كبسولة تأمين الدخول

- كلمات المرور والتحقق المتعدد -

كبسولة تأمين الدخول

(كلمات المرور والتحقق المتعدد)

مقدمة

كلمات المرور هي أشهر الوسائل التي نحمي بها حساباتنا وأجهزتنا، لكن مع تطور تقنيات الاختراق، صار من اللازم أن نستخدم كلمات مرور أقوى، وصار أيضا من المنطقي ألا نعتمد على كلمات المرور وحدها، فيمكننا إما أن نستخدم وسائل أخرى بالإضافة إليها، أو أن نعتمد على وسائل مختلفة للتحقق من هوياتنا غير كلمات المرور أساسا. نسعى في هذا الدليل إلى تغطية بعض المفاهيم والأدوات الهامة بخصوص حماية وتأمين دخولنا إلى حساباتنا الإلكترونية، فنتناول أهم الممارسات المتعلقة بكلمات المرور، والوسائل الأخرى للتحقق التي يمكن استخدامها إلى جانب كلمات المرور أو بديلا عنها، وتطبيقات إدارة كلمات المرور وبعض النصائح عند استخدامها.

جـــدول المحتويات

ما خياراتنا؟

عند دخولنا إلى أجهزتنا وحساباتنا التي نحميها بطرق مختلفة، فإن من يتحقق من هوياتنا آلات، وتتحق الآلات من هويتنا بواحدة (أو أكثر) من ثلاثة أنواع من طرق تأكيد الهوية:

1. شيء نعرفه

يمكننا اختيار معلومات نتذكرها ونقدمها عند الحاجة مثل إدخال كلمة المرور لفتح الحساب أو رسم نمط لفتح الهاتف أو الإجابة عن أسئلة التحقق عند نسيان كلمة المرور مثلا. وهذه الطريقة إحدى أشهر طرق تأكيد الهوية، لكنها تعتمد على ذاكرة الشخص ولهذا فإنها ليست فعالة دوما، خصوصا عند اختيار كلمات مرور مختلفة لكل حساب مثلا.

2. شيء نملكه

نتجنب في هذه الطريقة الاعتماد على ذاكرة الإنسان التي قد تنسى أو تختلط عليها المعلومات المختلفة، فتعود إلى الطريقة التي نفتح بها باب المنزل مثلا (باستخدام مفتاح نحرص على حيازته والحفاظ عليه من الضياع) فبدلا من الاعتماد على كلمة مرور نعتمد على شيء مادي بحوزتنا مثل الهاتف أو خط الهاتف (عندما نطلب إرسال كود تأكيد إلى الهاتف، فنحن نعتمد على حيازتنا لهذا الهاتف) أو استخدام مفتاح الدخول المادية (سنوضحها لاحقا).

3. شيء فينا

لأننا ننسى كلمات المرور، وقد نضيع ممتلكاتنا، فإن أسهل ما يمكننا استخدامه لتأكيد الهوية (بالنسبة للمستخدم) هو أنفسنا، ومع تطور التكنولوجيا صار بإمكان الأجهزة التحقق من بصمة العين أو الوجه أو الإصبع، وهذه تعرف بالبيانات البيومترية، لكن هذه الطرق تتطلب أجهزة تدعم وسائل تحقق من البيانات البيومترية خصوصا، لهذا فهي ليست شائعة على مستوى الحسابات إنما على مستوى الأجهزة.

