
دليل الأمان المرئي للميم
وباقي الهرف

إسم الإصدار:
دليل الأمان الرقمي للميم وباقي الأحرف
جهة الإصدار:
مؤسسة مساحات للتعددية الجنسية والجندرية
تاريخ الإصدار: مارس ٢٠١٨

هذا العمل مرخّص برخصة المشاع الإبداعي
نسب المُصنَّف - غير تجاري - الترخيص بالمثل
4.0 دولي
(CC BY-NC-SA 4.0)

فهرس المحتويات

| مقدمة

من المعتاد فى كتيبات الأمان الرقمى أن تكون مستهدفة لفئات معينة، إلا أننى أرى أن هوياتنا فى تداخل وتقاطع دائم. كوننا ننتمي لذلك التعريف الشامل الجامع المسمى "الميم" لايحصر هويتنا وكياننا – وبالتالى جهات المخاطر والاستخدامات. مع وضع ذلك فى الإعتبار، سيحتوي هذا الكتيب المصور على بعض العناصر المعنية بالمدافعات/ين عن حقوق الميم بالأخص، وتطبيقات أو برمجيات مخصصة للميم بشكل أساسى. فيما عدا ذلك فهذا الكتيب يعنى "بباقى الأحرف" أيضاً فلا تتردد فى المشاركة وإقتراح التعديلات على الكتاب.

فى كل يوم تستيقظ، تفتح باب غرفتك، تتجه للحمام وتغلق الباب، تقضي حاجتك؛ تستعد للخروج وتغلق الدولاب (الخزانة)، تجمع أغراضك فى الحقيبة، تغلق الحقيبة؛ تخرج من المنزل وتغلق الباب وتوصده.

هل من الممكن أن تعيش من دون أن تغلق أغلب هذه الأشياء؟ هل غلقك لتلك العناصر يعنى بالضرورة أنك تخبىء شيئاً هو عاراً أو إجرامياً (بإختلاف جهات التعريف)؟ إذا كانت الإجابة نعم، فلديك مشكلة كبيرة (إذهب لحلها حالاً). أما إذا كانت لا، فكذلك يجب أن يكون أيضاً إعتنائك بالمعلومات والبيانات التى تصدرها فى كل لحظة من حياتك وتعاملاتك اليومية، كشخص يعيش فى القرن ال٢٠ وال٢١. لا مجال للجدال حول ذلك الأمر، فحيواتنا "الافتراضية" أو "الرقمية" هى جزء لا يجزأ من حيواتنا "اللاإفتراضية" أو "اللارقمية"، وكلاهما هو "الواقع".

يتعرض كل الأشخاص بمختلف انتمائاتهم، ومجتمعاتهم الصغيرة أو الكبيرة للعنف بإستخدام الوسائل الرقمية والتى تتماهى آثارها على حالتنا النفسية والصحية واليومية اللارقمية أيضاً، فالبعض يضطر لترك منزله، أو بلده، والآخر يلجأ للقانون، وهؤلاء يشهرون بمعتديهم، أما هؤلاء فينصاعوا. وبذلك يكون العنف الالكترونى الذى يمكن أن نتحدث عنه فى أبحاث كثيرة، هو الشئ الوحيد الذى تختلف فيه معايير الامتياز (Privilege).

ولكن بينما تصارعنا هنا نزعتان، الأولى هى التكنوفيليا (الولع بالتقنية) والأخرى هى التكنوفوبيا (رهاب التكنولوجيا)، نريد أن تصل إلى حل واقعي ورزين، وهو أن "التكنو" لاتضر ولاتنفع إلا إذا سمح المستخدم لها بذلك، وهنا يأتى دور معرفة الإستخدام الآمن لتلك الأدوات من أجل تحقيق أعلى إستفادة بأقل ضرر ممكن. ولكي نعرف ذلك فى البداية، لابد أن تعرف أحد أهم خصائص التقنيات الرقمية: أنها دائمة التغيير، وأن الكود ككل شىء لن يكون أبداً "محايداً".

فلندعه إذاً ينصفنا، ولايضرنا أو من حولنا بقدر الإمكان عن طريق "الإستخدام المسؤول للبيانات".

| فروق وتعريفات

الخصوصية

هى أن يكون لك غرفة بها باب، تستطيع غلقه أو لا، وتحديد أطر ووسائل تعامل الآخر مع غرفتك وبابها، من حيث معرفة محتواها أو لا. ولكن هذا لا يعنى بالضرورة «الأمان» لهذا المكان.

الأمان

إذا أكملنا على المثال أعلاه، فمن أجل الحفاظ على تلك الخصوصية من العبث المقصود والغير مقصود، ستقوم بوضع **قفل** على الباب، إذا تم العبث بهذا القفل، فقد تم إختراق حاجزك الأمنى وإختراق خصوصيتك. وبذلك فإن الأمان يعنى زيادة فى الخصوصية وليس العكس.

الشفافية

كثيراً ما يلتبس هذا المصطلح مع المصطلحين أعلاه، خاصة فى المستوى المؤسسى (مجتمعات مدنية ومؤسسات). إلا أن الشفافية مصطلح معنى بالنزاهة ووضوح آلية أخذ المعلومات، وتوفرها لأكبر عدد ممكن من المستخدمين، ولا يعنى أنها مرتع لمن يشاء ليخترقها. ومثالاً لما يفعله العبث بها هو محاولة تغيير البيانات، أو القرصنة، أوحجبها أولا عن آخر، أو حذفها دون أن يكون قد تم عمل حفظ مسبق Back up لها وبالتالى لا يمكن إستعادتها.

التشفير Encryption

فى حالة وجود تراسل يتم بين «أميرة» و «ماجد» فإن تشفير التراسل يعنى أنه مرئي للإثنين بشكل مفهوم وواضح، ولكن لأى شخص سواهما- فى حالة الإختراق، أو في حالة أن يكون التراسلات بطبيعة الحال مرئية للجهة المتحكمة فى تنظيم الاتصالات- فإن المحتوى يظهر فى صورة محارف غير مفهومة، بمعنى آخر: شفرة.

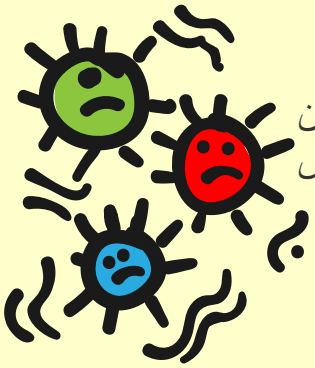
المجهولية Anonymity

فى نفس المثال أعلاه، فإن التعمية تعنى أن التراسل فى حد ذاته لا يمكن رؤيته، حتى من حيث الإستخدام إلا للأشخاص المعنية وبشروط. مثال: يعلم كل معطي لخدمة الإنترنت، المواقع وبيانات المرور للمستخدمين «الTraffic» وماهى الأجهزة؛ فى هذه الحالة فإن مقدم الخدمة لن يعلم أصلاً أنك دخلت على الموقع «س» فى الوقت «ص».

محارف

المحارف (أو Characters) هو لفظ يشمل: الحروف الأبجدية، الأرقام، علامات الترقيم، الحروف الغير لاتينية (مثل العربية والعبرية واليونانية وغيرها)، والمسافات. من أجل أن تكون كلمة السر قوية لابد لها أن تشتمل على ما يتعدى ال١٤ محرف.

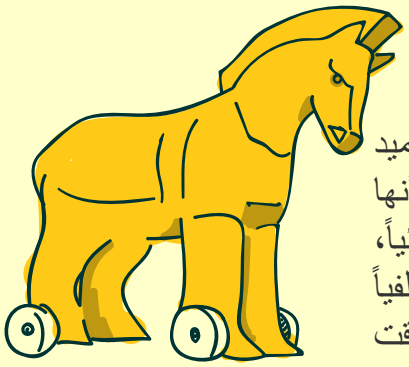
فيروس



هى برمجية أو كود يلصق نفسه بالبرنامج أو الملف دون أن تدرى، ويستطيع بذلك أن ينسخ نفسه فى كل جهاز يتنقل له، مستخدما أى وسيلة نقل (البريد الالكترونى، الأقراص الصلبة، وفلاشات الميمورى).

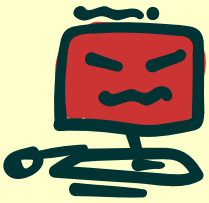
ولكنها لا تستطيع أن تبدأ العدوى من دون أن يقوم المستخدم بفتح الملف المريض.

حصان طروادة Trojan



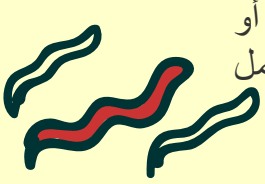
كما فى القصة اليونانية أحصنة طروادة هى برامج تظهر لك فى شكل حميد ولكن ما إن فتحتها وجدت أنها تدمر حاسوبك، أشهرها: تلك التى توهمك بأنها تمحى الفيروسات، والتروجان ليس مثل الفيروسات فهو لا ينسخ نفسه تلقائياً، ولكنه ليس أقل تدميراً. ومن المعروف عن التروجان إنها تخلق لنفسها باباً خلفياً فى حاسوبك لتمكن المبرمج الخبيث من السيطرة على حاسوبك، أغلب الوقت ليسيطر على معلومات شخصية.

البرمجيات الخبيثة Malware



هى برامج صممت خصيصاً لإتلاف الحواسيب مثل (الفيروسات، وأحصنة طروادة)

دودة worm



تعتبر فئة ثانية ملحقة بالفيروسات، ولكن على خلاف الفيروس، لا تحتاج الديدان إلى تفاعل بشرى لتنتشر، فهى تفرض سيطرتها وتتوالد بداخل حاسوبك، أو الحواسيب الأخرى أو قائمة بريدك كاملة بمجرد الوجود فى وسيط متنقل حامل للعدوى.

| كيف يتم التراسل بين جهتين أو أكثر؟

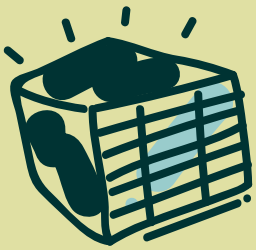
أولى خطوات الاستخدام المسؤول للبيانات، هو أن نعلم كيف يتم تناقل تلك البيانات فى الفضاء الرقمى. تعرف هذه العملية ضمن مبادىء علم السيبرناطيقية أو Cybernetics.


مقدم خدمة الإنترنت ISP (أ)


أبراج الاتصالات (أ)


راوتر ال WiFi (أ)


مستخدم/ة (أ)


الخواديم Servers


مقدم خدمة الإنترنت ISP (ب)


أبراج الاتصالات (ب)


راوتر ال WiFi (ب)


مستخدم/ة (ب)

لذلك فإن رؤيتك للأمان الرقمي هو أن تضع **دروعاً أمنية**، تحصن بها - قدر الإمكان- كل خطوة من خطوات التراسل تلك، بحيث يصعب/يستحيل الوصول لمعلوماتك، وحتى إذا تم الاختراق/ السرقة ...إلخ فإنه يحدث بأقل خسائر ممكنة.

فى الأساس، يعتمد ذلك عليك:

١- اختياراتك للخدمات التى تستخدمها فى التراسل عبر الشبكة العنكبوتية (أونلاين).

