كيف تجعل من وحدة

USB

وسيلة تحقق إضافية لجهازك

EUROPEAN
ENDOWMENT FOR DEMOCRACY

كيف تجعل من وحدة USB
وسيلة تحقق إضافية لجهازك

التحقق بخطوتين هو وسيلة فعالة لحماية الحسابات والأجهزة، ففي حين أن الدخول إلى الحساب أو إلى جهاز يتطلب شيء تعرفه، وهو ما يتمثل في كلمة المرور، يضع التحقق بخطوتين متطلب إضافي إلى جانب كلمة المرور للدخول إلى الحساب، وهو شيء تملكه. ذلك المتطلب الإضافي يجعل حسابك أكثر أمانًا، فحتى إذا استطاع أحدهم الوصول إلى كلمة مرورك، لن يستطيع الدخول إلى الحساب دون الوصول إلى (أداة التحقق؟).

توجد عدة وسائل للتحقق بخطوتين أكثرهم استعمالًا هو الرمز المصادقة الرقمي، بعض المواقع ترسل الرمز إلى الهاتف في رسالة نصية، ويمكن أيضًا استعمال أحد تطبيقات المصادقة التي تولد رمز متغير.

ليست تلك هي الوسائل الوحيدة للتحقق بخطوتين، فهناك عدة وسائل أخرى، أغلبها يعتمد على هاتفك بشكل أو بآخر الذي قد يتعرض للسرقة أو قد تكون بطاريته فارغة عندما تحتاج إليه، ولكن هناك وسيلة أخرى تحقق أيضًا متطلب "شيء تملكه" وهي مفتاح الأمان.

مفتاح الأمان هو جهاز صغير للمصادقة الثنائية وتأمين الحسابات، لا يعتمد على عرض رمز رقمي كالوسائل الأخرى وإنما يعتمد على بروتوكول المصادقة FIDO2 الذي يحتاج فقط إلى توصيله بالكومبيوتر أو الهاتف عند الدخول إلى حسابك.

هناك عدة شركات توفر مفاتيح الأمان مثل يوبيكو (Yubico) وجوجل وغيرهم، ورغم أنها رخيصة الثمن نسبيًا إلا أنها في النهاية تكلف المال، وعليك شرائها. وبينما هي خيار أفضل للحسابات التي تتطلب مستوى تأمين عالي (عال؟)، إنما يمكن للمستخدمين العاديين أن يعدّوا

مفاتيح أمان بأنفسهم لتأمين حساب المستخدم على الكمبيوتر لديهم. كل ما يحتاجونه هو وحدات تخزين USB؟ وتثبيت أحد البرامج المجانية أو رخيصة الثمن.

في هذا الدليل؟ سنشرح لك كيفية إعداد مفتاح أمان لحساب المستخدم على ويندوز وماك ولينُكس.

في البدء نود الإشارة إننا ننصح بتجربة الأدلة العملية التي تتضمن تغييرات في النظام على نظام تشغيل غير الذي تعتمدون/ تعتمدن عليه، أو حتى جهاز إفتراضي Virtual Machine، لتفادي أي مشاكل يمكن تؤثر على أجهزتكم/ن، فكروا/ فكرن في هذا الدليل كمساحة للعب والتعلم في قلب جدية موضوعات السلامة الرقمية.

كيف تعد مفتاح أمان USB على ويندوز

إعداد مفتاح الأمان على ويندوز أسهل قليلًا من لينُكس وماك:

1. زُر صفحة USB Raptor وحمّل البرنامج من هنا.
2. حفظ البرنامج على جهازك.
3. استخرج مجلد USB Raptor من الملف المضغوط.
4. شغّل برنامج USB Raptor.
5. اقرأ الشروط والأحكام ثم أكد على موافقتك عليها بالضغط على مربع الاختيار بجانب "I Agree".
6. قم بتوصيل وحدة تخزين USB إلى جهازك.
7. في خانة التشفير "Encryption"، أدخل كلمة مرور قوية لكن تستطيع تذكرها.
8. اضغط على قائمة "Select USB Drive" المنسدلة في قسم "Unlock File Creation" واختر وحدة تخزين USB التي قد وصلتها.
9. اضغط على زر "Create k3y File".
10. الآن اضغط على مربع الاختيار بجانب "Enable USB Raptor" في قسم "USB Raptor Status".

