

سلامتك الرقمية: رهينة اختيارك!

العمل الصحفي والنشاط المدني يعتبر من أكثر الأعمال التي يتم فيها تناقل وتداول للمعلومات المهمة سواء كانت معلومات سياسية أو أخبار حسرية، عادة ما تكون وسيلة تناقل هذه الأخبار في هذا الوسط عن طريق الاتصالات الشخصية أو البريد الإلكتروني بالتالي يكون صاحب هذا المجال عرضة للاختراق من أجل الوصول إلى "مصادر الأسماء أو جهات الاتصال، المراسلات مع هيئة التحرير، الأبحاث والوثائق والمقالات".

من أجل تأمين المعلومات التي تمتلكها هذه الجهة أو أي كيان أو شخص من الاختراق يجب أن يتم استخدام كل من الاتي:



كتيب إرشادي لدليل الاستخدام
الأمثل للتكنولوجيا التي بين يديك

استخدام شبكة افتراضية VPN عند استخدام الإنترنت من الأماكن العامة

عادة ما تقوم بعض الدول من حجب بعض المواقع الإلكترونية إما لكون هذه المواقع تنافي سياسات الدولة أو لوازع أخلاقي أو ديني أو لأسباب مجهولة، من شأن هذه السياسات أن تكون مضرّة بمصلحة المواطن حيث تحجبه عن الوصول إلى معلومة معينة أو من الولوج إلى موقع معين، في أغلب الأحيان يمكن تجاوز الرقابة عن طريق التمويه وتغيير عنوان الإنترنت إلى عنوان آخر يمكن أن يكون خارج البلد المقيم بها بالتالي لا يمكن أن تتأثر بالرقابة، عادة ما يساعد تغيير عنوان الإنترنت لدى المستخدم من تجاوز رقابة مقاهي الإنترنت التي تحتوي على عدد كبير من المستخدمين، حيث توجد إمكانية كون أحد المستخدمين شخص متطفل على بيانات الآخرين على نفس الشبكة وتعرف برمجيات تجاوز الرقابة على أنها عبارة عن برمجيات أو إضافات تعتمد على إنشاء...

تشفير البريد الإلكتروني والرسائل النصية

عن طريق هذه العملية يقوم المستخدم بحماية بريده الإلكتروني ورسائله الخاصة وتشفيرها بالتالي يصعب على المخترقين معرفة محتواها.

للقيام بالتشفير توجد عدة أدوات من شأنها أن تساعد في هذه العملية منها **"Mailvelope"** والتي تتوفر لكل من متصفح جوجل كروم، فايرفوكس.

لا يشترط أن يمتلك مستلم البريد الإلكتروني نفس هذه الأداة لفك التشفير إنما يمكنه أن يستخدم أي أداة أخرى. يمكن الاطلاع على كيفية تنصيب الأداة عبر الرابط:

<https://securityinabox.org/ar/guide/mailvelope/web>



تشفير البيانات الحساسة

البيانات الموجودة على جهاز الحاسوب أو الهاتف المحمول تعتبر بيانات شخصية وقد تكون هذه البيانات حساسة وسرية لا ترغب في أن يراها أحد حيث يمكن أن تمثل بيانات لمؤسسة ما أو لجهة معينة وتسريبها يمكن أن يسبب لك الضرر حتى وإن قمت بتخزينها في أجهزة تخزين محمولة ومن هذا المنطلق يجب إخفاء جميع بياناتك الحساسة عن أيدي المتطفلين. عملية إخفاء البيانات يطلق عليها مصطلح "التشفير" حيث يمكن أن يعرف بإخفاء جميع البيانات الموجودة على الأجهزة سواء كانت أجهزة حاسب آلي أو أجهزة هواتف محمولة عن أيدي الآخرين حتى لو كانوا مستخدمين على نفس الأجهزة.

توجد العديد من البرمجيات التي تهتم بتشفير البيانات منها "Vera Crypt".

شبكة خاصة افتراضية VPN تجعل الاتصال عبر الإنترنت يمر عبر خادم وسيط للوصول إلى الوجهة المرادة مساعدًا على تجاوز الرقابة والحجب. يوجد العديد من الأدوات التي من الممكن أن تستخدم لإنشاء الشبكات الافتراضية منها ما هو مجاني يعتمد على حصة شهرية معينة من الاستهلاك وآخر مدفوع.