٢- أساليبك فى حماية معلوماتك خارج الشبكة العنكبوتية (أوفلاين).

ما المخاطر المحتملة نتيجة للإهمال الرقمي؟

- **«أمانك هو أماني هو أماننا جميعاً»** إذا لم تهتم بأمانك الرقمي، فإنك بذلك تراهن بأمان أشخاص ذو أهمية بالنسبة لك، سواء مهنية، عائلية، حميمية.

- يعرضك الإهمال الرقمي لأشكال شتى مما يسمى بالعنف السيبراني (أو العنف الرقمي)، والذى بالإضافة للأضرار المادية قد ألحق بأضرار معنوية بضحاياه وصلت للإنتحار. تتعدد أشكال مايسمى بالعنف الرقمي، وتتراوح بين قيام شخص أو مجموعة من الاشخاص بالسباب والشتائم، وترويج الاشاعات على مواقع التواصل الاجتماعي، وهو ما يعرف بالتنمر الالكتروني Cyber Bullying، مروراً بالإبتزاز عن طريق معلومات أو بيانات كانت قد تم تبادلها بين الضحية والجاني فى وقت سابق، وصولاً إلى التنصُّت وقرصَنَة الحسابات والأجهزة؛ ومن شأن ذلك فى بعض الحالات «الغير محببة للسلطة» أن يؤدي بفرد أو مجموعة أفراد، بطريقة مباشرة أو غير مباشرة، للملاحقة أو/و الاعتقال أو/و الابتزاز.

- تشكل الأنماط السابق ذكرها وسائل دارجة ومتعارف عليها، ولكن هناك أشكال من العنف أخرى تكون مستترة فى شكل آخر، مثلا: أن يقوم الأهل (أو الشريك) بوضع آلية مراقبة جغرافية على أجهزة أولادهم لتعقب والتحكم فى حركتهم، أن يقوم الشريك بالمطالبة بمعرفة كلمة السر الخاصة بأي حساب خاص بشريكه. الرضوخ عنوة أو عن رضاء لمثل تلك الطلبات لا يمثل ثقة فى الشخص بل على العكس تماماً.

| كيف إذن نحمي أنفسنا؟

الاجابة: ورقة التقييم Assessment Sheet

تلك الورقة هى **أقصر طريقة** لتقييم الاستخدامات وآليات الحماية، وأكثرها تنظيماً - والتنظيم شيء ضرورى فى الحوسبة بشكل عام. **ويمكن تطبيق تلك الورقة على المستوى الشخصى أو المؤسسى.**

طريقة (أ): الأجهزة Device Based

وهى أننا نجمل **الأجهزة، إستخداماتها، والمعلومات التى تنتقل علي كل جهاز، ومن ثم أساليب الحماية.** فيما يلى أغلب الاجهزة المعتاد إستخدامها، لك أن تزيد أو تنقص حسب حالتك.

١- الحواسيب الشخصية (المحمولة, حواسيب سطح المكتب)

يقصد بها الحواسيب التى لا يستخدمها أحد سواك. وسنقسم الاستخدام لأوفلاين وأونلاين:

الاستخدامات

١- ملفات العمل
٢- ملفات شخصية
٣- ملفات حساسة (لايمكن أن تقع فى يد أحد)
٤- الحاسوب نفسه
٥- الأقراص الصلبة المتصلة ومحتوياتها

أوفلاين

١- وضع **كلمة سر طويلة** للحاسوب، تحمل تنوعا من جميع «المحارف» (يمكن أن تكون بأي لغة)

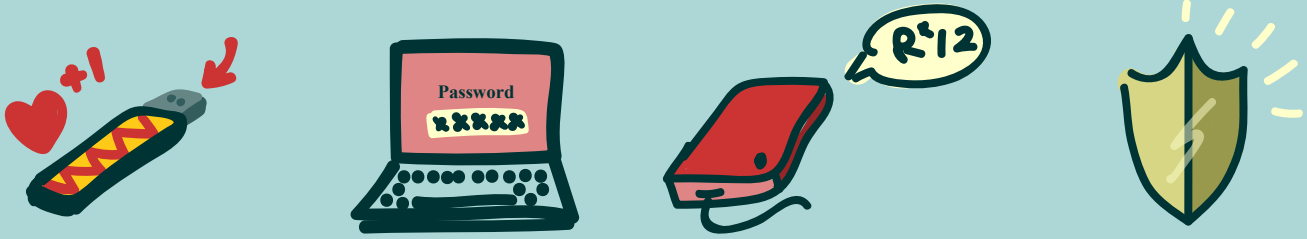
٢- تنصيب (Install) **مضاد فيروسات** مضمون. AVAST أو AVG من البرامج التي تحتوي على قدر لابأس به من الجودة. **نسخ الحاسوب دورياً، ونسخ أى فلاش ميموري أو ماشبه فور دخوله وقبل فتحه.**

لا تحمل شيئا مقرصن (بكراك) بهذا الشأن- لأنك لا تعلم الثغرة التى تم وضعها حتى تتم القرصنة وكيف ستؤثر على أداء البرمجية، أو علي المحتويات الموجودة بالحاسوب.

٣- بالنسبة للملفات الحساسة والأقراص والأجهزة الخارجية أو الداخلية ذات المحتوي الحساس: يتم **تشفير الجهاز**: بإستخدام برنامج **VeraCrypt (سواء فى نظام Mac أو Windows).**

يمكن خ لق قرص صلب مشفر إفتراضى، فى شكل ملف ذو شكل عادى (ملف .doc أو .avi مثلاً)، ثم وضع كل المحتويات الشخصية به. مع مراعاة أن يتم تنصيب السعة لتناسب المحتوى المراد تخزينه.

٤- فيما يتعلق بكل الملفات المهمة، مثل ملفات العمل وماشبه: يتم **أخذ نسخ إحتياطية بشكل دوري،** لضمان عدم فقدها فى حالة حدوث أى تلف لأى جهاز.



Veracrypt |

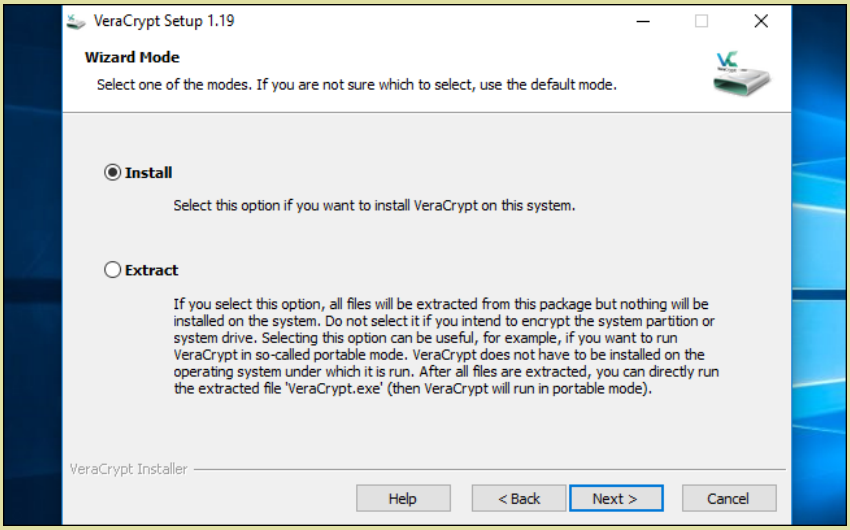
كيفية خلق قرص مشفر على جهازك

التحميل

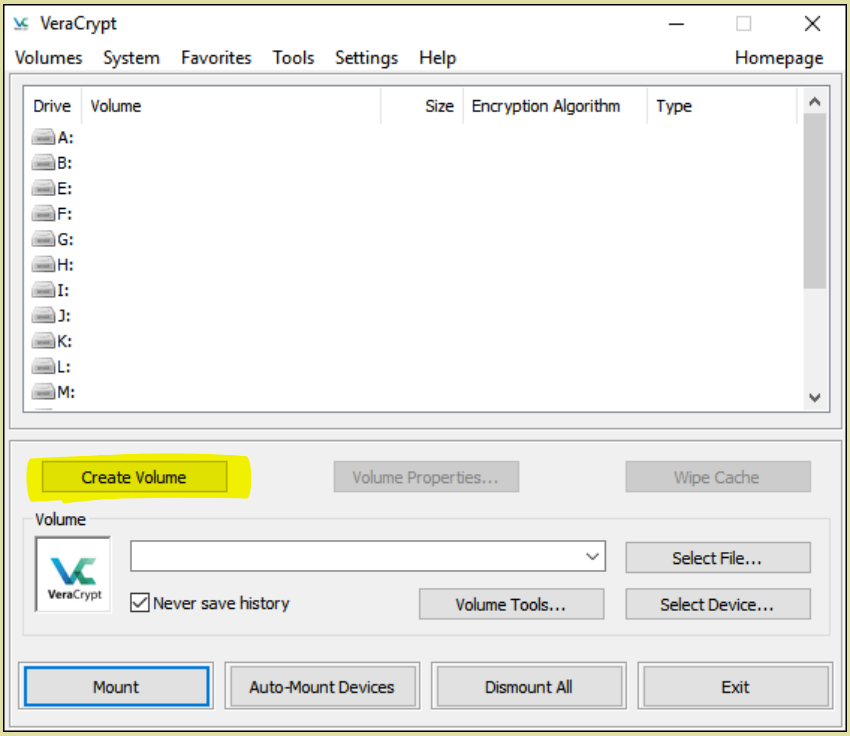
قم بتحميل البرنامج من رابط https://www.veracrypt.fr/en/Downloads.html (بحسب نظام التشغيل الذي تعمل عليه)

خلق الأقراص المشفرة

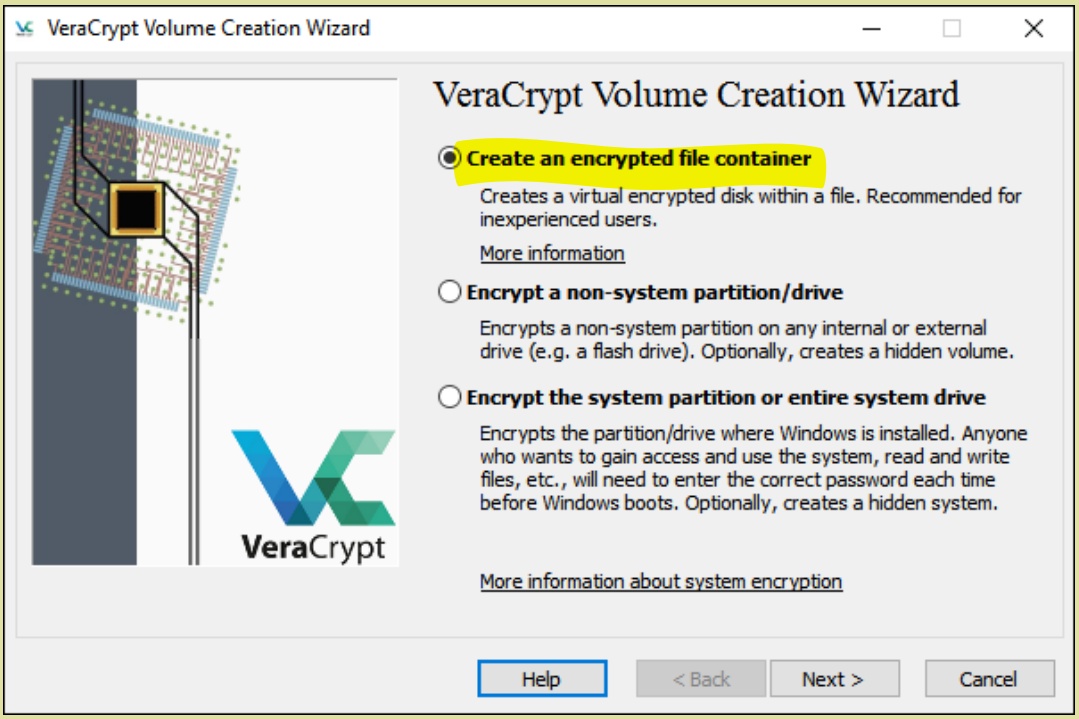
- بعد أن قمنا بتحميل البرنامج، وتنصيبه (Setup) على الجهاز.