عند هذه النقطة إزالة وحدة تخزين USB سيؤدي إلى قفل سطح المكتب حيث سيبدأ USB Raptor في العمل. ولكن لضمان تفعيل USB Raptor كل مرة تشغل فيها جهازك عليك القيام بالخطوات التالية.

لتخصيص إعدادات إضافية مثل إعداد كلمة مرور احتياطية في حال فقدان وحدة تخزين USB، أو إعدادات بدء التشغيل، أو إعداد مهلة انتظار قبل قفل سطح المكتب عند إزالة وحدة تخزين USB، اضغط على مربع اختيار "الإعدادات المتقدمة".

ألقِ نظرة على الإعدادات واختر منها الذي ترغب في إعداده لوحدة التخزين خاصتك. ننصح بالإعدادات التالية:

Run USB Raptor at Windows startup

Start in the system tray

USB Raptor always starts armed

تضمن هذه الإعدادات عمل USB Raptor بشكل تلقائي عند تشغيل الجهاز. ولإيقاف USB Raptor، فقط اضغط على العلامة من مربع اختيار "Enable USB Raptor" لإزالتها.

عند تفعيله، سيحمي USB Raptor جهازك من الدخول غير المصرح به عن طريق قفل سطح المكتب ما دامت وحدة تخزين USB غير موصولة.

كيف تعد مفتاح أمان USB على ماك

إعداد مفتاح الأمان على ماك أمر سهل حتى وإن كنت لم تستعمل ماك من قبل

1. زُر صفحة Rohos Logon Key for Mac من هنا وحمل البرنامج.
2. استخرج المجلد من الملف المضغوط.
3. شغل ملف Rohos Logon Installer واضغط على متابعة.

4. اضغط على "Continue"، ثم "Agree"، ثم "Install for all users of this computer"، ثم "Continue"، وأخيرًا "Install".
5. قد يتطلب منك الكمبيوتر إدخال اسم المستخدم وكلمة المرور، إذا طلب منك، أدخل البيانات ثم ثم اضغط تثبيت البرنامج "Install software".
6. بعد اكتمال التثبيت، اضغط اغلاق "Close".
7. الآن قم بتوصيل وحدة تخزين USB إلى جهازك.
8. افتح Rohos Logon Key واختر USB drive لإعداد وحدة تخزين USB الخاصة بك كأداة المصادقة.
9. أدخل اسم، وكلمة مرور (إذا رغبت)، وأداة المصادقة من النافذة، ثم اضغط OK.
10. اختر خيار قفل سطح المكتب Lock the Desktop من القائمة المنسدلة المسماة USB removal action. جهازك الآن محمي بـ Rohos.

كيف تعد مفتاح أمان USB على لينُكس

باستعمال وحدات المصادقة القابلة للتوصيل (PAM: Pluggable Authentication Modules)، يمكنك جعل مفاتيح أمان USB وسيلة المصادقة الأساسية أو الثانوية.

في حين أن الخطوات التي سنسردها هي خاصة بتوزيعة أوبونتو، بإمكانك استعمال الأوامر المكافئة على التوزيعات الأخرى لإعداد مفاتيح أمان USB على لينُكس.

1. ثبّت الحزم المطلوبة للمصادقة عبر PAM عن طريق إدخال الأمر التالي في سطر الأوامر (what is a proper translation for terminal):

```
$ sudo apt-get install pamusb-tools libpam-usb
```

2. الآن أدخل وحدة تخزين USB في جهازك واستعمل أمر pamusb-conf لإعدادها كما يلي:

```
$ sudo pamusb-conf –add-device
```

3. سيظهر التالي ليطلب منك اختيار وحدة تخزين USB من الأجهزة المتاحة:

.Please select the device you wish to add

*Using “Verbatim STORE N GO *
((Verbatim_STORE_N_GO_07A10D0894492625-0:0)” (only option*