نصائح عامة

كلمات مرور قوية

إحدى الطرق التي يمكن كسر كلمات المرور بها هي استخدام برمجية تقوم بتجربة العديد من كلمات المرور المكنة، وكلما كانت كلمات المرور قوية ومعقدة كان من الأصعب على هذه البرمجيات تخمينها، فإذا بدأت هذه البرمجية بتخمين الأرقام بشكل تصاعدي، وكانت كلمة المرور هي 99999999، فهذا يعني أن البرمجية ستقوم بمائة مليون محاولة، وهذا لن يستغرق وقتا طويلا مع قوة المعالجات الموجودة حاليا، أما إذا كانت كلمة المرور تتألف من حروف كبيرة وصغيرة ورموز وأرقام وزاد طولها عن 16 حرفا فلن تتمكن برمجية كهذه من كسر كلمة المرور هذه في فترة حياة المهاجم. لهذا يُنصح دوما بتعقيد كلمة المرور عبر جعلها تتألف من:

- 16 حرفا أو أكثر
- حروف صغيرة (abc)
- حروف كبيرة (ABC)
- أرقام (123)
- رموز (!@#)

5^38KJ5UbbFPt&XAW!ou2
397M6J&79ADuzk6OdG@h
D%An.Sa3Xmg#kGHFpYSX
KbZZ!TUUdUozmTrXV3JKH
n!2euC2.F#uzk!fYPsn!Sa*3

كلمات مرور فريدة

إذا كانت كلمة المرور التي تستخدمها قوية للغاية ومعقدة لكنك تستخدمها لجميع الحسابات، وحدث خرق أمني في أحد المواقع التي تستخدمها أدى إلى تسريب كلمات المرور وعناوين البريد الإلكتروني للمستخدمين، فيمكن للمهاجم ببساطة أن يجرب نفس كلمة المرور على المواقع الشهيرة الأخرى، وسيتمكن بذلك من الوصول إلى جميع حساباتك الأخرى. لهذا يجب أن يكون لكل حساب كلمة مرور فريدة تختلف عن كلمات مرور الحسابات الأخرى.
(لن نطلب منك حفظ كل هذه الكلمات المعقدة في ذاكرتك، سنقدم حلا في الصفحات التالية)

كلمات مرور عشوائية

الاعتماد على خيالنا في ابتكار كلمات مرور يجعلنا نواجه خطر تكرار كلمات مرور تم استخدامها سابقا أو جعل هذه الكلمات قابلة للتوقع مع تطور أدوات كسر كلمات المرور وأدوات الذكاء الاصطناعي. فمثلا إذا قررنا استخدام كلمة password مع تغيير بعض الحروف حتى لا يمكن تخمينها فصارت P@$$w0rd وبحثنا عن هذه الكلمة في قاعدة بيانات للاختراق ↓ ، سنجد أن هذه الكلمة قد تم استخدامها في 34,168 حسابا تم تسريب بياناته.

ما هي قواعد بيانات الاختراقات؟
عند اختراق خدمة أو منصة أو موقع أحيانا ما ينشر المهاجم البيانات التي حصل عليها من خلال هذا الاختراق، وتقوم بعض المنصات بجمع تلك البيانات لتساعد الناس على البحث عن معلوماتهم ومعرفة إذا كانت قد تعرضت للتسريب من قبل أو لا. استخدمنا هنا موقع Have I Been Pwned والذي يسمح بالبحث عن عناوين البريد الإلكتروني وأرقام الهاتف وكلمات المرور التي تعرضت للتسريب من قبل، ومن المفيد أن نشترك لتلقي التنبيهات أو أن نتحقق من بياناتنا في هذا الموقع كل فترة.

ولضمان عشوائية كلمة المرور لا يجب أن يعتمد الشخص على نفسه إنما يجب الاعتماد على أدوات خارجية مثل مولدات كلمات المرور الموجودة في معظم أدوات إدارة كلمات المرور، أو إذا كان بحاجة إلى حفظها يمكنه توليد عبارة مرور ↓ ، إما باستخدام مدير كلمات المرور (وهو الخيار الأسهل والأقوى) أو باستخدام النرد (وهو أمر ممتع أكثر).