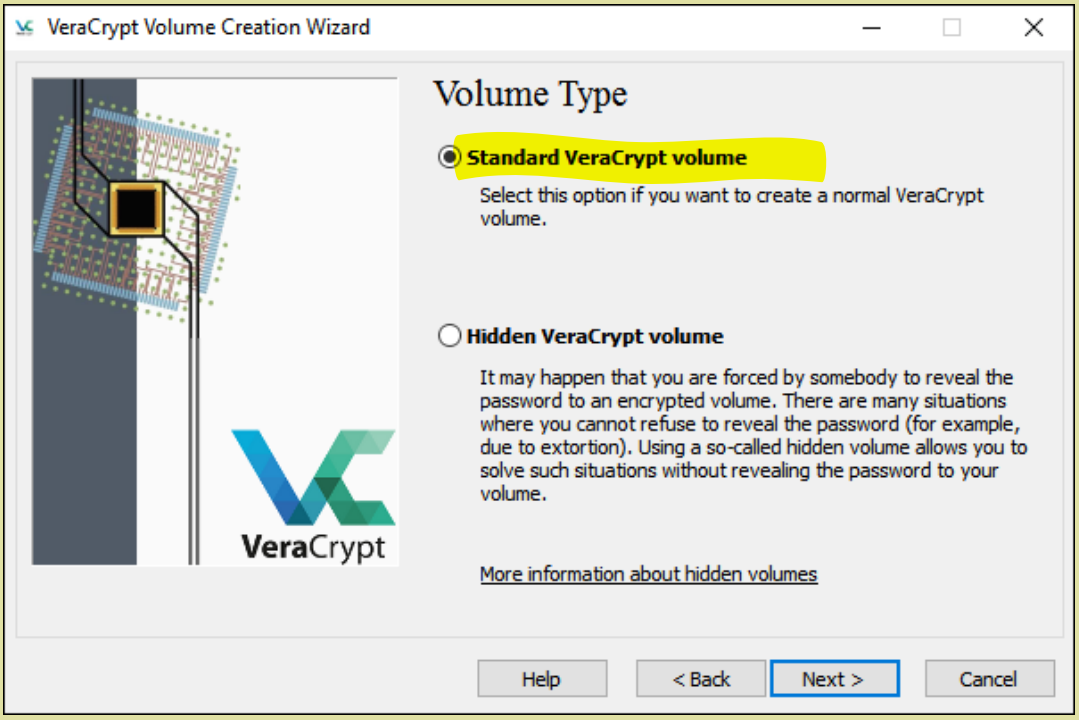
- نقوم بتشغيل البرنامج والضغط على الزر المشار إليه:



- من الممكن أن يكون التشفير لقرص محتوي كبي، يصل إلى تشفير القرص الصلب الخاص بالحاسوب، ولكن لهاذا التدريب فسنبقى الأمور بسيطة بخلق «مستند محلى» Local File يحتوي على المواد المراد تشفيرها...

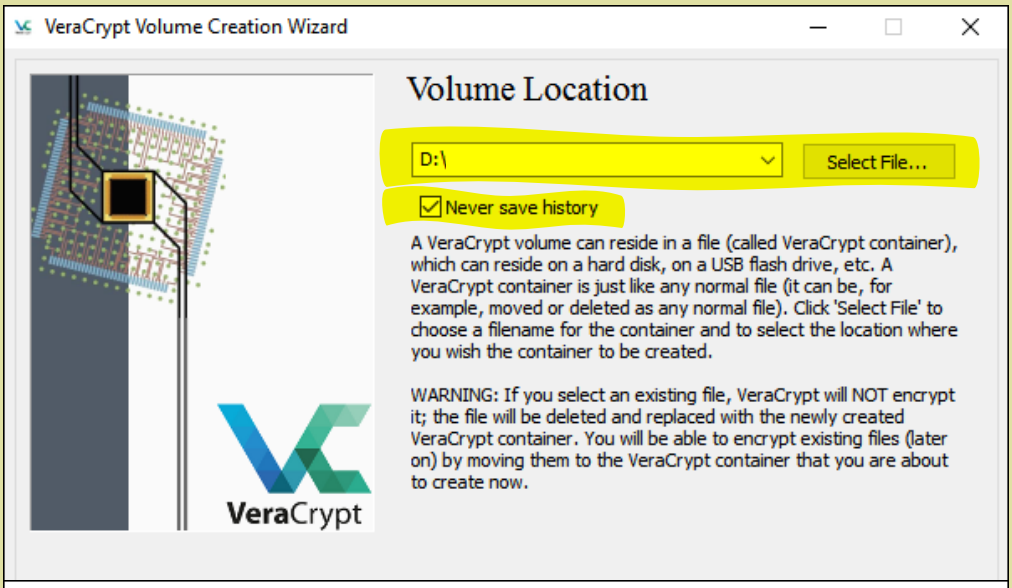


- سيطلب منا إختيار «حاوي نموذجى»، أم «حاوي مختفى»؛ ثانياً سنبقى الأمور بسيطة ونختار «حاوي نموذجي»

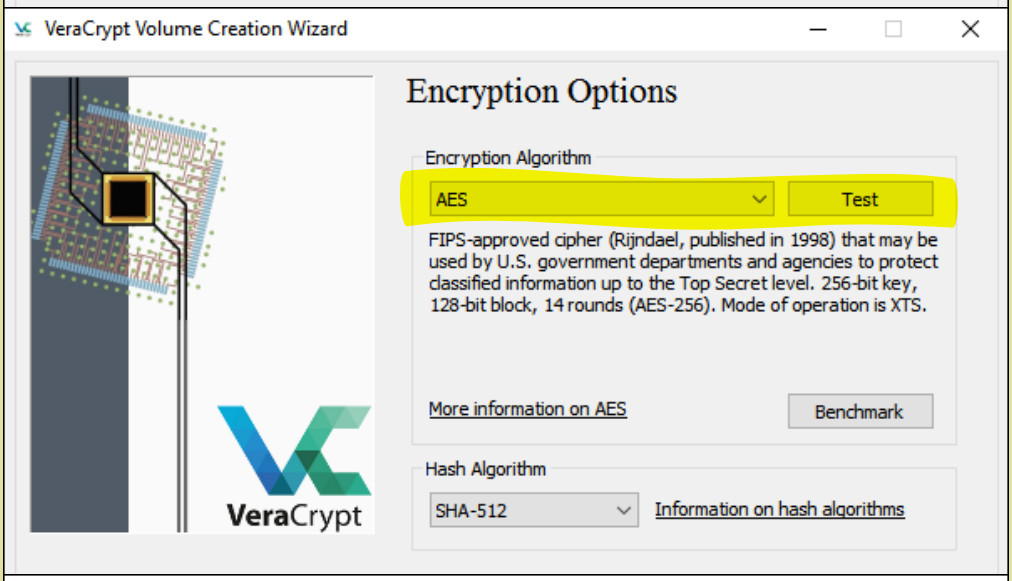


- فى هذه الخطوة سنخلق ملف من أي نوع، على أي من الأقراص صلبة Hard Drive أو المحمولة Flash/Portable Drive المتصلة بالجهاز:

(مثال: ملف Word تحت إسم: hossam) ونختار هذا الملف...

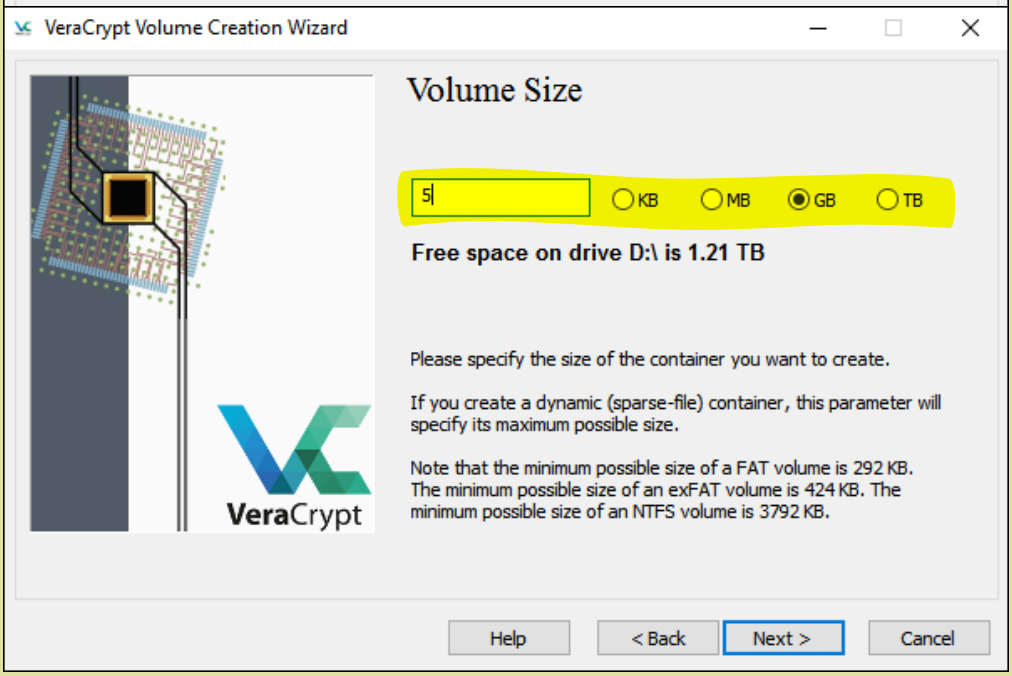


- نختار آلية التشفير

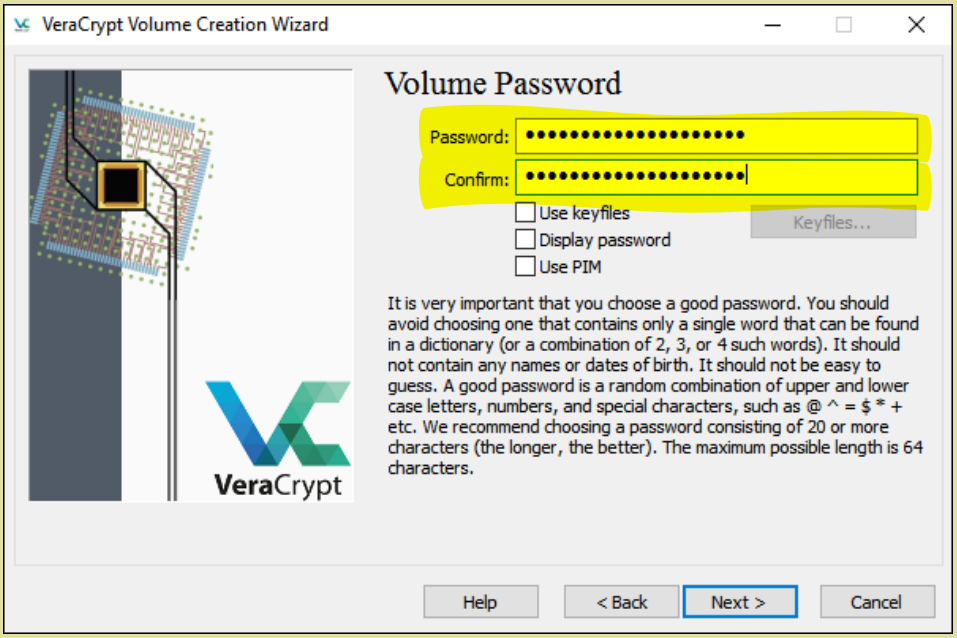


- وحجم الحاوي المرغوب فيه (حسب تقديرك لما ستحويه).

