نشرتك الشهريه للتوعية بأمن المعومات

أربع خطوات سهلة لتبقي بأمان

نظرة عامة

الاستفادة القصوى من التكنولوجيا بشكل آمن قد يعتبر شيء صعب. ومع ذلك، وبغض النظر عن التقنية التي تستخدمها أو كيفية استخدامها، إليك أربع خطوات بسيطة ستساعدك على الحفاظ على أمانك.

1. أنت: أولاً وقبل كل شيء، التكنولوجيا وحدها لا تستطيع حمايتك بالكامل، فأنت أفضل خط دفاع. المهاجمون يعلمون أن أسهل طريقة للحصول على ما يريدون هو استهدافك، بدلاً من الكمبيوتر أو الأجهزة الأخرى. إذا كانوا يريدون كلمة المرور أو بطاقة الائتمان أو التحكم في حاسوبك الشخصي، فسيحاولون خداعك لإعطائها لهم، وذلك غالبًا عن طريق خلق شعور بالإلحاح. على سبيل المثال، يمكنهم الاتصال بك متظاهرين بأنهم دعم فني من شركة ميكروسوفت ويدَعون أن حاسوبك مصاب، في حين أنهم في الحقيقة مجرمون إلكترونيون يريدون منك منحهم إمكانية الوصول إلى جهازك الكمبيوتر. أو ربما يرسلون إليك رسالة بالبريد الإلكتروني تحذر من أنه لا يمكن تسليم الحزمة الخاصة بك وليتم تسليمها عليك بالضغط على الرابط التالي لتأكيد عنوانك البريدي، بينما هم في الواقع يخدعونك لزيارة موقع ويب ضار يتسلل إلى جهازك. ولذلك فخلاصة الأمر، أن أعظم خط دفاع ضد المهاجمين هو أنت. بالحرص والمنطق السليم، يمكنك اكتشاف العديد من الهجمات وإيقافها.

2. كلمات المرور: التطور السريع في أجهزة الحاسوب جعل كلمات المرور القديمة المكونة من 8 أحرف قابلة للكسر. ولذلك فعندما يطلب منك موقع ما إنشاء كلمة مرور، قم بإنشاء عبارة مرور قوية وفريدة بدلاً من ذلك. عبارة المرور هي نوع من كلمة المرور التي تستخدم سلسلة من الكلمات التي يسهل تذكرها، مثل «حان وقت القهوة القوية». كلما كانت عبارة المرور أطول، كلما كانت أقوى. ولابد أن تكون كلمة المرور فريدة أي بمعنى آخر استخدام كلمة مرور مختلفة لكل جهاز أو حساب عبر الإنترنت. وبهذه الطريقة، في حالة اختراق كلمة مرور واحدة، تظل جميع حساباتك وأجهزتك الأخرى آمنة. فإن كنت لا تستطيع تذكر كل كلمات المرور الفريدة؟ استخدم مدير كلمات المرور، وهو برنامج متخصص يخزن جميع عبارات المرور الخاصة بك بشكل آمن بتنسيق مشفر (والكثير من الميزات الرائعة الأخرى أيضًا).

وأخيرًا، قم بتمكين التحقق من خطوتين (وتسمى أيضًا مصادقة ثنائية أو متعددة العوامل). حيث أنه يستخدم كلمة المرور الأساسية ولكنه يضيف أيضًا خطوة ثانية، مثل رمز يتم إرساله إلى هاتفك الذكي أو تطبيق ينشئ الرمز لك. ربما يمثل التحقق من خطوتين أهم خطوة يمكنك اتخاذها لحماية حساباتك على الإنترنت، وهي أسهل بكثير مما تعتقد.

3. التحديث: تأكد من تحديث جميع البرمجيات والتطبيقات إلى أحدث إصدار في جميع أجهزة الكمبيوتر والأجهزة المحمولة. حيث يبحث مهاجمو الإنترنت باستمرار عن نقاط ضعف جديدة في البرنامج الذي تستخدمه أجهزتك. عندما يكتشفون نقاط الضعف، يستخدمون برامج خاصة لاستغلالها والتسلل إلى الأجهزة التي تستخدمها. وفي الوقت نفسه، فإن الشركات التي أنشأت البرنامج لهذه الأجهزة تعمل بجد لإصلاحها من خلال إصدار التحديثات. وعليك التأكد بشكل دوري من قيام أجهزة الكمبيوتر والأجهزة المحمولة بتثبيت هذه التحديثات على الفور، فإنك تجعل من الصعب على شخص ما اختراقك. وللتأكد من التحديث الدائم، ما عليك سوى تمكين التحديث التلقائي كلما أمكن ذلك. تنطبق هذه القاعدة على أي تقنية متصلة بشبكة تقريبًا، بما في ذلك أجهزة التلفزيون المتصلة بالإنترنت أو أجهزة مراقبة الأطفال أو الكاميرات الأمنية أو أجهزة التوجيه المنزلية أو أجهزة الألعاب أو حتى سيارتك.

4. النسخ الاحتياطي والاسترداد: في بعض الأحيان، بغض النظر عن مدى حرصك، قد يتم اختراقك. إذا كان هذا هو الحال، فغالبًا ما تكون الطريقة الوحيدة لاستعادة جميع معلوماتك الشخصية هي النسخة الاحتياطية. تأكد من عمل نسخ احتياطية منتظمة لأية معلومات مهمة وتحقق من أنه يمكنك استعادة بياناتك منها. تدعم معظم أنظمة التشغيل والأجهزة المحمولة النسخ الاحتياطي التلقائي، إما لمحركات الأقراص الخارجية أو السحابة.

الضيف المحرر

ستيف أنسون مدرب معتمد من SANS، ويقدم إرشادات إلى فرق أمن تكنولوجيا المعلومات والحكومات في جميع أنحاء العالم لتحسين وضعهم الأمني. ستيف مؤلف الكتاب القادم «الاستجابة للحوادث التطبيقية» ويوفر موارد مجانية لممارسي أمن تكنولوجيا المعلومات على موقع www.AppliedIncidentResponse.com.

مصادر إضافية

Social Engineering: https://www.sans.org/u/W3G
Personalized Scams: https://www.sans.org/u/W3Q
Making Passwords Simple: https://www.sans.org/u/W3V
Got Backups: https://www.sans.org/u/W40