ما هي عبارة المرور (passphrase)؟
هي بديل لكلمة المرور يتألف من سلسلة من الكلمات المفهومة، وتتميز بأنها قابلة للحفظ في الذاكرة أكثر من كلمات المرور الاعتيادية.
(مثال: eardrum-swan-fridge-pushing-trustee-vitamins)
في هذا المثال لدينا 6 كلمات تفصل بينها علامة (-) وهي قابلة للحفظ وصعبة التخمين حتى باستخدام برمجيات الحاسب.

كيف يمكن توليد عبارة مرور باستخدام النرد؟

1. أحضر النرد وقم بإلقائه خمس مرات مع تدوين النتيجة في كل مرة، فإذا كانت النتيجة في المرة الأولى 2، وفي الثانية 6، وفي الثالثة 1، وفي الرابعة 2، وفي الخامسة 5، يصبح الرقم النهائي 26125
2. ابحث في قائمة كلمات كبيرة مخصصة لهذا الأمر، مثل **قائمة EFF** عن الكلمة المقابلة لهذا الرقم، فستجد أنها excavate
3. كرر الأمر بعدد الكلمات التي تريدها في عبارة مرورك. مثال:

2	6	1	2	5	excavate
6	1	5	3	4	t-shirt
3	4	5	1	6	impolite
1	5	4	2	3	chase
3	1	5	2	1	fridge

4. قرر كيف ستفصل بين كل كلمة والأخرى، (دون فاصل، بمسافة، (-)، أن تبدأ كل كلمة بحرف كبير، إلخ)، الأمر يعود إليك.

كلمات مرور متجددة

يعتمد هذا على بضعة عوامل، لكن لا يجب أن تقوم بتغيير كلمات المرور التي تحتفظ بها في ذاكرتك كثيرا، مثل كلمة مرور برنامج إدارة كلمات المرور، أما الكلمات التي تحتفظ بها في مدير كلمات مرور فيجب تغييرها حسب أهميتها واحتمالية تعرضها للكشف، فيُفضل تغيير كلمات المرور للحسابات المهمة كل بضعة أشهر، خصوصا إذا لم يكن بها وسيلة مفعلة للتحقق المتعدد.

التحقق المتعدد

مع تطور تقنيات الاختراق، أصبح عدد كبير من المواقع والتطبيقات يدعم طرقا إضافية للتحقق من هوية صاحب الحساب. إذ لا تكتفي تلك المواقع بالحاجة لكلمة مرور للدخول إلى الحسابات عليها، بل تستلزم وسيلة إضافية للتأكد من أن صاحب الحساب الفعلي هو من يحاول الدخول إليه. وهناك العديد من الخيارات للتحقق المتعدد وهي تختلف في قوتها، لكنها تعتمد بشكل أساسي على طلب طريقتين في تأكيد الهوية:

- **شيء نعرفه** وهو كلمة المرور
- **شيء نملكه** وهو ما نستخدمه في الوسيلة الإضافية

الرسائل النصية

الشيء الذي نملكه في هذه الطريقة هي شريحة الهاتف التي نستقبل عليها الرسائل، وهي ليست منيعة لأنها قابلة للسرقة أو الاعتراض، فشركة الاتصالات (وبعض من يعملون بها) قادرة على الوصول إلى محتوى الرسائل النصية المرسلة إلى أرقام الهواتف التابعة لها، وبينما هذه الطريقة ليست ضمن أقوى طرق التحقق الإضافية، لكنها بالطبع أفضل من عدم استخدام وسيلة تحقق إضافية على الإطلاق.

إشعارات الموافقة

تعتمد هذه الطريقة على إرسال إشعار إلى الأجهزة الأخرى التي تستخدم حسابك عليها وتطلب منك التأكيد على عملية تسجيل الدخول. (مثال: عند محاولة تسجيل الدخول إلى حسابك على فيسبوك من حاسب جديد، يرسل فيسبوك إشعارا عبر تطبيق فيسبوك على هاتفك ويطلب منك الموافقة أولا على عملية تسجيل الدخول هذه)، وهذا يعني أن الشيء الذي تملكه هنا هو جهازك الذي قمت بتسجيل الدخول عليه من قبل، وهذه الطريقة أفضل من الرسائل النصية في أن المهاجم بحاجة إلى الاستيلاء على أحد أجهزتك حتى يستطيع الدخول إلى حسابك.