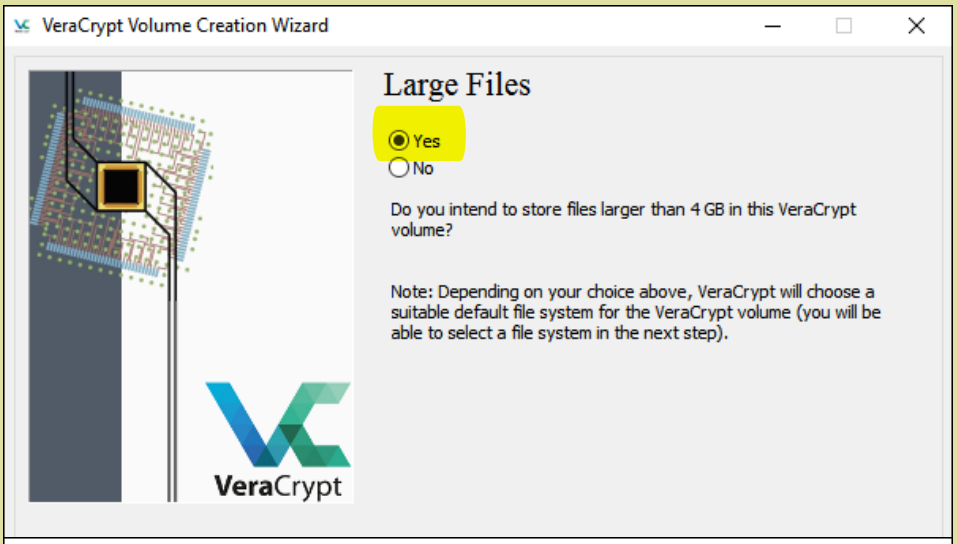
يراعى أن يكون ال Hard الموجود عليه هذا الملف المشفر، يمتلك سعة كافية لتقبل هذا الحجم.

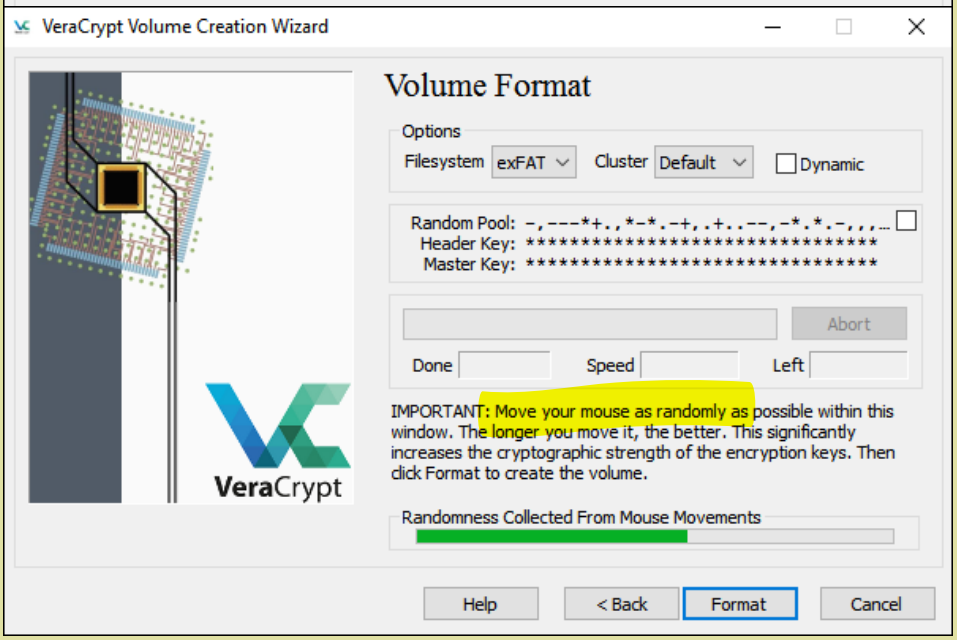


- هنا تأتي مرحلة كلمة السر: **تذكر ماقلناه عن كلمات السر وطولها؟ هنا أيضاً لابد من خلق كلمة سر طوييييلة ويمكن تذكرها (مثال: taMalli M٣ak/AmrD!ab٢٠٠٠)**



ملحوظة: سأقوم بشرح برمجية أخرى، هى Keepassx لحفظ كلمات السر، وخلق كلمات سر جديدة، بعدد محارف مختلفة.





قم بتحريك الفأرة بشكل عشوائي داخل المربع حتى تمام عملية التشفير.

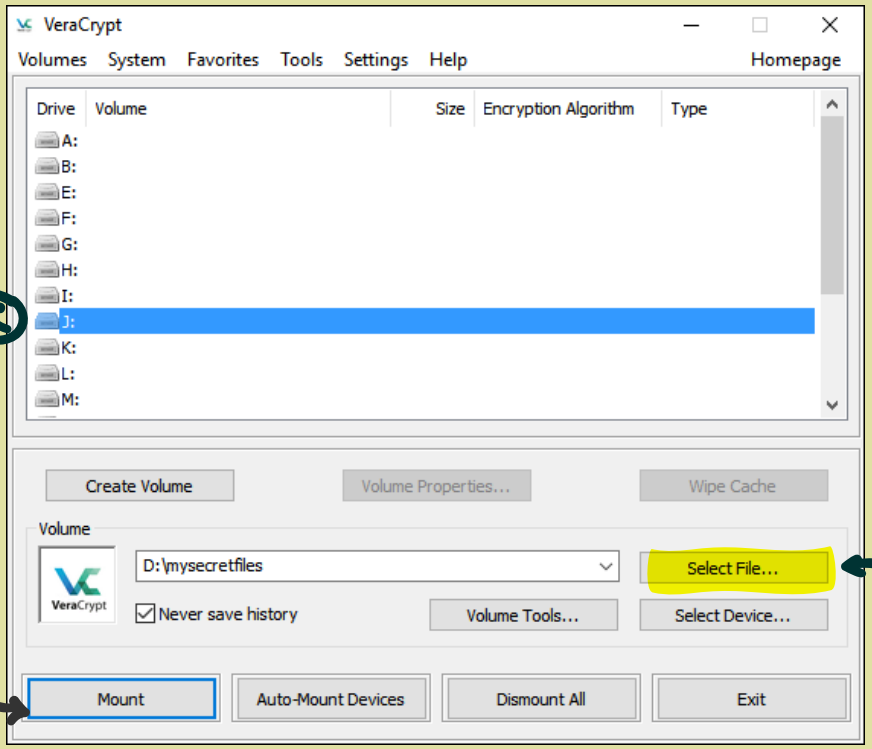
تمت مهمة خلق الملف الحاوي بنجاح! هيا لنفتحه، ونضيف محتوى له...

فتح ملف حاوي مشفر

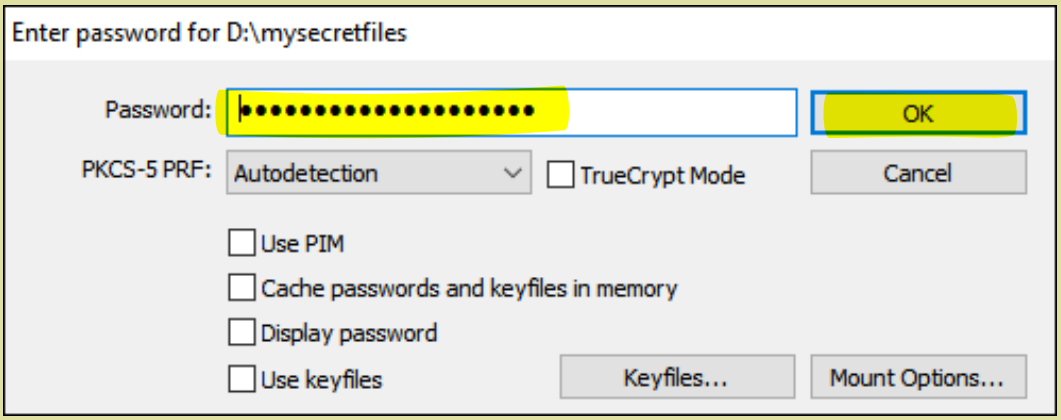
١- سنذهب لمكان حفظ الملف المشفر الذي خلقناه من قبل **hossam.docx** ويراعي ألا يكون إسم الملف ملفت للنظر «بطبيعة الحال طبعاً»! :)

٢- ثم نختار أى من أحرف الأقراص الصلبة المتاحة أمامنا

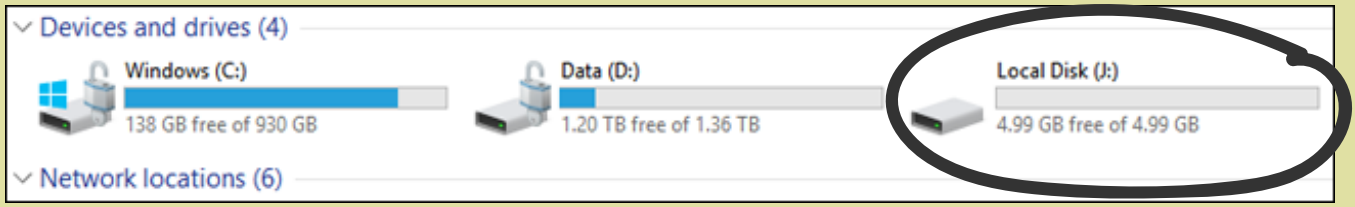
٣- نضغط على زر **Mount**



ندخل كلمة السر الطوييييلة التى خلقناها من قبل (**taMalli M٣ak/AmrD!ab٢٠٠٠**)



وهاهو ملفنا الحاوي المشفر علي شكل قرص صلب فى My Computer!!