من الأدوات المجانية لانتيرن "Lantern" وهو عبارة عن تطبيق يعمل على كل من أنظمة تشغيل الويندوز والماك والأوبنتو، حيث يعتمد هذا التطبيق على حصة شهرية معينة من الاستهلاك، إلا أن النسخة المدفوعة منه يمكن استخدامها بشكل كامل.



<https://getlantern.org/ar>

أيضًا توجد أداة: <https://www.hotspotshield.com>

وأداة: <https://your-freedom.net>

أيضًا <https://www.securitykiss.com>



تقوم هذه الأداة بتشفير جزء من القرص الصلب الموجود على جهاز الحاسوب أو على وسيلة تخزين خارجية ووضعتها داخل ملف واحد يدعى الحاوية ويمكن فتحها وإغلاقها برمز سري عن باستخدام "Vera Crypt" كي تمنع أشخاص غير مخولين من الوصول إليها، حيث يستخدم نظام التشفير الفوري on-the-fly عندما تكتب الملفات داخل المجلد الموجود بالقرص المراد تشفيره.

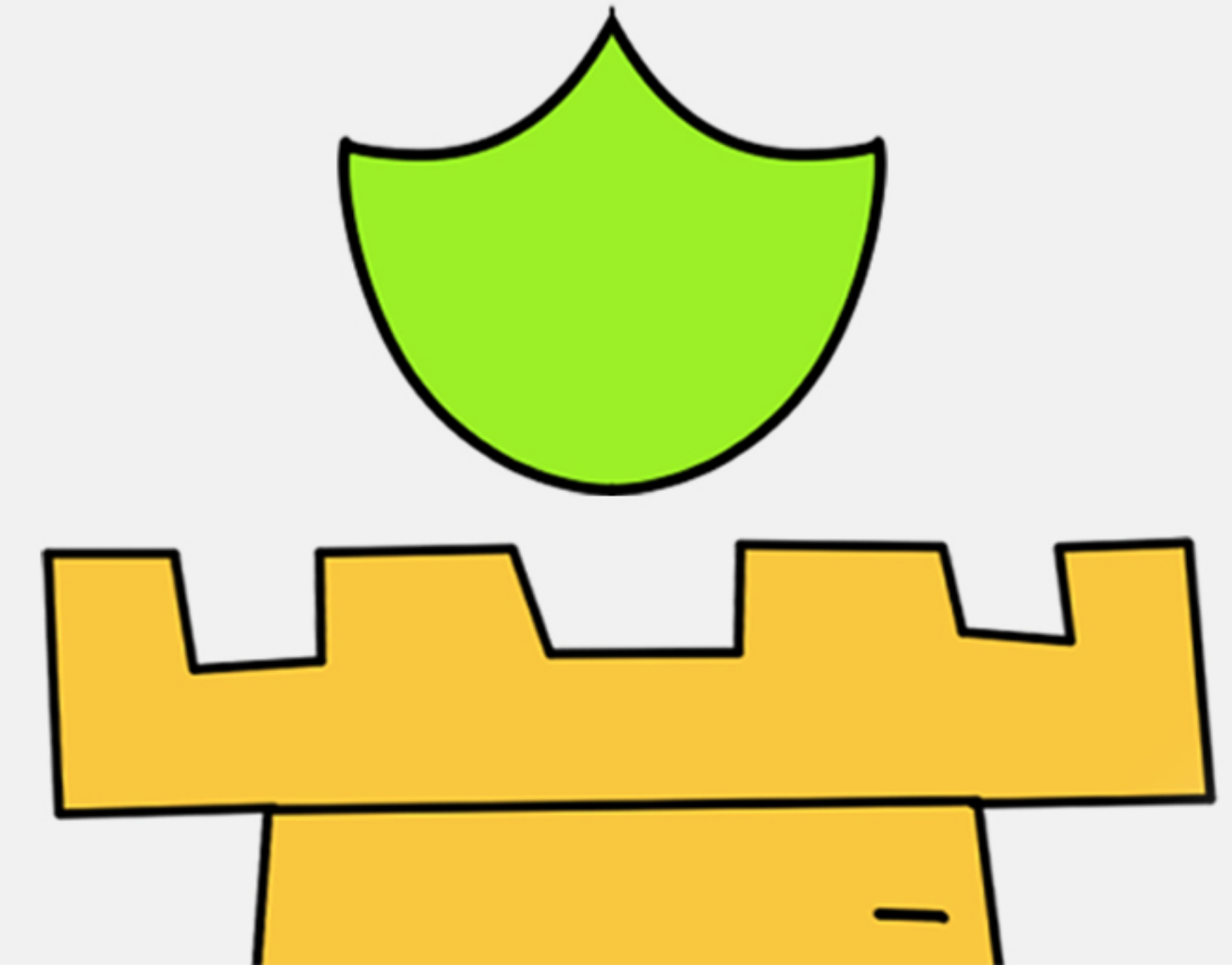


<https://www.veracrypt.fr/en/Downloads.html>

يهتم العمل المدني بالعديد من القضايا سواء كانت الاجتماعية منها أو السياسية أو البيئية أو التكنولوجية التي تمس حياة الناس، إلا أن بعض الأشخاص لا يتفق مع ضرورته بالتالي من الممكن أن يجلب بعض الخطر على العاملين بهذا المجال ومن أبرز هذه الأخطار التي تكون متعلقة بالأمن على الإنترنت، منها خطر انتحال الشخصية حيث يلحق ضرر كبير على الشخص مسبباً بذلك الشك في مصداقيته من قبل المتابعين له.

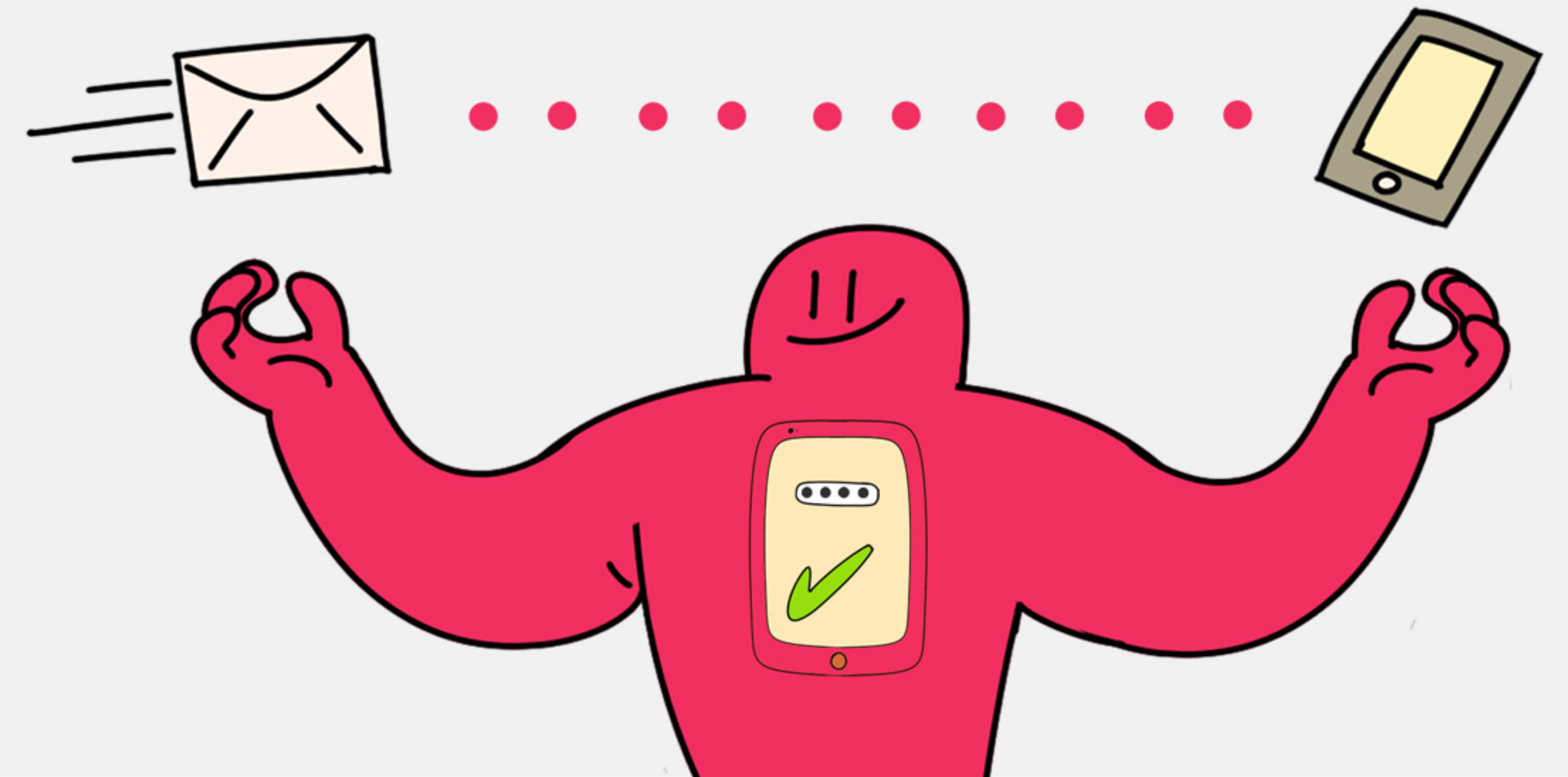
لحد من عملية القرصنة وانتحال الشخصية يجب اتباع بعض طرق الحماية منها:

أيضاً يوجد في أجهزة الويندوز برنامج يطلق عليه **BitLocker** يقوم بعملية تشفير البيانات.



تفعيل التحقق بخطوتين

هي عبارة عن ميزة توفرها شبكات التواصل الاجتماعي للمستخدمين للرفع من مستوى الأمن لديهم لتفعيل التأكد بين الحساب والمستخدم الراغب في الدخول اليه، حيث يقوم الحساب بإرسال رمز خاص بالمستخدم مكون عادة من ستة أرقام إلى بريده الإلكتروني أو هاتفه المحمول ومن ثم يقوم المستخدم بإدخالها للتأكد من مطابقته للحساب، تساعد هذه الميزة في إمكانية تغيير كلمة المرور لدى المستخدم في حالة نسيانها وتقوم بمنع المتطفلين من الوصول إلى جهازك إلى عن طريق المرور بها.



ومن التطبيقات التي تقوم بهذه العملية:

جوجل أوثنتيكاتور "Google Authenticator"



عبارة عن تطبيق مجاني يعمل على كل من أنظمة تشغيل "الآي أو إس، الأندرويد، البلاك بيري". يوفر هذا التطبيق إمكانية توفير رموز التحقق دون الاستعانة بشبكة الإنترنت أو الهاتف المحمول.

يوجد أيضًا أداة مايكروسوفت أوثنتيكاتور

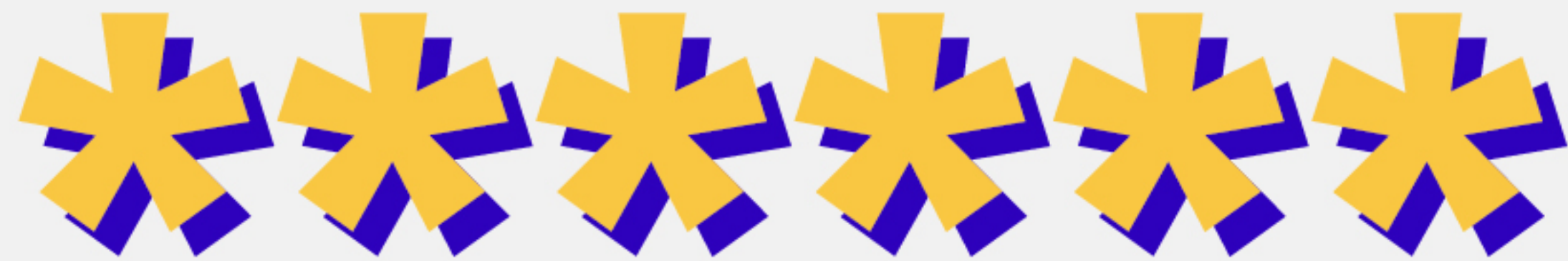


microsoft.com/en-us/account/authenticator

لتفعيل التحقق بخطوتين داخل حسابات مواقع التواصل الاجتماعي يمكن العثور عليها في خانة الإعدادات.

