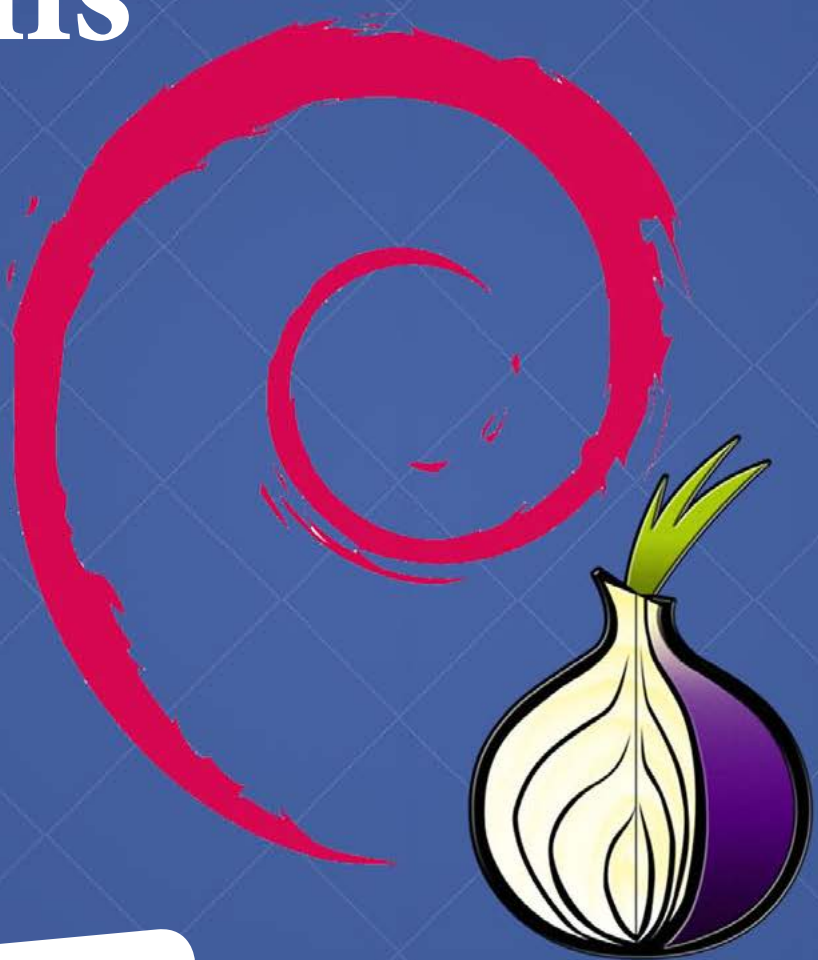
cyberarabs
Digital Security for the Arab World
الأمن الرقمي في العالم العربي

العدد 8 - ديسمبر/كانون الأول 2013

Tails



كيف يتم اختراقكم؟

نظام التشغيل «تايلز»

«تشات سيكيور» للدردشة الآمنة

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

للإتصال بنا:

magazine@cyber-arabs.com

تابعنا على:

مقدمة

سوزان فيشر

مرحباً بكم في العدد الثامن من مجلة «سايبر آرابز»

لقد وصلنا إلى الختام؛ إنه العدد الثامن والأخير من مجلة «سايبر آرابز».
بالطبع، سوف نستمر في تزويدكم بمعلومات ومقالات من عالم الانترنت على موقعنا، ولكن في المستقبل سوف ننشر المقالات بشكل متتالٍ حال جهوزها، لإعطائكم سرعة أكبر في الوصول إلى الأخبار والتنبيهات.

أيضاً، سوف تحصلون دائماً على آخر التحديثات والنصائح الأمنية على صفحة فيس بوك الخاصة بنا والتي لديها الآن اكثر من ٨٠,٠٠٠ متابع، وهو رقم يجعلنا فخورين وسعداء. لكن هذا لا يعني أننا لا نريد الوصول إلى عدد أكبر من الناس. ساعدونا على نشر الأخبار عنا حتى نصل إلى الرقم السحري ١٠٠,٠٠٠!