عند إنتهائنا من العمل على الملف المشفر تماماً:

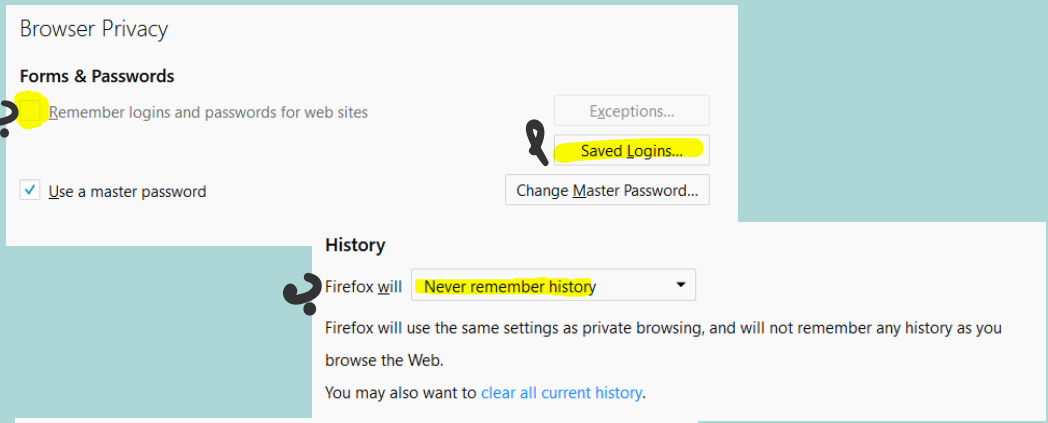
نغلق كل الملفات، ثم نذهب للبرنامج ونضغط Dismount.

١- الحواسيب الشخصية (المحمولة, حواسيب سطح المكتب)

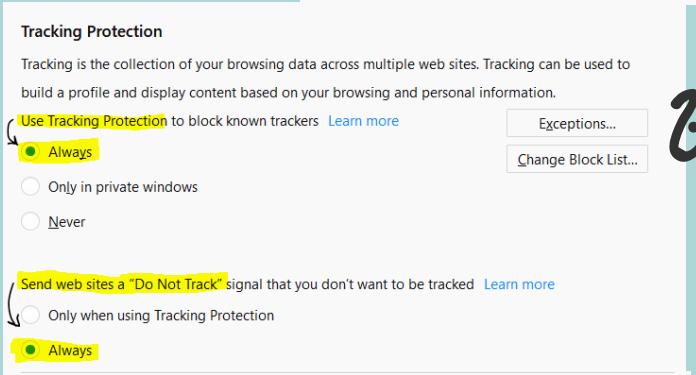
١- إستخدام متصفح آمن فى كل وقت، مثال: Firefox، نظراً لإمكانية **تعديل الإعدادات Options بقائمة الأمان والخصوصية:**

أ - يتم معرفة ماهية **كلمات السر المحفوظة** بالفعل من المتصفح.

ب - **يتم إلغاء/ نسيان** كل كلمات السر والصفحات المفتوحة ومحتويات الإستمارات ...إلخ **عند الغلق.**

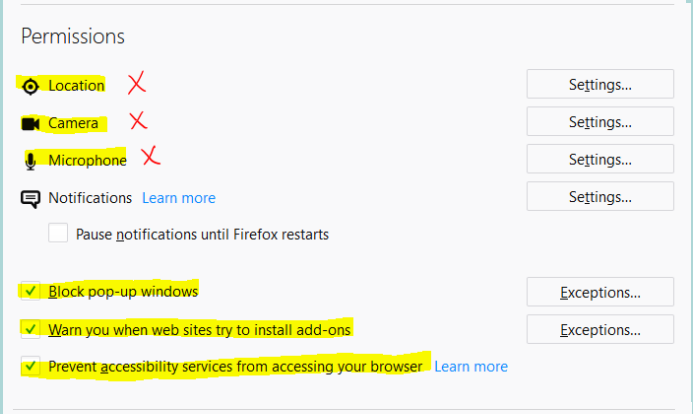


ج- إلغاء خاصية التعقب، وإرسال رسالة «عدم تعقب» للمواقع «دائماً»



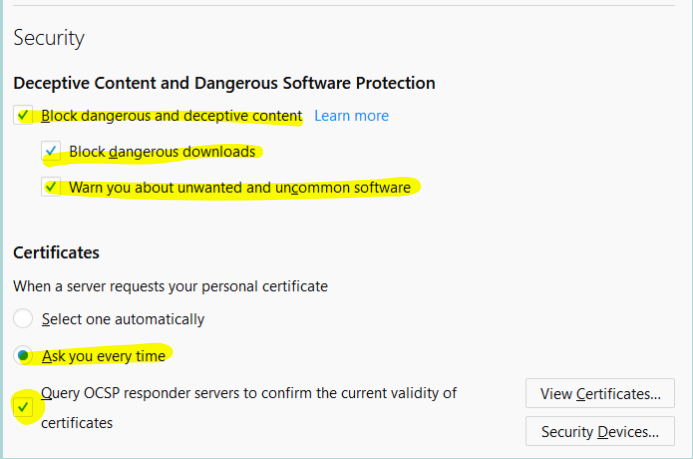
د- فى التصريحات: **إلغاء الولوج للمواقع الجغرافية، الكاميرا، المايكروفون.**

وحجب النوافذ المفاجئة، التحذير عندما تحاول المواقع تنصيب إضافة على المتصفح، منع خدمات المساعدة من الولوج بدون إذن.

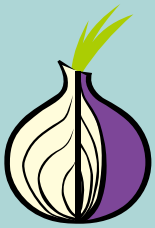


هـ- **فى الأمان:** منع المحتوى الخادع والخطير.

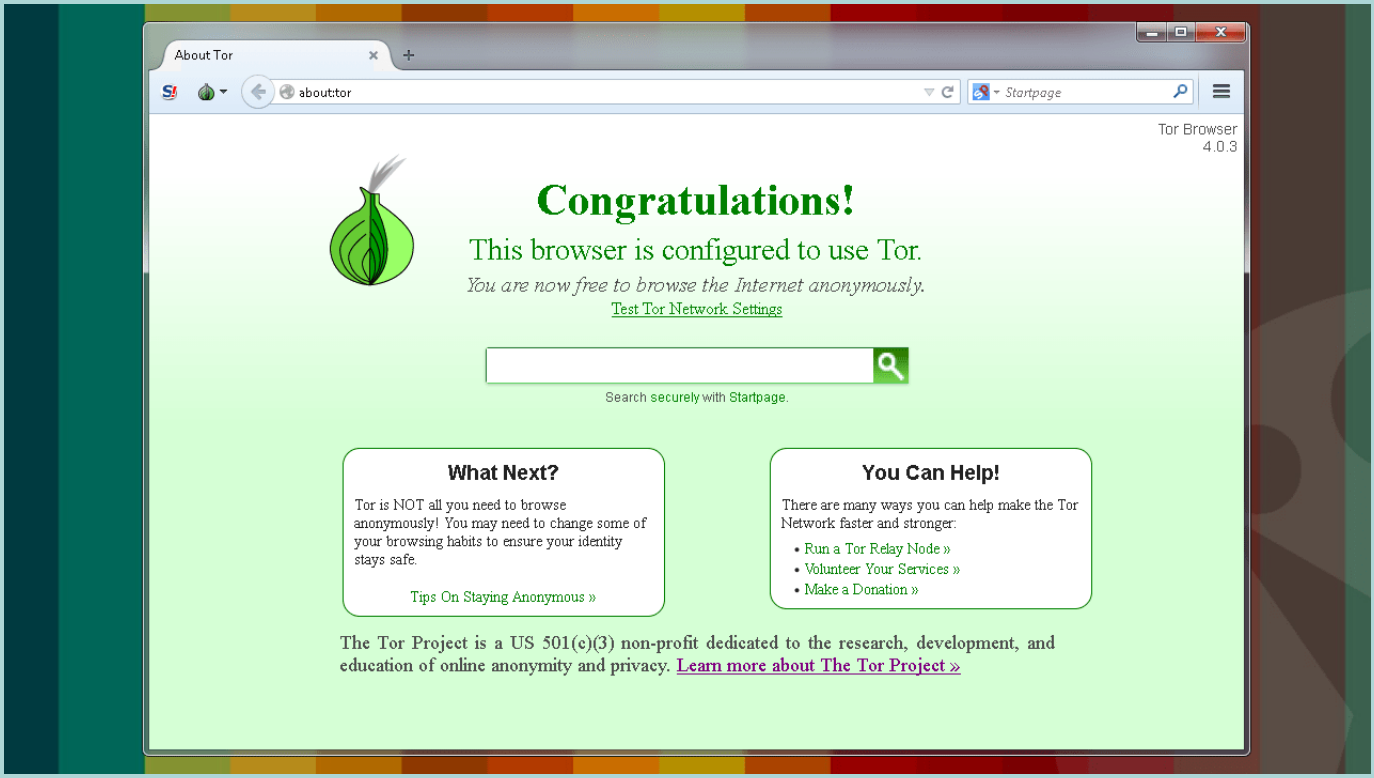
فى **الشهادات التوثيقية:** السؤال كل مرة عندما يريد خادوم التأكد من شهادة متصفحك.



١- الحواسيب الشخصية (المحمولة, حواسيب سطح المكتب)



٢- فى حالة **الرغبة فى المجهولية والتعمية:** إستخدام **متصفح «تور»** والذي يقوم بتحويل إتصالاتك عبر **خواديم صديقة** فى أماكن مختلفة بالعالم، وبالتالى فإن **«عنوان بروتوكول الولوج للإنترنت» (IP Address)** يظهر فى مكان عشوائي فى كل مرة ولوج. وحتى فى حالة محاولة تعقب IP ما وأساسه، فإن أبعد نقطه يمكن الوصول لها هى الخادوم الذى قبله وهو أيضا خادوم وهمي.



ملحوظة: حتى نشر هذا الكتيب, مازال الموقع الأساسى لمشروع تور محجوباً فى مصر, لذلك يرجى إستخدام تلك **الوصلة لتحميل الموقع.**

«عنوان بروتوكول الولوج للإنترنت» هى آليتك لدخول عالم الشبكة العنكبوتية، وبالتالى فإن عنوانك من حيث الأرقام، يحتوي - فى حالته العادية - على مكانك الجغرافى، وجهازك.

لزيادة التأمين فى التصفح: **تستخدم آلية «الشبكات الافتراضية» Virtual Private Network- VPN**، وهى آلية تشبه نفق الأرنب تحت الأرض، إلا أن بعض الحكومات قد تقوم بحجب بعض تلك الأنفاق.

(حتى نشر هذا الكتيب، فمن ضمن «الشبكات» المتاحة هو PsiPhone وهو مدفوع الأجر.)

كيف يعمل تور بتجهيلك؟ عندما نقوم بتشغيل تور، فإنه يستخدم آلية البروكسي الخاصة به فى إدخال الحاسوب فى سحابة من سلسلة خواديم مشفرة متطوعة، ويتنقل بروتوكولك ويختلف من بلد إلي أخرى بعشوائية بين تلك الخواديم، ليصل فى النهاية للموقع المطلوب كأنه من بلد مختلفة عن البلد الموجود أنت بها. وبالتالي حتى - مع الافتراض البعيد- فى حالة تعقب البروتوكول الذي وصلت به حالياً (مثال: ألمانيا) لن يستطيع المتجسس فى كل الأحوال الوصول إلا للخادوم الذي سبق ذلك فى السلسلة العشوائية (فلنقل: النرويج). بينما واقع الأمر أنك تجلس فى مصر مثلاً.

