كلمات المرور القوية والمصادقة متعددة العوامل

كلمة المرور هي القفل على معظم حساباتنا، ويحاول المهاجمون فتحه بطرق كثيرة. فهم يخمنون كلمات المرور الشائعة، ويجربون كلمات مرور تسربت من مواقع أخرى، ويخدعون الناس ليكشفوها. وتشكل إرشادات المعهد الوطني الأمريكي للمعايير والتقنية، المعروف باسم NIST، جزءاً كبيراً من نصائح اليوم. وهي تفضل الطول على القواعد المعقدة، وتدعم مديري كلمات المرور وخطوات التحقق الإضافية. ويحسن تامر، وهو مدير مكتب، أمان حساباته بأربع عادات.

1. العبارات المرورية الطويلة

العادة الأولى هي تفضيل كلمات المرور الطويلة. والعبارة المرورية المكونة من عدة كلمات عشوائية أسهل في التذكر من كلمة مرور قصيرة ومعقدة، وأصعب بكثير في التخمين. وينصح NIST بعدم فرض الرموز الخاصة والتغيير المنتظم، لأن الناس عندئذ يختارون أنماطاً متوقعة. والكلمات المرتبطة باسمنا أو تاريخ ميلادنا أو فريقنا المفضل ضعيفة، حتى عندما تكون طويلة. والطول مع عدم القابلية للتوقع يصنعان القوة.

مثال: تستبدل عائلة كلمة مرور الواي فاي بأربع كلمات لا علاقة بينها تستطيع تذكرها. وباستخدام العبارة المرورية الطويلة، تحصل على كلمة مرور يسهل على العائلة تذكرها ويصعب على غريب تخمينها.

في العمل: يغير تامر كلمة مرور بريده من رمز قصير بالرموز إلى أربع كلمات لا علاقة بينها. وباستخدام العبارة المرورية الطويلة، يتذكرها دون ملاحظات، وتحتاج برامج التخمين إلى وقت أطول بكثير لكسرها.

2. كلمات مرور فريدة ومدير

العادة الثانية هي استخدام كلمة مرور مختلفة لكل حساب. وعندما يسرب موقع كلمات المرور، يجرب المهاجمون التركيبة نفسها في مواقع أخرى، فقد تفتح كلمة مرور مكررة أبواباً كثيرة. ولا يستطيع أحد تذكر عشرات كلمات المرور الطويلة، لذلك يخزنها مدير كلمات المرور بأمان ويدخلها تلقائياً. ويكفي عبارة مرورية قوية واحدة لفتح المدير. وتدعم إرشادات NIST استخدام مديري كلمات المرور.

مثال: لنتخيل أن متجراً سرب كلمات مرور عملائه. وبما أننا استخدمنا كلمات مرور فريدة مخزنة في مدير، يبقى حسابنا المصرفي آمناً لأن كلمة مروره كانت مختلفة.

في العمل: يكتشف تامر أنه استخدم كلمة مرور واحدة لست أدوات عمل. وبكلمات مرور فريدة مع مدير كلمات المرور، ينشئ كلمة جديدة لكل أداة، فلا يهدد تسرب في موقع واحد بقية الأدوات.

3. إضافة عامل ثان

العادة الثالثة هي المصادقة متعددة العوامل، وتسمى اختصاراً MFA. وهي تطلب إثباتين أو أكثر من أنواع مختلفة: شيئاً نعرفه مثل كلمة المرور، وشيئاً نملكه مثل الهاتف أو مفتاح الأمان، وشيئاً نكونه مثل بصمة الإصبع. وحتى لو سرق مهاجم

حقوق الطبع والنشر محمية © - أكاديمية أساسيات (شركة أساسيات للخدمات الاستشارية)

كلمة المرور، يبقى الإثبات الثاني ناقصاً. والبريد الإلكتروني والحسابات المصرفية وحسابات العمل أفضل أماكن للبدء. وعادة لا يستغرق إعدادها سوى دقائق قليلة.

مثال: يطلب مصرف كلمة مرور ثم رمزاً من تطبيق على هاتفنا. وبإضافة عامل ثان، يبقى اللص الذي يعرف كلمة المرور عاجزاً عن دخول الحساب.

في العمل: يفعل تامر المصادقة متعددة العوامل لبريد الشركة. وبإضافة عامل ثان، يحبط محاولة دخول من بلد آخر، لأن المهاجم يملك كلمة المرور ولا يملك هاتفه.

4. اختيار طرق أقوى

العادة الرابعة هي اختيار أقوى عامل ثان متاح. والرموز الصادرة عن تطبيق مصادقة أو مفتاح أمان مادي أكثر أماناً عموماً من الرموز المرسلة برسالة نصية، لأن الرسائل النصية قد تعترض أو تحول. وتستطيع مفاتيح الأمان ومفاتيح المرور أيضاً مقاومة المواقع المزيفة، لأنها تتحقق من العنوان الحقيقي. ولا نشارك رمزاً مع أحد، ونغير كلمة المرور عند وجود دليل على انكشافها. وينبغي حفظ خيارات احتياطية بأمان تحسباً لضياع الهاتف.

مثال: يستولي محتال على رقم هاتف أحد أفراد العائلة، فتصل الرموز النصية إلى الشخص الخطأ. وباختيار طريقة أقوى، ينتقل إلى تطبيق مصادقة، فتبقى الرموز على هاتفه.

في العمل: يعطي تامر فريق المالية مفاتيح أمان لبوابة المصرف. وباختيار طريقة أقوى، يجعل سرقة الدخول عبر صفحة مزيفة أصعب بكثير.

الخاتمة

وخلاصة القول، يقوم أمان الحسابات القوي على أربع عادات. فنستخدم عبارات مرورية طويلة، وكلمة مرور مختلفة لكل حساب، وعاملاً ثانياً، وأقوى عامل ثان متاح. وتدعم إرشادات NIST الطول ومديري كلمات المرور والتحقق الإضافي، وتنصح بعدم فرض التعقيد والتغيير الروتيني. وحسابات تامر اليوم أصعب بكثير على الاختراق. والتغييرات الصغيرة التي نقوم بها مرة واحدة تمنح حماية كل يوم.

المصادر

- المعهد الوطني الأمريكي للمعايير والتقنية (NIST): المنشور الخاص 800-63B، إرشادات الهوية الرقمية، المصادقة وإدارة وسائلها – https://pages.nist.gov/800-63-4/sp800-63b.html
- وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA): استخدام كلمات مرور قوية – https://www.cisa.gov/secure-our-world/use-strong-passwords
- المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC): ثلاث كلمات عشوائية – https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

حقوق الطبع والنشر محمية © - أكاديمية أساسيات (شركة أساسيات للخدمات الاستشارية)