و ماذا لدينا لكم في عددنا الأخير؟ سوف نخبركم كيف تتمكنون من الدردشة مع أصدقائكم براحة، دون أن تشعروا بالقلق من أن يكون شخص ما يقرأ رسائلكم، وذلك عبر استخدام إما Cryptocat أو ChatSecure وكلا هاتين الأداتين تشفران دردشتكم وتجعلها خارج متناول الغرباء والأشخاص غير المرغوبين.

نساعدك أيضاً على التنقل عبر عالم الخدمات السحابية، بحيث يمكنكم اختيار أفضل وأسلم حل تخزين على الإنترنت لتلبية احتياجاتكم المحددة.

كما نقدم لكم عالم «تايلز» Tails حتى تتمكنوا من الاستفادة من نظام التشغيل الحي هذا، الذي من شأنه أن يساعدكم على حماية خصوصيتكم واستخدام الانترنت في الخفاء وعدم ترك أي أثر وراءكم. بالإضافة إلى ذلك، يساعدكم نظام «تايلز» على تشفير ملفاتكم وبريدكم الإلكتروني ورسائلكم الفورية. هل يبدو وكأنه أداة سحرية؟ جربوه.

أخيراً وليس آخراً، نشرح لكم كيف يجد المتسللون طريقهم إلى جهاز الحاسوب الخاص بكم، وهو أمر نأمل بالطبع ألا يحدث لكم بعد اتباع كل النصائح التي يقدمها فريق «سايبر آرابز».

نتمنى لكم ميلاداً مجيداً وعاماً سعيداً، وسوف نكون إلى جانبكم في العام ٢٠١٤.
مع أفضل التمنيات من فريق «سايبر آرابز»

سوزان فيشر
مديرة برنامج الشرق الأوسط
«معهد صحافة الحرب والسلام» (IWPR)

الدردشة باستخدام «كريبتوكات»

يستعمل الملايين من الناس خدمة التراسل الفوري أو الدردشة في مواقع مثل «فيس بوك» أو «غوغل»، كما أن خدمة الدردشة في «سكايب» تفوق بشعبيتها خدمة الإتصال الهاتفي الذي يوفره البرنامج نفسه. إلا أن برمجية الدردشة في «فيس بوك» و«غوغل» تولي التغطية الواسعة وسهولة الاستخدام أهمية أكبر مما تمنحه للتشفير. يسهل اختراق معظم هذه الخدمات، مما يتسبب بتسرب غير مرغوب لرسائلكم الخاصة، كما يترك «سكايب» نسخ غير مشفرة عن محادثاتكم على كل جهاز حاسوب تزورونه. كل ذلك يجعل من الواضح الحاجة إلى استعمال تطبيقات دردشة أكثر أمناً.

أحد هذه التطبيقات اسمه «كريبتوكات» Cryptocat ويمكن الوصول إلى موقعه من هنا. يعمل «كريبتوكات» من خلال المتصفح، بالاستعانة بإضافة خاصة. الإضافات التي تعمل مع المتصفحات التي تحظى بشعبية يمكن تحميلها وتنصيبها من الموقع، وثمة تطبيق آخر لأجهزة «ماك». يشفّر «كريبتوكات» رسائل الدردشة على أجهزة الحاسوب عبر استعمال معيار التشفير القوي AES-256، ومن ثم يبعثها إلى الشخص الذي تجرون معه المحادثة، ويقوم بفك التشفير على جهاز الصديق. بنفس الطريقة، يصبح من الصعب للغاية على أي طرف ثالث أن يعترض رسائلكم.

بعد تنصيب إضافة متصفح «كروم» أو «فَيرفوكس»، كل ما عليكم فعله هو انتقاء اسم مستعار وعنواناً لغرفة الدردشة الخاصة بكم. بعد النقر على «اتصال»، سيقوم «كريبتوكات» بتهيئة غرفة دردشة جديدة ومشفرة. في هذه الغرفة، يمكنكم أن تتحادثوا مع أي مستخدم «كريبتوكات» آخر. هذا الشخص يمكنه أن ينضم إلى الغرفة عبر تسجيل الدخول، مستخدماً اسم الغرفة نفسه الذي تستخدمونه.