وفيما يلي رابطاً لشرح تفصيلي:

٢- حواسيب العمل

ملحوظة عامة: فى معظم الأحيان تكون شبكة البريد الالكتروني وحواسيب الشركات، والمؤسسات (بما فيها الجامعات ومنظمات المجتمع المدنى) مدارة ومراقبة من قبل وحدة الIT أو ال Media.

وذلك سلاح ذو حدين؛ من ناحية: فهم بذلك يحفظون الإتصالات والمعلومات من القرصنة بسبب خبراتهم، كما يقومون بإلغاء الحسابات فى الأجهزة المتعلقة بالأفراد فى حال القبض عليهم، أو فقدهم للجهاز.

ولكن من ناحية أخرى: فهم يملكون الصلاحية لتغيير محتويات وكلمة السر، إيقاف، رؤية المحتويات وكل الأجهزة المتعلقة بهذا الحساب! لذلك...

فى كل الأحوال، لا تقوم بحفظ أي معلومات شخصية، أو قد تعرضك للخطر على تلك الأجهزة، أو حسابات البريد الالكترونى!

(يعنى ذلك أن بريدك الإلكترونى الخاص بالعمل لا يتم ربطه بحسابك البنكي، أو حسابات التواصل الاجتماعي)

١- التأكد دائماً، من وضع **كلمة سر للجهاز.**

٢- وضعه على الSleep أو ال Log off إذا تركته ولو حتى لبرهة.

٣- **عدم السماح** لأى شخص بالإطلاع على محتوياته بدون وجودك.

٤- وضع كل **معلومات العمل،** وكلمات السر...إلخ على قرص صلب محمول Portable Drive.

تبعاً للإجراءات عمل **نسخ Back up بشكل دورى** على أقراص أخرى، خارج منطقة العمل.

٥- لوضع طبقة أقوي من الحماية، ربما تريد تشفير القرص الصلب المحمول خاصتك قبل القيام بحفظ شيء عليه **(راجع VeraCrypt)** وتذكر حفظ كلمة السر.

٦- القيام بتحديث مضاد الفيروسات، **ونسخ أى جهاز يدخل على حاسوبك قبل العمل به.**

٧- إخراج أى أجهزة محمولة مدخلة فى الحواسيب بشكل آمن، لا تقوم بإخراج الأجهزة بشكل مفاجيء دون عمل Safely remove USB drive

٨- **التأكد من غلق كل الحسابات على الجهاز قبل غلقه وترك مكان العمل.**

يمكن لك أن تحفظ أغلب **البرمجيات التي تحتاجها فى شكل «محمول»** على فلاش ميموري، والعمل بإستخدامها ثم إخراجها من الحاسوب فور الإنتهاء.

فلا يكون هناك أثر لهذه البرمجيات على الجهاز، أو تستطيع إستخدام أى جهاز مهما كانت تجهيزاته والعمل فوراً (لأن معك برمجياتك اللازمة بالفعل): الموقع هو...

PortableApps.com

٢- حواسيب العمل

كما نوهنا مسبقاً فإن التعامل مع الحسابات البريدية والحواسيب يكون فى منتهى الحرص...

١- تلف الأجهزة، أو الأقراص الصلبة

٢- عطل بالجهاز قد يستدعي ذهابه لمكان خارج العمل لإصلاحه، أنت لا تعلم ماذا يمكن أن يحدث للجهاز وهو بحوزة شخص آخر (من باب عدم الثقة أو الجهل)

٣- إقتحام المكان وسرقة الأجهزة أو التحفظ عليها

٤- تركك للمكان بشكل مباغت

٥- عدم الوثوق فى الهيئة القائمة على إدارة ومراقبة التراسلات (مثل: الجامعات والمستشفيات ...إلخ)

- **نفس إحتياطات الأمان المتعلقة بالمتصفحات السابق ذكرها.**

- إذا كنت ف أحد منظمات المجتمع المدني (عموماً والتى تعمل على مجتمع الميم خاصة)، أو تقوم بالتصفح والبحث عن أمر لاتريده أن يظهر على لدي شركة الاتصالات المانحة للخدمة ISP، أو لتخطي الحجب **ينصح بإستخدام متصفح تور** فى التواصل.

- ينصح **بعدم إستخدام** أى من خواديم الحفظ السحابية مثل Google Drive - Dropbox للإحتفاظ بأى مواد بها مخاطرة، أو شخصية، وإستخدام **send.firefox.com** أو **Cryptpad** بدلاً منهم.

يمكن الحيلولة دون ذلك برفع **ملفات مشفرة** بكلمة سر **(تشارك عن طريق تطبيق واير Wire)***.

- **عدم كتابة أى كلمات سر على ورق**، وإذا تمت الكتابة، لا يكون تحت تلك الورقة ورق آخر، ويتم التخلص من الورقة عن طريق الحرق (لا التقطيع، ولا الإلقاء فى سلة المهملات).

- إستخدام **KeepassX أو بدائله** للحفاظ على/ وخلق أى كلمات سر للحسابات الالكترونية

(وتنطبق تلك الآلية على أى حساب وأى بريد إلكترونى خاص بك)

- إستخدام منصة **meet.jit.si، أو appear.in أو meet.greenhost.net أو Wire** للتواصل المسموع المرئي (Video conference) لأن الاتصال يكون أأمن، ف Skype ليس آمناً ويستهل الكثير من حزمة الشبكة (السبب الذي يجعل التراسل بطيئاً).

- إستخدام معطي خدمة إيميل تضع عليه حسابات الإيميل خاصتك مثل: **Thunderbird (ومعه إضافة Enigmail) أو Mailvelope** (وتوجد منه نسخ لجميع أنظمة التشغيل، و نسخة محمولة على Portable Apps).

- إستخدام خدمة ال**PGP** (إختصار: Pretty Good Privacy) مع أي حساب إلكتروني شخصى أو خاص بالعمل، وهو آلية تشبه آلية المافيا فى التعارف على حقيقة هوية الشخص الذى يحمل الرسالة.

تمكنك أدوات آلية الPGP من خلق مفتاحين (خاص، وعام)، تُبقى الخاص لديك، ويحمَّل العام على الخادوم الذى يمثل دليل التليفون لأي شخص يود مراسلتك برسالة مشفرة، وبذلك - **وفقط فى هذه الحالة**- يحدث ما يسمى بال End-to-End Encryption، أي التشفير بين كل أطراف المحادثة. يشمل ذلك أيضاً مقدمي خدمة الإيميل مثل: Protonmail - Riseup، أو خدمات التراسل مثل: Wire.

عند إستخدامك الآلية (مثال: تطبيق Mailvelope أو Thunderbird Enigmail) تقوم بإختيار تشفير الرسالة المرسلة، وهنا يطلب منك: إدخال الرقم السرى لخزانة المفتاح خاصتك - والمفتاح العام الخاص بالمرسل إليه (ويكون مكانه إما الخواديم المتاحة على التطبيق، أو أن يكون قد أرسله إليك مسبقاً). عند إستقبال رسالة من شخص تتوقع رسالته، سوف تحتاج إلى نسخة مفتاحه العام (المتاحة أيضاً على الخادوم) لحل الشفرة.

* تم حذف تطبيق **سيجنال** نظراً لكثرة محاولات حجبه، لدرجة تجعله غير مستقر حالياً لتبادل الرسائل المشفرة. **لطريقة إنشاء حساب على واير، برجاء الرجوع لقائمة المراجع.**

برنامج KEEPASSX لخلق وحفظ كلمات السر

نصائح

- برنامج Keepass (وله نسخة على أندرويد)
- برنامج Onepass (لهواتف وأنظمة أبل)
- برنامج KeepassXC (لأنظمة ويندوز ولينوكس)

- يتم تحميل كل البرمجيات **من مواقعها الأصلية**، لا من مواقع مضيفة.

[إلا فى حالة متصفح تور حالياً نظراً لكون الموقع الرئيسى محجوباً فى مصر]

- يفضل إستخدام النسخة المحمولة Portable، وتكون على فلاش ميمورى لسهولة التعامل.
- لا تنس الBack up بشكل دورى.

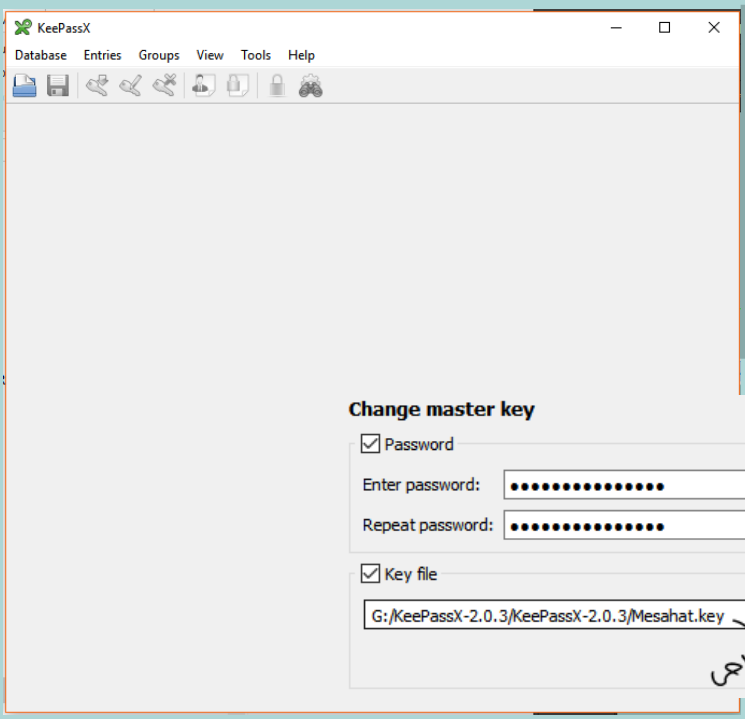
طريقة العمل

نقوم بالتحميل من موقع: https://www.keepassx.org/downloads

-بعد التحميل نفرغ الملف المضغوط، لملف عامل عن طريق Extract، ثم نفتح هذا الملف العامل لنشغل البرنامج.

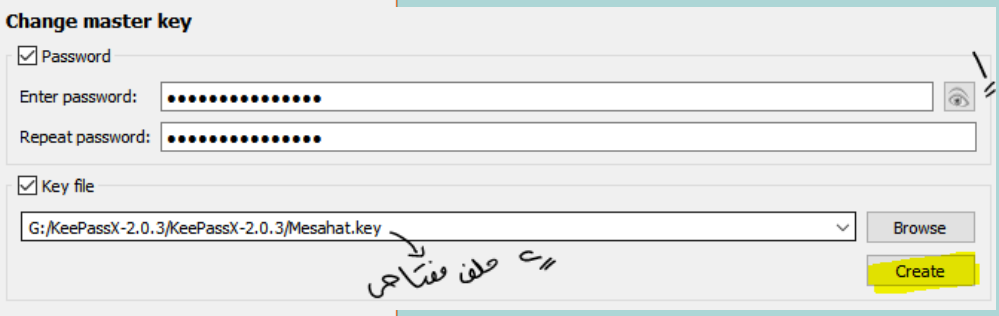
- من قائمة **Database** < **New Database** لخلق قاعدة بيانات لكلمات السر لدينا
- أدخل كلمة سر طويلة **تستطيع تذكرها**

فى حال عدم تذكرها لن تستطيع الولوج لقاعدة كلماتك.