استخدام كلمات مرور قوية

عند إنشاء أي حساب إلكتروني لابد من الاختيار الأمثل لكلمة المرور حيث يفضل أن تكون خليط من الحروف الكبيرة والصغيرة والرموز والأرقام وأن لا تكون صغيرة الحجم، وأن يصعب تخمينها ويفضل أن تكون معقدة وأن يتم تغييرها بشكل دوري وأن لا تستخدم كلمات مرور مثل رقم هاتفك، تاريخ ميلادك أو أي شيء يكون له صلة مباشرة معك والناس ذو دراية به، هذا ويفضل أن تكون كلمات المرور مختلفة في شتى وسائل التواصل الاجتماعي أي لا تكون كلمة مرور كغيرها في وسيلة تواصل أخرى.



متابعة الأجهزة التي قامت بتسجيل الدخول عن طريقها

عن طريق هذه الميزة تستطيع أن تتابع جميع الأجهزة التي قمت بتسجيل الدخول عن طريقها وإمكانية تسجيل الخروج لأي جهاز كان حيث تتوفر هذه الميزة في أغلب مواقع التواصل الاجتماعي منها " فيسبوك، جوجل " حيث يمكن لمستخدمي الفيسبوك معرفة الأجهزة المتصلة عن طريق نفس الحساب ذلك عن طريق الذهاب إلى الإعدادات ومن ثم الأمان وتسجيل الدخول ثم المكان الذي سجلت دخلك منه حيث يقوم بعرض كافة الأجهزة المتصلة.



استخدام مدير كلمات المرور

يفضل أن تسير كلمة المرور على الأنماط الآتية:

1 التنوع في أشكال الأحرف اللاتينية الكبيرة والصغيرة بغير التزام بالقواعد الأصلية.

2 استبدال أحرف بأرقام.

3 استبدال أحرف برموز.

4 تضمين كلمات من لغات عدة.

5 كتابة كلمات عربية بأحرف لاتينية.

عندما نتكلم عن الحماية الإلكترونية نجد جميع المُستخدمين يقومون بتثبيت برامج الحماية المناسبة أو تثبيت نظام تشغيل أكثر آمنًا مثل Mac OS X أو Linux ومع ذلك تحدث بعض حوادث الاختراق فذلك غير كافٍ لحماية حساباتك وبياناتك، فالكثير من المُستخدمين يستخدمون كلمات مرور ضعيفة و سهولة التخمين رغم أن كلمة مرور حسابك تُعتبر خط دفاعك الأخير عن حسابك فلماذا لا نهتم بقوة كلمة المرور؟

كلمة المرور القوية يجب أن تكون بطول **16 حرف** وتحتوي على **رموز وحروف كبيرة وصغيرة وأرقام** ولا تحتوي على أسمك أو اسم المُستخدم أو أي بيانات خاصة بك لذا فإن كلمة المرور يجب أن تكون كلمة لم تخطر على بالك قط، كما يجب اختيار كلمة مرور مختلفة لكل حساب من حساباتك لأنه إذا تم اختراق حساب واحد فسيتم اختراق باقي الحسابات أيضًا إذا كنت تحميهم بكلمة مرور واحدة...

استخدام برامج الدردشة المجهولة

من أمثلة هذه البرامج برنامج سيجنال "Signal" حيث يقوم هذا البرنامج بتشفير مراسلاتك لضمان عدم استغلالها من قبل أي طرف حتى من قبل مطوري البرنامج أنفسهم. هذه البرامج متوفرة بشكل مجاني لكل من الويندوز والأندرويد والآي أو إس.



لتحميل هذا البرنامج عليك الذهاب إلى:

<https://www.signal.org>

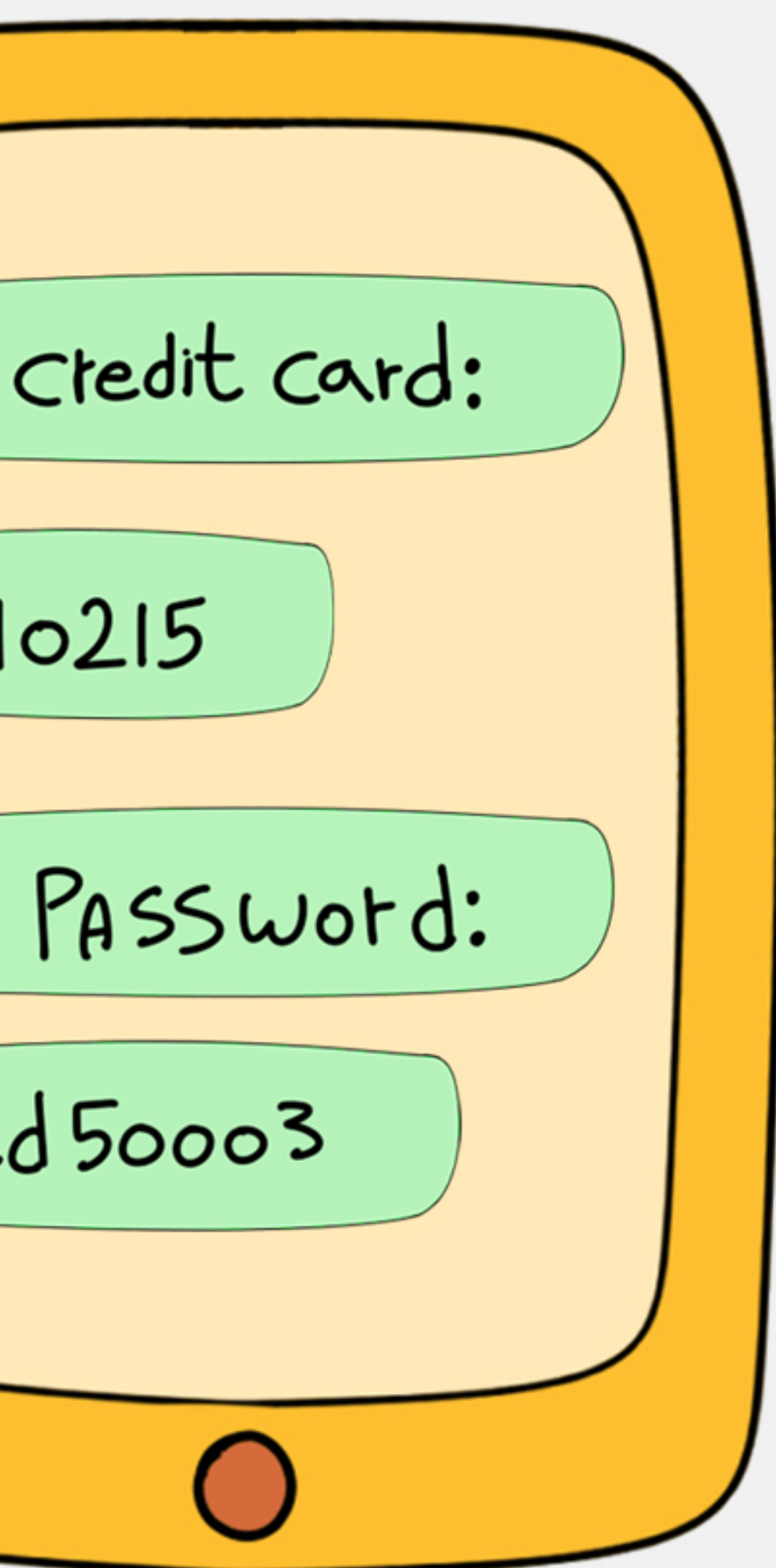
ومع وجود الكثير من المواقع الالكترونية التي يمكنك الاشتراك بها ستجد صعوبة في تذكر كلمات المرور لكل حساب، فمن سيقوم بذلك نيابة عنك؟ الاجابة هي "مدير كلمة المرور" عبارة عن برنامج أو تطبيق دوره هو انشاء كلمات مرور مُعقدة وحفظ جميع حساباتك مع كلمات المرور الخاصة بها وحمايتها.

من البرامج التي تساعد في إدارة كلمات المرور برنامج "كي باس" وهي عبارة عن أداة سهلة الاستخدام تعمل على كل من أنظمة الويندوز والماك واللينكس أيضاً على الأندرويد حيث تتمحور فكرته في تخزين كلمات المرور داخل قاعدة بيانات مشفرة بواسطة رمز سري ويمكن من خلالها أيضاً توليد كلمات مرور قوية، أيضاً هناك عدة أدوات أخرى منها برمجية "لاست باس".