غرفة الدردشة سهلة الاستخدام للغاية، بما أنه لا توجد خيارات كثيرة يمكن إعدادها. في أعلى اليمين، يمكنكم تغيير حالتكم، ورؤية بصمة التشفير على تطبيق «أو تي أر»، كما يمكنكم أن تشغّلوا خيار إشعارات سطح المكتب، وتشغيل الصوت، والخروج من غرفة الدردشة. أما في ما يتعلق بالباقي، يعمل «كريبتوكات» مثل أي تطبيق آخر للدردشة.

ثمة ميزة مهمة في البرنامج، وهي القدرة على إعداد دردشة خاصة، لا يمكن لأي أحد آخر غيركم والشخص الذي تتحادثون معه أن يطلع عليها. لفعل ذلك، أنقروا على اسم الشخص الذي تريدون التحدث إليه في غرفة الدردشة. تأكدوا دوماً من التدقيق في هوية الشخص قبل أن تشرعوا في مشاركة أي معلومات خاصة أو سرية.

مع أن هذه الطريقة تعتبر آمنة إلى حد بعيد، إلا أن القيّمين على «كريبتوكات» يشدّدون على محدوديّتها:

- «كريبتوكات» ليس أداة سحرية. عليكم ألا تضعوا حياتكم تحت رحمة أي برمجية.
- «كريبتوكات» لا يحميكم من الأشخاص غير الموثوقين أو البرمجيات التي تسجّل ضربات المفاتيح، كما لا يقوم بإخفاء هويتكم أثناء الإتصال بالانترنت.

خدمات التخزين السحابية

ودرجة الأمان التي تقدمها

تسمح لكم خدمات التخزين مثل Dropbox وGoogle Drive بتخزين نسخ احتياطية عن بياناتكم الخاصة على الانترنت والوصول إليها عبر أجهزتكم المختلفة. ولكن هل تكون بياناتكم آمنة عندما تخزن على هذه الخدمات؟ للجواب عن هذا السؤال، عليكم أولاً فهم الفرق بين التشفير الذي يحصل على خوادم مزود الخدمة، والتشفير الذي يحصل عند عبور بياناتكم شبكة الانترنت في طريقها بينكم وبين مزود الخدمة، والتشفير الذي يحصل على جهازكم الخاص.

التشفير على الخادم يحصل من قبل مزود الخدمة لمنع أطراف غير مصرح لها من الوصول إلى البيانات الموجودة على الخادم، عن طريق الاختراق أو مصادرة أجهزة المزود مثلاً. ولكن هذا النوع من التشفير لا يمنع مزود الخدمة نفسه من الوصول إلى بياناتكم الخاصة أو مشاركتها مع أطراف ثالثة إذا اختار ذلك أو أُجبر عليه، فكيفية التشفير وفكه تخضع لسيطرة المزود.

التشفير عند عبور بياناتكم شبكة الانترنت، كما في البروتوكول SSL/TLS المعتمد داخل الـ HTTPS، يحمي بياناتكم من المتطفلين خلال عبورها شبكة الانترنت بين جهازكم وبين خوادم المزود. هذه الآلية تقوم بتشفير البيانات قبل إرسالها وتقوم بفك التشفير عنها عند وصولها، مما يعني أن المزود أو أي طرف لديه إمكانية الوصول إلى خوادم المزود، يمكنه الوصول إلى بياناتكم الخاصة، إلا إذا كان المزود يستخدم أساليب إضافية لحمايتها.

التشفير على جهازكم الخاص يحصل من قبلكم بإستخدام مفاتيح التشفير الخاصة بكم. إفتراضاً أن تقنية التشفير قوية وأن مفاتيح فك التشفير الخاصة بكم تبقى سرية، فهذا النوع من التشفير يمنع أي طرف، إن كان مزود خدمة التخزين أو متطفل بينكما، من الوصول إلى ملفاتكم الخاصة.

وإذاً عندما يدّعي مزود خدمة تخزين بأن خدمته «آمنة»، قد يقصد بذلك أنه يستخدم أحد أساليب التشفير هذه، فمن المهم معرفة أي منها يستخدم لإدراك مدى أمان بياناتكم.