تطبيقات المصادقة

تعد هذه التطبيقات أشهر طريقة للتحقق الإضافي وتتطلب وجود تطبيق مصادقة على جهازك تقوم من خلاله بمسح رمز استجابة سريعة (QR code) واستقبال أكواد متغيرة كل 30 ثانية على التطبيق يمكن استخدامها عند تسجيل الدخول.

كيف تعمل الأكواد المتغيرة؟
تعتمد الأكواد المتغيرة على ما يسمى بالسر المشترك (shared secret) وهو مفتاح يقدمه لك الموقع في صورة رمز استجابة سريعة (QR code) وعند مسحه باستخدام التطبيق يحتفظ التطبيق بهذا المفتاح ويعتمد عليه وعلى الساعة في استخراج كود يتغير كل 30 ثانية، وإذا حصل أي شخص على هذا المفتاح يمكنه استخراج نفس الأكواد، لكن لا يمكن أبدا استنتاج المفتاح من خلال الأكواد المتغيرة.

تعمل جميع تطبيقات المصادقة تقريبا بنفس الطريقة، لذا يمكن استخدام أي تطبيق مصادقة للحصول على هذه الأكواد، لكن يفضل استخدام تطبيقات

توفر خيارات جيدة، مثل تأمين التطبيق بكلمة مرور أو إمكانية استخراج نسخة احتياطية من الأكواد عند الرغبة في تغيير الجهاز أو تغيير التطبيق.

	ente Auth	Aegis Authenticator	Google Authenticator
مفتوح المصدر	✅	✅	❌
النسخ الاحتياطي	✅	✅	محدود
قفل التطبيق	قفل الشاشة	كلمة مرور البصمة	❌
يعمل على أنظمة	أندرويد، iOS، ويندوز، لينكس، macOS، الوب	أندرويد	أندرويد، iOS

نرشح استخدام ente Auth لأنه يوفر خيارات جيدة ويعمل على أكبر عدد من الأجهزة كما أنه يدعم إنشاء حساب للمزامنة ويعمل أيضا دون وجود حساب، ولأجهزة أندرويد خصيصا يمكن استخدام Aegis Authenticator للمزيد من الخيارات لكنه لا يدعم إنشاء حسابات للمزامنة. ولا ننصح باستخدام Google Authenticator إلا لمن يجدون استخدام تطبيقات المصادقة مرهقا، فهو الأسهل بينها وبوسعه مزامنة الأكواد مع حسابات جوجل، لكن خيارات الأمان به أضعف مقارنة بالتطبيقين الآخرين.

مفاتيح الدخول المادية

مفاتيح الدخول المادية (hardware security keys) وسيلة مصادقة جيدة جدا لكنها ليست دائما متوفرة بسهولة وبسعر رخيص، وهذه المفاتيح هي أدوات يمكن توصيلها بالحاسب أو الهاتف للتأكيد عند دخول الحساب، فتعمل كما تعمل مفاتيح الباب، وتختلف هذه المفاتيح فيما بينها، فلها أنواع كثيرة وتعمل بطرق مختلفة، فمنها ما يتصل عبر منفذ USB ومنها ما يتصل عبر منفذ USB-C ومنها ما يتصل عبر خاصية NFC وتأتي هذه المفاتيح بأشكال وأحجام مختلفة لتناسب الاستخدامات المختلفة.
أشهر المفاتيح المادية هي مفاتيح YubiKey.