للاطلاع على هذه الأدوات يمكنك زيارة الموقع المخصص لها:

<https://www.Keepass.info>

<https://www.lastpass.com>





التأكد من الروابط المختصرة

هناك بعض الأمور التي من الممكن أن تكونت سبباً للإلحاق الضرر بأي فرد كان في المجتمع نتيجة أفكاره الذي يقوم بمشاركتها مع الناس أو عن طريق بعض المعتقدات التي يتبناها فكرياً، لهذا يجب توخي الحذر واتباع بعض الإجراءات التي من الممكن أن تكون حائلًا بينك وبين الخطر منها:

استخدام برامج تجاوز الرقابة

متصفح **تور "Tor"** هو عبارة عن برنامج مفتوح المصدر يمكنك من خلاله تجاوز الرقابة والتجول بحرية على الإنترنت حيث يقوم بإخفاء بيانات تصفحك عن المتتبعين ويحميها ويستخدم أيضاً لتجاوز الحجب على المواقع .



للاطلاع أكثر على هذا البرنامج يمكنك زيارة الرابط:

<https://www.torproject.org>

عند القيام بفتح روابط صفحات الإنترنت عليك التأكد من صحة هذه الروابط ذلك بتوسيعها والتأكد من مكان توجيهها حيث أن عملية تزيف الروابط تعتبر من الطرق الفعالة في عملية انتحال الشخصية لذلك يجب التأكد منها قبل اتخاذ أي إجراء حيالها.

تحديث البرمجيات بشكل دوري

عند تحديث البرمجيات يقوم النظام بإصلاح الأخطاء والمشاكل الموجودة فيه حيث من الممكن أن تكون هذه الأخطاء مساعدة للمتطفلين الذين يستغلونها في إلحاق الضرر الإلكتروني بالناس.

استخدام إضافات المتصفح

توجد هناك مجموعة كبيرة من الإضافات التي تساعد في حماية بياناتك مساعدة لك في بعض المهام، إلا أن ليس كل الإضافات الموجودة تركز إضافات مفيدة فمنها ما هو ضار وقد يشكل وسيلة خطر عليك لذا يجب التأكد من سلامة الإضافة التي تريدها قبل تثبيتها لديك، ومن الإضافات التي قد تساعدك:

إتش تي بي إس في كل مكان **HTTPS Everywhere** حيث تساعد هذه الإضافة في تعزيز سلامتك أثناء زيارة المواقع المختلفة حيث يمكن عن طريقها زيارة الأماكن التي تحتوي على بروتوكول الأمان فقط مستخدمة بذلك الاتصال المشفر.