نحن في «سايبر آرابز» ننصحكم بإستخدام الخدمات التي تضع مسؤولية إدارة التشفير ومفاتيحه في أيدي المستخدم، فبنظرنا هذا النوع من التشفير هو الوحيد الذي يمكن القول عنه «آمن» بالفعل.

وفي ما يلي مقارنة لبعض خدمات التخزين الشهيرة مع بعض خدمات التخزين البديلة التي ينصحكم بها موقع «سايبر آرابز».

خدمة التخزين	المساحة المجانية	أين يحدث التشفير	وصول المزود إلى بيانات المستخدم	يعمل على
Dropbox	2GB	على الخادم	نعم	
GoogleDrive	15GB	تخزن البيانات غير مشفرة	نعم	
Skydrive	7GB	تخزن البيانات غير مشفرة	نعم	
Mega.co.nz	50GB	في المتصفح أو التطبيق على جهاز المستخدم	لا	
Wuala.com	5GB	في التطبيق على جهاز المستخدم	لا	
SpiderOak.com	2GB	في التطبيق على جهاز المستخدم	لا	
TeamDrive.com	2GB	في التطبيق على جهاز المستخدم	لا	

نقل جهات الاتصال بين أجهزة الأيفون والأندرويد

نضطر أحياناً إلى تبديل أجهزة هواتفنا الجوالة، وتقريباً كل البيانات، مثل الصور والفيديو والموسيقى والملفات المماثلة، يمكن نقلها بسهولة. لكن حين يتعلق الأمر بجهات الاتصال (Address book) (الجزء الأكثر أهمية من المعلومات المخزنة على الجهاز)، تبدو المهمة أصعب.

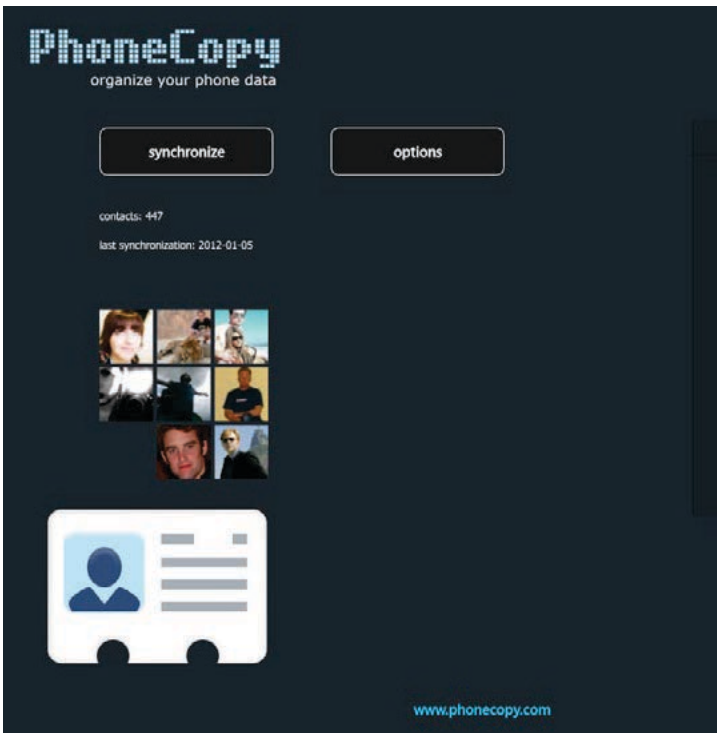
أولاً: الطريقة الأقصر (الحد الأقصى 500 جهة اتصال):

الطريقة الأسهل والأسرع لنقل جهات الاتصال بين جهاز أندرويد وأيفون، هي باستخدام موقع PhoneCopy. نقوم عبر هذا الموقع باستخدام تطبيق خاص بكلا الجهازين، وإعطاء الصلاحية للوصول إلى دليل الهاتف، ومزامنة (Synchronization) جهات الاتصال عبر خوادم الموقع.

لمزامنة جهات الاتصال علينا إنشاء حساب على الموقع، مجاني ومحدود بـ 500 جهة اتصال للمزامنة كحد أقصى؛ تتوفر حسابات مدفوعة لعدد أكبر من جهات الاتصال.

