جوالك هاتفك كعامل ثانٍ، لأنهك قد تفقد جوالكهاتفك. استخدام البريد الإلكتروني هو خيار أكثر موثوقية.