من الممكن خلق ملف مفتاحى من خانة **Keyfile** < **Create** وإختيار مكان الملف وإسمه، كما هو مشار للأسفل؛

لكن يفضل عدم فعل ذلك لأنه بمجرد حصول أي شخص على هذا الملف سيحصل على كلمات السر خاصتك...أشك فى أنك تريد ذلك!

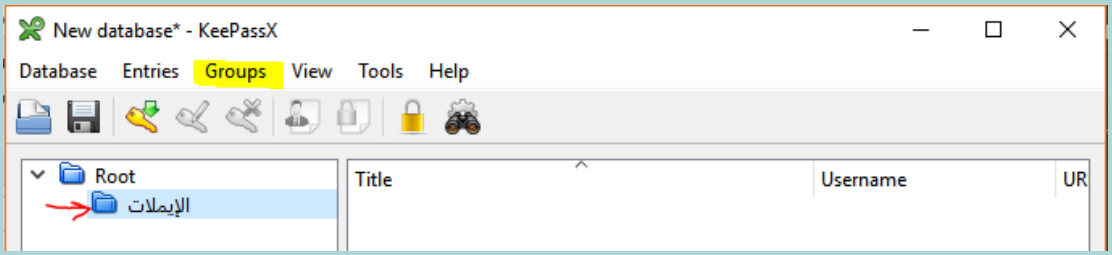


من الممكن خلق ملف مفتاحى من خانة **Keyfile** < **Create** وإختيار مكان الملف وإسمه، كما هو مشار للأسفل؛

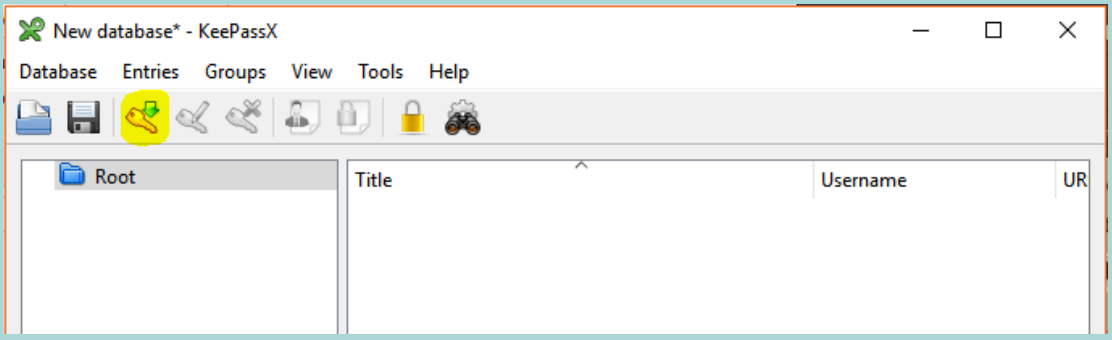
لكن يفضل عدم فعل ذلك لأنه بمجرد حصول أي شخص على هذا الملف سيحصل على كلمات السر خاصتك...أشك فى أنك تريد ذلك!

برنامج KEEPASSX لخلق وحفظ كلمات السر

- لخلق **ملف جديد** (مثال: ملف يحوي على كلمات سر حسابات البريد الالكترونى)
قائمة Groups ثم Add New Group: ونعطيها إسماً (مثال: الإيميلات)



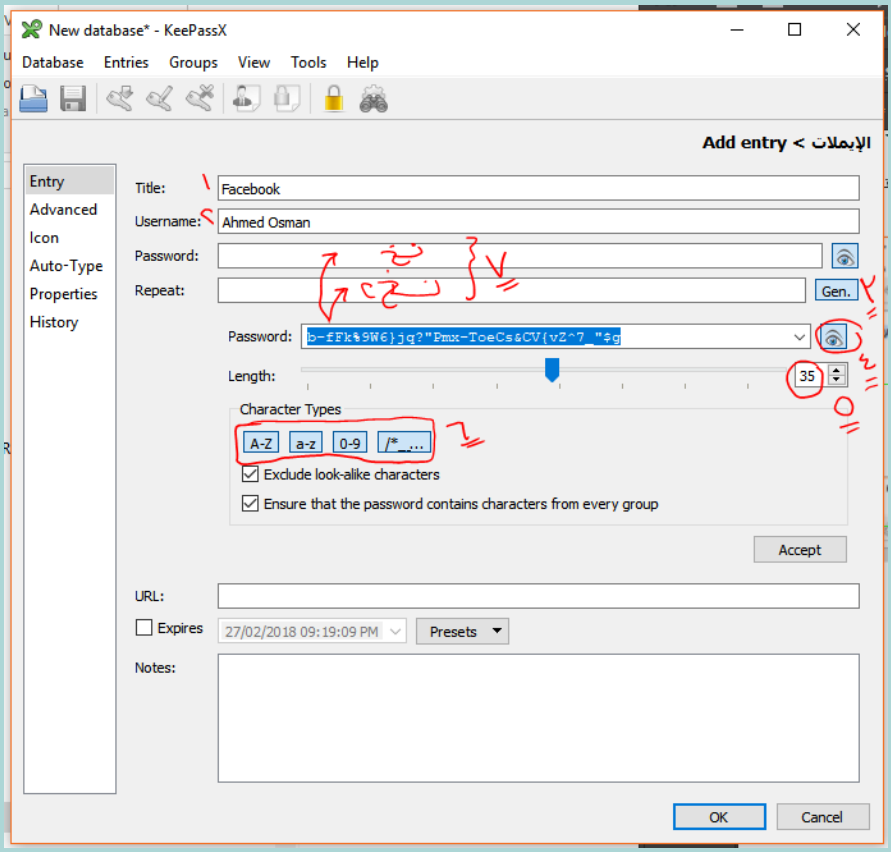
- لخلق **مدخل جديد من كلمات السر**
قائمة Entries ثم Add New Entry (مختصر ١: زر Ctrl/ Cmd + N)
(مختصر ٢: علامة المفتاح ذو السهم الأخضر المبينة أسفله)



- **ضبط المدخل الجديد:**

إتبع الخطوات من ١ - ٧ لإدخال معلومات إرشادية لك عن نوع الحساب وطبيعته، ثم خلق كلمة السر وطولها (هنا جعلتها ٣٥ محرف) ثم حفظها.

بإمكانك خلق ميعاد تجديد لكلمة السر، وذلك من زر Expires



- **بعد خلق وإدخال كلمات السر والحسابات المرادة، لا تنس نقر «حفظ Ctrl/Cmd + S لحفظ الملف الجديد)**

٣- الهواتف النقالة (الموبايل والتابلت)

١- تجنب إقحام رقم هاتفك **الشخصي** مع هاتف **العمل** أو هاتف **المواعدة**، وبالتالى فى التطبيقات المتعلقة.

٢- **فى حالة الوجود فى إجتماعات مغلقة:** أ- إفصل بطارية هاتفك، وضعوا كل هواتفكم خارج تلك الغرفة (المايكروويف ليست فكرة سيئة حيث أنه يفصل ترددات كل الشبكات، لكن تذكروا ألا يشغله أحد!)

ب- يمكن أن تبدل المايكروويف بأي إناء طهي مغطي

فيما يتعلق بالتطبيقات

٣- تأكد من أن تقرأ تعليمات السماح Permissions جيداً لتطبيقات الهاتف، حتى تعلم ماذا يمكن أن يحصل أو لا يحصل عليه مقدك خدمة التطبيق.

٤- بإمكان بعض التطبيقات لديك (أندرويد أو أيفون) أن تصل إلى المايكروفون، حتى وأنت لا تستخدمه هاتفك. ضع وصلة AUX قديمة من دون سلكها فى مخرج السماعة (فأنت بذلك تخدع الجهاز بوهمه بوجود سماعة خارجية بينما لا يوجد)

٥- **لا تحمّل تطبيقات أنت لا تعلم مصدرها** (مثال: مصدر تطبيق سيجنال هو شركة «أوبن ويسبرز» لذلك لا تكن واثقاً من أى مقدم آخر لنفس الخدمة.

٦- **قم بتشفير هاتفك:** من إعدادات > الأمن Security > تشفير الجهاز Encrypt.

[لتجنب نسيان كلمات السر] أدخل كلمة السر فى برنامج Keepassxc

٧- **فيما يتعلق بحفظ المعلومات** قم بعمل حفظ نسخ بديلة لمحتويات الهاتف **Backup**، سواء تسجيلات، صور هامة ...إلخ ولا تجعلها فى هاتفك بالأساس.

٨- أيضا، قم بحفظ المعلومات المهمة على خزانة خارجية بالهاتف **(SD Card) وليس على ذاكرة الهاتف الداخلية** - خاصة الأرقام (لأن ذلك سيجعل الأرقام أأمن، وسيجعل نقلها من هاتف للآخر أسهل)، **ثم قم بتشفير الSD Card عن طريق الإعدادات بالهاتف.**

٩- **فيما يتعلق بالأرقام:** لا تقم بحفظ الأرقام بكتابة دليل يوضح إنتماء الشخص لمنظمة ما (خاصة منظمة ميم)، أو تطبيق مواعدة ما خاص بالميم.

١٠- فى حالة سرقة، أو أخذه عنوة بطريقة من الطرق: أ- **تأكد أنك قد قمت بتحميل خدمة Find my phone** الخاصة بأندرويد، أو آيفون.

يمكن لك أو لشخص تأمنه على معلوماتك أن **يدخل على حسابك وكلمة السر خاصتك وتعقب مكان الجهاز/ محوه بالكامل** حتي إن كان مغلقاً (فسيمحى فور فتحه وتوصيله بالواي فاي).

ب- **كارت الSim خاصتك** من ضمن الوسائل التي يمكن للشخص الحصول بها علي كل المعلومات التي تمت عن طريق تلك النمرة أو نمرة أخرى، لذلك: فى حالة إستخدام هذا الكارت للمواعدة أو للعمل الحقوقي، عليك توخي الكثير من الحذر (لذلك نصحنا بفصل الإستخدامات ووجود أقل كم ممكن من المعلومات عليهم)، وتدميره فى حالة الشعور بالقلق.

١١- **واتساب ليس تطبيقاً آمناً بالرغم أنه مشفر:** ١- هو مملوك لإحدى أكثر الشركات إشكالية سواءأ على مستوى سياسات المستخدم، أو على مستوى الممارسات التى تفصح عن محتوى المستخدم للحكومات، وهي شركة فيسبوك. [سنناقش التطبيقات الآمنة والغير آمنة لاحقاً]

٢- بسبب تلك السياسة وهذا المالك، فإنه حتى مع تشفيره فهو موجود بداخل خواديم فيسبوك الخاصة، وهو غير مفتوح المصدر (فالبرمجيات مفتوحة المصدر تسمح للمبرمجين من شتى بقاع الأرض معرفة الكود، وقراءته وبالتالي عمل تأكيد أمنى مستمر للتأكد من عدم إختراقه).