وبالإضافة إلى كون هذه الخدمة تهدف إلى مزامنة جهات الاتصال، يمكننا استخدام الموقع كمكان لإجراء نسخة احتياطية من جهات الاتصال لدينا، أو في حال كنا نمتلك جهازين، وعلى كل منهما قائمة بجهات الاتصال تختلف عن المتواجدة على الجهاز الآخر، نستطيع المزامنة بين القائمتين والحصول على جهات الاتصال نفسها على كلا الجهازين.

1 – بعد التسجيل في الموقع وتحميل التطبيق وتنصيبه على كلا الجهازين، سجلوا الدخول إلى حسابكم من التطبيق أولاً على الجهاز الذي تريدون نسخ جهات الاتصال منه.



2 – قوموا بالضغط على نسخ جهات الاتصال (Copy contacts)

3 – بعد انتهاء عملية النسخ، سجلوا الدخول على الجهاز الذي تريدون نسخ جهات الاتصال إليه، وقوموا بالضغط على مزامنة جهات الاتصال (Synchronize).

في حال كنتم تملكون أكثر من 500 جهة اتصال، تستطيعون دفع مبلغ 25 دولار والحصول على حساب بعدد غير محدود من جهات الاتصال، ولكن يمكنكم توفير هذا المبلغ لأننا سنرشدكم إلى طريقة أخرى لمزامنة جهات الاتصال مهما كان عددها.

ثانياً: الطريقة الأطول (عدد جهات الاتصال غير محدود)

لاستخدام هذه الطريقة نحتاج أولاً إلى استعمال جهاز الحاسوب بالإضافة إلى عدة برامج:

1 – برنامج Microsoft Outlook الذي يأتي مع مجموعة برامج Office

2 – MyPhoneExplorer وتستطيعون تحميله من هنا

3 – iTunes تستطيعون تحميله من هنا

4 – أيضا قوموا بتحضير كل من وصلات USB للجهازين لكي يتم وصلهما بجهاز الحاسوب

الخطوة الأولى – نسخ جهات الاتصال من جهاز أندرويد إلى الأوتلوك

1 – قوموا بإنشاء ملف على برنامج أوتلوك (تستطيعون مشاهدة فيديو عن الطريقة هنا)

2 – قوموا بتنصيب برنامج MyPhoneExplorer وتشغيله.

3 – فعّلوا خيار USB Debugging (تستطيعون مشاهدة الطريقة هنا) ثم قوموا بتوصيل جهاز أندرويد إلى الحاسوب عبر وصلة USB، ودعوا الجهاز يعمل في وضع الشحن (Charge only mode)

4 – من برنامج MyPhoneExplorer ، قوموا بالضغط على ملف > توصيل (File > Connect) سيقوم البرنامج بتخمين نوع جهازكم ثم يطلب منكم إضافته؛ قوموا بذلك.

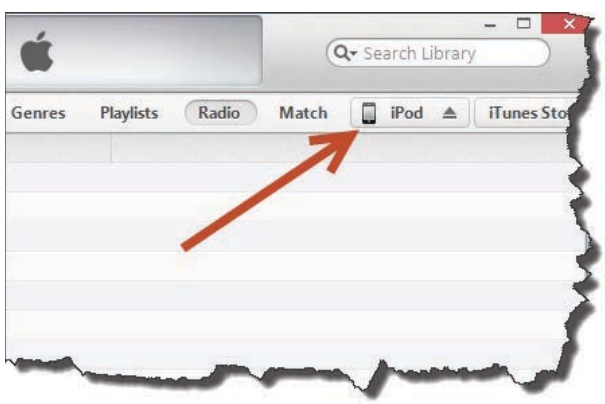
5 – إضغطوا على ملف > الإعدادات > مزامنة، ثم حدّدوا Outlook2007/2010 بالنسبة إلى جهات الاتصال أو File > Settings > Contacts: Outlook 2007/2010 Sync ثم اضغطوا على موافق.