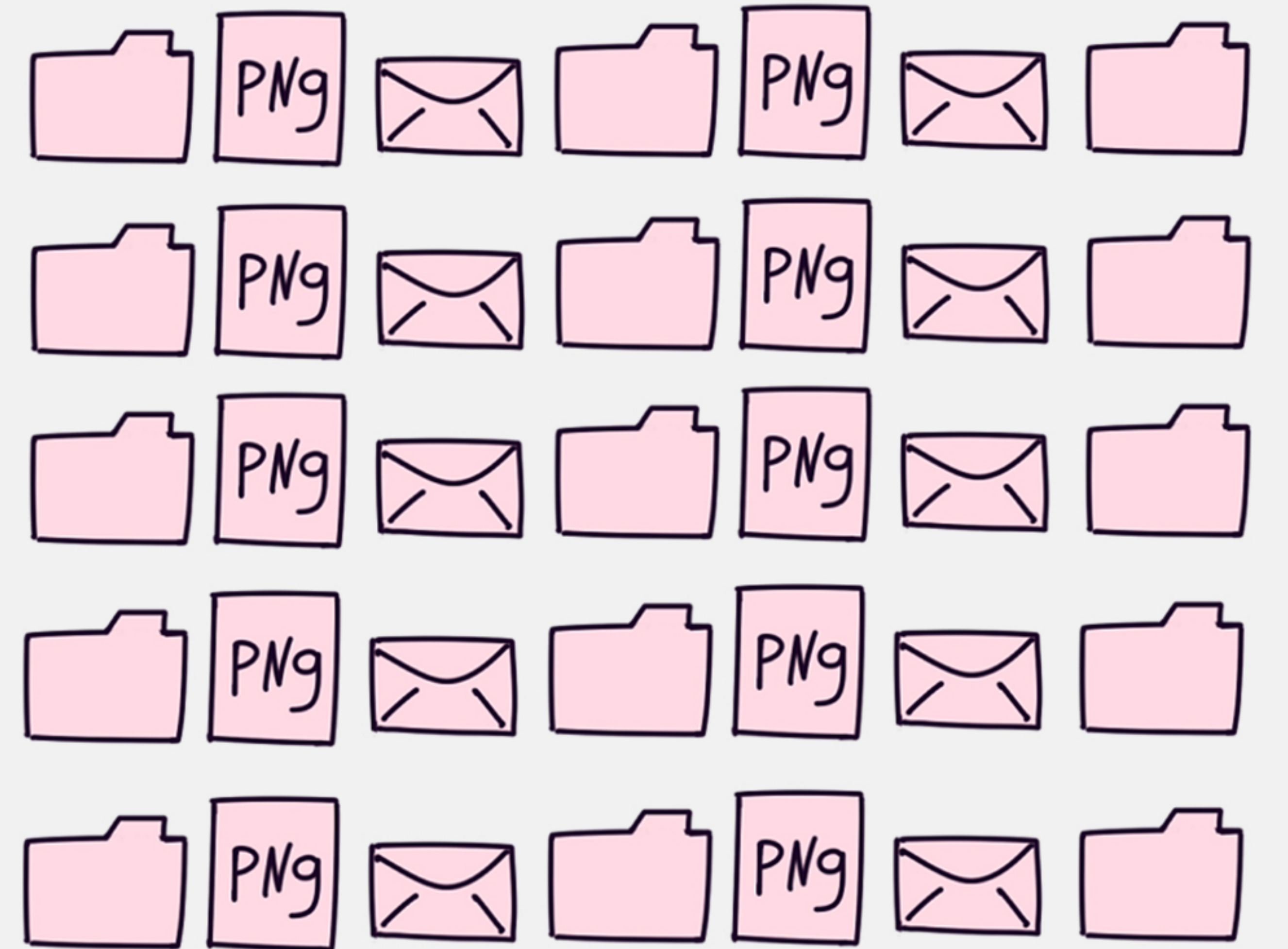


للاطلاع أكثر على هذه الأداة يمكن ذلك عن طريق:

<https://www.eff.org/https-everywhere>

مسح سجلات التصفح والدردشة

للتأكد من ضمان سلامتك بشكل أمثل عليك أن تقوم بتنظيف سجلات التصفح خاصتك والدردشات حيث تكون عرضة للتجسس عليها من ما يشكل خطراً على سلامتك الشخصية.



النسخ الاحتياطي

هي عملية تتم بشكل دوري لضمان عدم فقدان البيانات في حالة حدوث أي طارئ، حيث يمكن النسخ الاحتياطي من استرجاع البيانات وقت الحاجة لها.

من برامج النسخ الاحتياطي

في حالة استخدام الماك:

<https://securityplanner.org/#/tool/update-your-windows-computer>

في حالة استخدام الويندوز:

<https://securityplanner.org/#/tool/windows>

التحقق من إعدادات الخصوصية

عند استخدامك لمواقع التواصل الاجتماعي لابد من الفحص الدوري لإعدادات الخصوصية للتأكد من الناس المستهدفة في التواصل معها ومشاركة الأخبار لها.

استخدام البرامج مفتوحة المصدر

معظم البرامج الموجودة اليوم يوجد لها بدائل أخرى تعرف بالبرامج مفتوحة المصدر، توفر هذه البرامج خدمات مشابهة للبرامج التجارية الأخرى، حيث توفر هذه البرمجيات الخدمات بشكل مجاني وتوفر الدعم المستمر لها.

من المواقع الإلكترونية التي توفر عدد كبير من البرامج مفتوحة المصدر موقع:

<https://alternativeto.net>





هكسا كونشكن هي منظمة ليبية،
غير ربحية، تُعنى بالتنمية التكنولوجية،
تسعى للمساهمة في بناء وتطوير
المجتمع الليبي بواسطة التكنولوجيا،
تأسست سنة 2013.