? Which volume would you like to use for storing data

*(****-**** :dev/sdb2 (UUID/ (0*

*(****-**** :dev/sdb1 (UUID/ (1*

:[0-1]

4. أدخل الرقم الموافق لوحدة تخزين USB المراد إعدادها. سيتم إعداد وحدة التخزين وستُسأل عما إذا كنت ترغب بحفظ الإعدادات

: Name

Vendor : Verbatim

Model : STORE N GO

*Serial : Verbatim_STORE_N_GO_**********-0:0*

*UUID : ***-**** *

? Save to /etc/pamusb.conf

[Y/n]

5. أجب بنعم عبر إدخال حرف Y

سيظهر لك Done للدلالة على حفظ الإعدادات

بعد هذه الخطوة، سيتم تحديث ملف /etc/pamusb.conf تلقائيًا لتعريف وحدة تخزين USB الخاصة بك.

6. بعد إعداد الجهاز، يجب إعداد مستخدم. في حين أنه يمكن إعداد عدة أجهزة PAM بعدة مستخدمين لكل منها، الأمر التالي يوضح كيفية إعداد مستخدم واحد للجهاز الذي أعددناه سابقًا، باستعمال هذا الأمر ستربط حساب المستخدم الذي تستعمله بوحدة USB.

```
sudo pamusb-conf –add-user $
```

7. ستُسأل عن الجهاز الذي ترغب في استعماله للمصادقة، ثم ستُسأل عما إذا كنت ترغب في حفظ الإعدادات

Which device would you like to use for authentication ?

*(Using “” (only option **

User :

Device :

Save to /etc/pamusb.conf ?

[Y/n]

8. أجب بنعم عبر إدخال حرف Y

سيظهر لك Done للدلالة على حفظ الإعدادات.

بعد هذه الخطوة، سيتم تحديث ملف /etc/pamusb.conf تلقائيًا لتعريف المستخدم الذي قد أعددناه.

9. بعد الإعداد الذي أتممته لوضع المصادقة يجب تعديل ملف المصادقة /etc/pam.d/common-auth/ (أو ملف /etc/pam/system-auth على أنظمة Fedora أو RedHat) لإعداد pam_usb ليكون ضمن عملية مصادقة النظام عبر تعديله ليتضمن التالي:

auth sufficient pam_usb.so

auth required pam_unix.so nullok_secur

10. بعد حفظ التعديلات، لنختبر ما قمنا بإعداده عبر الأمر التالي

$ su ubuntu-user

في حال نجاح الإعداد سيظهر التالي:

* *pam_usb v0.4.2*

* *(Authentication request for user "" (su*

* *(Device "" is connected (good.*

* *Performing one time pad verification...*

* *Regenerating new pads...*

* *Access granted.*

إذا لم يتم التعرف على المستخدم، استبدل "required" بـ "sufficient" في سطر ملف pam_usb.so السابق. سيتطلب هذا إعداد كلمة مرور أيضًا.

11. الآن لإعداد قفل النظام حسب اتصال وحدة USB عليك تعديل ملف /etc/pamusb.conf على النحو التالي، لقفل سطح المكتب كلما أُزليت وحدة USB:

gnome-screensaver-command -l

gnome-screensaver-command -d

12. احفظ/ي التعديلات

وأخيرًا، لقد نجحت في إعداد وحدة USB لتعمل كمفتاح أمان لنظام أوبونتو على جهازك! للتوزيعات الأخرى، ابحث عن الأوامر والملفات المكافئة.

بمفتاح الأمان الذي قد أعددته بوحدة USB، أنت الآن تؤمن جهازك الكمبيوتر لديك ضد استعمال أحدهم لكلمة المرور والوصول إلى بياناتك.
هناك استعمالات أخرى لمفاتيح الأمان، مثل تأمين الحسابات على المواقع المختلفة، إذا كنت ترغب في تأمين حساباتك على الويب، ألقِ نظرة على مفاتيح الأمان التي تقدمها يوبيكو وغيرها، فهي توفر ميزات أكثر من حيث دعمها للبروتوكول FIDO2 وأيضًا وسائل لحماية مفاتيح الأمان نفسها من العبث والاختراق.