6 – اضغطوا على زر المزامنة في البرنامج لتبدأ عملية نقل جهات الاتصال من هاتفكم الجوال إلى برنامج Outlook

الخطوة الثانية – نسخ جهات الاتصال من برنامج أوتلوك إلى جهاز أيفون :

1 – أوصلوا جهازكم إلى جهاز الحاسوب عبر وصلة USB، ثم شغّلوا برنامج iTunes

2 – اضغطوا على اسم جهازكم كما هو موضح في الصورة



3 – توجهوا إلى معلومات > مزامنة جهات الاتصال > أوتلوك أو Info > Sync contacts with > Outlook

4 – إضغطوا على «تطبيق» (Apply) لتبدأ عملية نقل جهات الاتصال من برنامج أوتلوك إلى الجهاز العامل بنظام أندرويد.

أخيراً، نستطيع القيام بنقل جهات الاتصال بالطريقة المعاكسة، من جهاز أيفون إلى جهاز أندرويد بتطبيق العملية بشكل معاكس، أي مزامنة الأيفون ثم مزامنة الجهاز العامل بنظام أندرويد.

التشفير باستخدام GPG4USB

تشفير (GNU Privacy Guard) GPG معروف بأنه أحد أقوى آليات تشفير الرسائل، ولكنها ليست سهلة الاستخدام، لذلك يتم استخدامها فقط من قبل الأشخاص الذين لا يستطيعون إنجاز أي عمل دون التأكد من الأمان التام لرسائلهم. أحد الأسباب التي تجعل من تشفير GPG يصنف على أنه «معقّد» هو استخدامه ما يسمى «المفاتيح» وهو المفهوم الذي يسبب الارتباك للمستخدم.

ما يفعله تشفير GPG هو التالي:

يقوم المستخدم بإنشاء مفتاحين، المفتاح الخاص والمفتاح العام، يتكوّنان من سلسلة من حروف عشوائية وتخزّن في ملف.

المفتاح الخاص لا تتم مشاركته، ويُحفظ على حاسوب المستخدم، بينما المفتاح العام تتم مشاركته مع الأشخاص الذين تريدون التواصل معهم. بالمقابل، يشارك هؤلاء الأشخاص أيضاً مفاتيحهم العامة معكم.

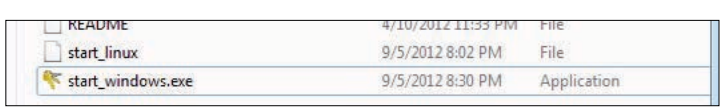
عندما تريدون توجيه رسالة، يتم تشفيرها عبر خوارزمية تدمج بين «المفتاح الخاص» العائد لكم، و«المفتاح العام» العائد للمتلقي.

يعني ذلك أن الأشخاص الذين يستطيعون فتح الرسالة هم فقط الأشخاص الذي وجّهت إليهم الرسالة، والذين شارك المستخدم معهم مفتاحه العام ويستطيعون تأكيد هويتهم عبر مفتاحهم الخاص، وهو محمي بكلمة سر.

هل لا زلتم تستطيعون المتابعة؟ إذا لحسن الحظ هناك برنامج يقوم بكل هذا عنكم؛ برنامج سهل ومحمول اسمه GPG4USB.

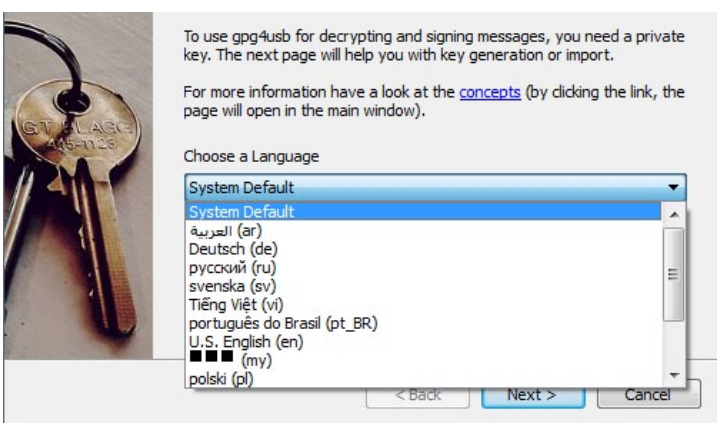
تستطيعون تحميل البرنامج من هنا، حيث يأتي بصيغة ملف مضغوط ZIP، ما يعني أنه يجب عليكم فك الضغط عنه ووضع الملفات في مكان ما على جهاز الحاسوب لديكم. ولأن البرنامج لا يحتاج إلى التنصيب، تستطيعون وضعه في أي مكان على حاسوبكم، أو على قرص USB.