١٢- لا تستخدم متصفحات/ تطبيقات تفصح عن مكانك، هويتك، ملفات الوسائط المتعددة Media files المتاحة لديك قدر الإمكان.

[وإن كنت ستستخدمها فإعلم أنك تعرض الآخرين أيضا لذلك، وألا تناقش أمورا شائكة عليها.]

١٣- إستخدم المتصفح للولوج للمواقع بدلا من التطبيقات (مثل موقع فيسبوك- تويتر...إلخ)

DuckDuckgo
iOS + Android
Desktop
(for Searching)

Appear.in
iOS + Android
Desktop

Orbot
iOS + Android

ProtonMail
iOS + Android

Firefox Focus

Orfox
iOS - Android

Wire
iOS - Android
Desktop

واتساب - سكايب - سنابشات - فيسبوك/ميسنجر - شازام- إنستاجرام - أوبر/ كريم (لإمكانيتهم ومثيلاتهم من ولوج تاريخ تنقلاتك وموقعك الجغرافي) - فايبر - تويتر- برامج البنوك - أى برمجية مضادة للفيروسات أو توهمك بأنها ستفرغ مساحة فى ذاكرة الهاتف - جوجل فيتنس أو برامج الرياضة - برامج الصحة (مثل الدورة الشهرية وخلافه)

برامج المواعدة بشكل عام سواء للمثليين/ات أو العابرين/ات خصيصاً أو لا (لباقي الأحرف) غير آمنه على مستوى العالم، ولا سيما فى مصر. بعضها يحاول التحديث من إحتياطات الأمن ولذلك ينصح بعدم إستخدامها فى مصر إطلاقاً، وإذا كنت تستخدمها يرجى التأكد من التحديثات متابعتها.

بذلك نكون إنتهينا من التقسيمة #١ من إستمارة التقييمات, والتي تأخذ الأجهزة وجهتها الأساسية, ثم تقوم برصد المعلومات, وآليات الحماية والخصوصية تبعاً لتلك المعلومات.

| التقسيمة ٢ (على أساس الإستخدامات)

١- مواقع التواصل الاجتماعي

١- إستخدام بريد إلكتروني منفصل، بهوية منفصلة.

٢- حسابك الشخصي مهما كانت درجة حمايته هو ليس غرفة نومك، بل مكان على الإنترنت، فكن حذرا لما تقوله وتجهر به عليه.

٣- كلمات سر طويلة (+ ٢٥ محرف - إستخدام Keepass X أو بدائله لإنتاج كلمات سر عشوائية).

٤- كل حساب بكلمة سر مختلفة.

٥- **فى حالة الهواتف الجوالة:** إستخدام **المتصفح** بدلا من التطبيق.

٦- عدم ربطه برقم تليفون محلي، ولاسيما هاتفك الشخصي.

٢- البريد الالكترونى الشخصي

١- كلمات السر الطويلة

٢- عدم فتح بريد إلكتروني لا تعرف مصدره (Spam)

٣- إستخدام ال PGP فى حالة إرسال ملفات أو مراسلات ذو طابع شخصى جدلى

٤- التأكد من الخروج من الحساب Sign out بعد كل مرة إستخدام

٥- يفضل إستخدام المتصفح بدلا من التطبيق

٦- عدم إلصاق هذا الحساب بأي نشاطات حقوقية سواء بمجتمع الميم أو لا

٤- البريد الالكترونى للعمل

١- كلمات السر الطويلة

٢- عدم فتح بريد إلكتروني لا تعرف مصدره (Spam)

٣- إستخدام ال PGP فى حالة إرسال ملفات أو مراسلات ذو طابع شخصى جدلى

٤- التأكد من الخروج من الحساب Sign out بعد كل مرة إستخدام

٥- يفضل إستخدام المتصفح بدلا من التطبيق

٦- يفضل إستخدام موفر خدمة الإيميل مثل Thunderbird (ومعه Enigmail) لدرجة أعلى من الأمن

٧- فى حالة المؤسسات الحقوقية: أ- يفضل إنشاء الايميلات على خادوم مضمون مثل RiseUp أو Protonmail للحسابات الفردية الهامة. ب- يفضل وضع خاصية Find my phone و Google Device Manager للهواتف الشخصية بحسابات المؤسسة، للتمكن من إلغاء أى معلومات على الهواتف المتعلقة بأفراد المؤسسة فى حالة حدوث كارثة

٨- عدم مناقشة أشياء شخصية على إيميل المؤسسات عامة (جامعات أو حقوقية)

٩- فى حالة المؤسسات الدراسية، والبحث: إنشاء حساب خاص على RiseUp أو Protonmail

٥- تطبيقات المواعدة

يفضل عدم إستخدامها بتاتاً. فوفقاً للتقارير الحقوقية* خاصة الصادرة بعد حفلة مشروع ليلي (أو مايعرف بواقعة أعلام قوس قزح) فإن نسبة القبض والإيقاع عن طريق التطبيقات إرتفعت لتمثل أسهل وأسرع طريقة قبض، إلى جانب الحسابات الشخصية للفيسبوك. [راجع تقرير المصيدة للمبادرة المصرية للحقوق الشخصية]

إذا كنت ستظل تستخدمها: أ- إستخدم هاتف منفصل لها فقط! حتى لا تتسبب فى أذى الآخرين فى حالة وقوع الهاتف فى اليد الخاطئة.

ب- عدم إعطاء أى معلومات شخصية أو عناوين أو مواقع من هاتفك.

ج- عدم إلصاقها ببريدك الالكتروني أو حساب الفيسبوك الشخصي.

د- متابعة التحديثات على التطبيقات، وملاحظات الأمانة والخصوصية.

ه- نقل أى تشات داخلى على تطبيق Wire أو Appear.in وليس على التطبيق ذاته (مع تفعيل خاصية الرسائل التي تمحى بعد وقت قليل من استقبالها).

٦- حفظ المستندات والأرشفة

١- إستخدام Veracrypt ومعه Keepassx (وبدائله) لحفظ الكلمات السرية بنظام.

٢- البحث عن خواديم سحابية Cloud Drives آمنة بدلاً من Dropbox- onebox - Google Drive، مثل send.firefox.com

٣- عمل Backup بإنتظام وتعددية.

٧- المحادثات المسموعة والمرئية أون لاين

١- إستخدام meet.greenhost.com أو appear.in أو meet.jit.si

٢- إستخدام Wire (تم حذف **سيجنال** من المنصات الآمنة نظراً لكثرة محاولات إختراقه من قبل الحكومات، حتى أصبح غير مأمون الجانب) وإنشاء حساب عن طريق بريد إلكتروني منفصل، وليس عن طريق رقم الهاتف الخاص بك.

٨- المتصفحات

١- الرجوع لقائمة الاعدادات لمتصفح **(فاير فوكس)** فى أول ذلك الكتيب.

٢- إستخدام متصفح «تور» أو «أورفوكس أو فايرفوكس فوكس» (فى حالة الهواتف النقالة)

٣- إستخدام البروكسى مثل «أوربوت» (فى حالة الهواتف النقالة) وال VPN فى (حالة الحواسيب).

---

* تقرير «المصيدة» الصادر عن «المبادرة المصرية للحقوق الشخصية»: رابط

| نصائح و إرشادات عامة وهامة

١- التكنولوجيا بشكل عام، هى سلاح ذو حدين، وهى دائمة التغيير، فكن دائماً على اطلاع.

٢- إذا كنت أنت مؤمّن، فلا يعنى هذا بالضرورة أنا الشخص/الأشخاص الذي/ن تقوم بمراسلاتهم هم أيضاً على نفس القدر من الأمان. مما يعني...

٣- أمنك، هو أمني، هو أمننا جميعاً

٤- تقع أغلب المشاكل ذات الطابع الرقمي، أو حوادث العنف الالكترونى، بسبب الإستخدام السئ وغير الحذر للتقنية، وليس بالضرورة بسبب قدرة المعتدي على الاختراق.

٥- لا تترك معلوماتك أو حساباتك فى أى مكان أو تحت يد أي شخص آخر، سواء فيزيائياً عن طريق ترك متعلقاتك الرقمية بدون ملاحظة، أو رقمياً عن طريق عدم الاعتناء بالخروج من حساباتك، أو إعطاء كلمة السر لشخص «ثقة» (مثل حبيبك/تك)

٦- للتقنيين: أسهل ما يمكن فعله لضمان إجراءات الأمن والخصوصية لدى شخص هى أن تفعل ذلك له، سواء على جهازه أو هاتفه... رجاءاً لا تفعل ذلك! لابد للشخص أن يعلم أنه ليس من حق أحد معرفة محتويات أجهزته الرقمية سواه، وذلك أول طريق التعلم، هو أن يقوم هو «بمعاونتك» بتنصيب وتشغيل البرمجيات والتطبيقات.

٧- لا يوجد تقنية فى العالم آمنة طوال الوقت (راجع رقم ١، والمقدمة) ولكن المعيار هنا هو: ماإذا تم إختراق، أو إيقاف العمل بآلية ما، هل سيتم إكتشاف/تسريب معلوماتنا بأثر رجعي أم منذ لحظة الإختراق؟ هذا السؤال لابد أن يكون من أولويات إختيار البرمجية أو/ و تطويرها.

| مراجع هامة

١- دليل تدريبي لاستخدام تطبيق التراسل الآمن **Wire**
/https://digital-protection.tech/2018/06/06/wire

٢- **دليل سيناريوهات حول الأمن (للميم)** - Electronic Frontier Foundation (EFF)
https://ssd.eff.org/ar/play-list/%D8%B4%D8%A8%D8%A7%D8%A8-%D9%88%D8%B4%D8%A7%D8%A8%D8%A7%D8%AA-%D9%85%D8%AB%D9%84%D9%8A%D8%A7%D8%AA%D8%8C-%D8%AB%D9%86%D8%A7%D8%A6%D9%8A%D8%A7%D8%AA%D8%8C-%D9%85%D8%AA%D8%AD%D9%88%D9%84%D9%8A%D8%A7%D8%AA%D8%8C-%D8%A3%D8%AD%D8%B1%D8%A7%D8%B1-%D8%AD%D8%B1%D8%A7%D8%AA%D8%8C-%D9%85%D8%B2%D8%AF%D9%88%D8%AC%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%AC%D9%86%D8%B3%D8%9F

٣- **موقع «أنا وظلّي»**، للتعرف على معلومات خاصة بإستخدامك اليومي وأثره على كم المعلومات التي تفصح عنك - مؤسسة تاكتيكال تيك
https://myshadow.org/ar

٤- مبادئ الإنترنت النسوي - Association for Progressive Communication- ترجمة: مؤسسة «إختيار» للدراسات الجندرية
https://www.ikhtyar.org/?page_id=21309

٥- Security in a Box - أدوات وممارسات في الأمن الرقمي للجميع
/https://securityinabox.org/ar

6- **Our Data Ourselves** - Tactical Technology Collective:
https://ourdataourselves.tacticaltech.org/

7- **Safer Sisters** (GIFs)- Coding Rights
https://www.codingrights.org/safersisters-feminist-digital-security-hints-in-gifs

8- **The Wire** Guide to Digital Security
https://www.wired.com/2017/12/digital-security-guide/

9- Article 19

10- Global Advox- Neitizen Report

نتمنى لكم تحليقاً آمناً