مدير كلمات المرور

عند الحديث عن أهمية اختيار كلمات مرور قوية ومعقدة تختلف من حساب إلى آخر وتغييرها كل فترة، يرى الكثيرون أن هذا غير واقعي بسبب عدم قدرة الناس على تذكر هذه المعلومات المعقدة والمتغيرة بسهولة، أو يلجأ البعض إلى كتابة كلمات المرور في أماكن غير آمنة مثل تطبيق الملاحظات أو في دفتر وهو ما يعرض بياناتهم إلى خطر السرقة. الحل الأمثل لحفظ كلمات المرور هو استخدام تطبيق لإدارة كلمات المرور يضع له المستخدم كلمة مرور رئيسة ويحفظ باقي كلمات مروره داخل هذا التطبيق فلا يحتاج إلى تذكرها بنفسه. تتميز هذه التطبيقات باحتوائها أيضا على أدوات لتوليد كلمات مرور قوية ولدى بعضها إضافات للمتصفح تسمح للتطبيق بأن يملأ بيانات تسجيل الدخول بشكل تلقائي، ولهذه التطبيقات نوعين أساسيين:

الأول: يتصل بالإنترنت

يسمح هذا النوع للمستخدم بإنشاء حساب على خادم ما، ويحتفظ بكلمات مرور المستخدم على هذا الخادم بطريقة مشفرة، بحيث يمكنه الوصول إلى كلمات مروره على أي جهاز باستخدام هذا التطبيق بعد تسجيل الدخول عليه باستخدام كلمة المرور الرئيسة.

التطبيق الذي نرشحه من هذا النوع هو **Bitwarden** وهو يعمل على معظم أنظمة تشغيل الهواتف والحواسيب ويمكن إضافته إلى معظم المتصفحات.

الثاني: لا يتصل بالإنترنت

يحتفظ هذا النوع بكلمات مرور المستخدم بشكل مشفر في ملف على الجهاز، وحتى يصل المستخدم إلى كلمات مروره باستخدام جهاز آخر يجب عليه نقل هذا الملف إلى الجهاز الآخر.

من هذا النوع نرشح عائلة التطبيقات المبنية على KeePass

	KeePassXC	KeePassDX	Strongbox
يدعم أنظمة	ويندوز، لينكس، macOS	أندرويد	iOS, iPadOS, macOS

لا تضع البيض في سلة واحدة

رغم أن استخدام مدير لكلمات المرور قد يبدو حلا رائعا للعديد من المشاكل المرتبطة بكلمات المرور، لكن للوقاية من مخاطر وقوع حساب المستخدم على مدير كلمات المرور في يد أحد المهاجمين عبر خداعه لإرسال كلمة السر مثلا، لا

يجب وضع كل شيء بالكامل في مكان واحد، فيمكن للمستخدم مثلا الاحتفاظ بكلمات مروره في أحد تطبيقات إدارة كلمات المرور، والاحتفاظ بمفاتيح المصادقة التي يستخدمها لاستخراج أكواد التحقق المتغيرة في مكان آمن آخر، مثل تطبيق ملاحظات آمن ومشفر أو مدير كلمات مرور مختلف، وهذا بهدف توزيع البيانات حتى إذا استولى أحد على حساب مدير كلمات المرور لا يصبح في يده تحكما كاملا بكل الحسابات وتسقط جميع حوائط دفاع المستخدم في نفس اللحظة.

النسخ الاحتياطي

سواء أقمنا باستخدام مدير كلمات مرور يتصل بالإنترنت أو لا، يجب الاحتفاظ بنسخة مشفرة من بياناتنا المحفوظة عليه وتحديثها من وقت لآخر والإبقاء عليها في مكان آمن حتى نتمكن من استعادتها في أي ظرف، وقد يكون هذا المكان خزنة مشفرة على أحد الأقراص أو مساحة تخزين سحابية لدى مقدم خدمة جيد السمعة، ما يهم هو قدرتنا على الوصول إلى هذه النسخة الاحتياطية عند الحاجة.