في المجلد الذي قمتم بفك الضغط عنه ستجدون ملفاً اسمه «start_windows.exe». افتحوا الملف عبر النقر مرتين عليه،



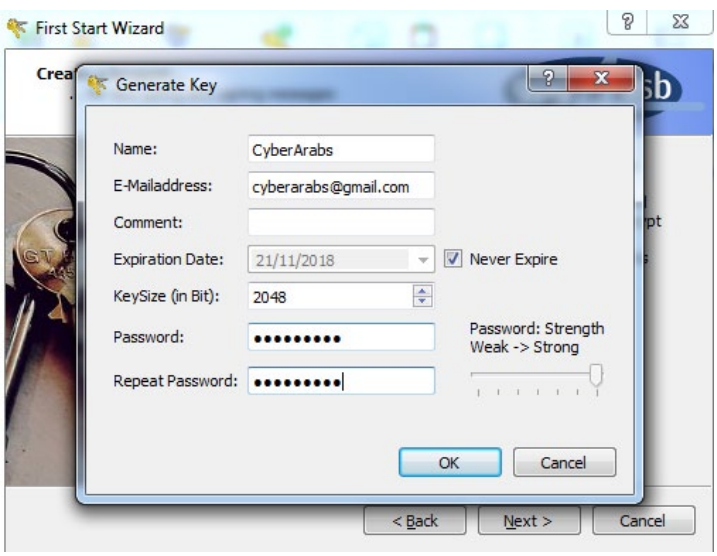
بعد أن يفتح البرنامج للمرة الأولى سيقوم بفتح نافذة مرشد الإعدادات. إذا لم تكونوا قد استخدمتم تشفير GPG من قبل ولا تملكون أية مفاتيح خاصة وعامة، ننصحكم باتباع الخطوات الموجودة في مرشد الإعدادات.

في النافذة الأولى سيطلب منكم اختيار اللغة



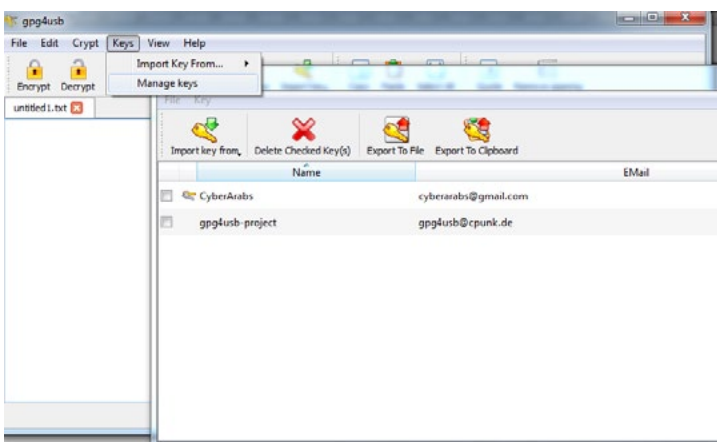
النافذة التالية ستسألكم عن المفاتيح الخاصة والعامة. إذا كان لديكم مفاتيح مسبقاً بإمكانكم استيرادها إلى البرنامج عبر النقر على الخيار الثاني. على كل حال، سنقوم بإنشاء زوج مفاتيح جديد، لذا انقروا على «create new keypair» أو «إنشاء زوج مفاتيح جديد» لإنشاء مفتاح خاص وآخر عام خاصين بكم.

لإنشاء زوج مفاتيح جديد عليكم تزويد البرنامج ببعض المعلومات. تأكدوا من إدخال عنوان بريدكم الإلكتروني بشكل صحيح، وذلك لتسهيل إيجاد مفتاحكم العام من قبل جهات الاتصال. أيضاً، اختاروا كلمة سر قوية (راجعوا مقالاتنا عن كلمات السر هنا وهنا وهنا). بعد ملء البيانات، أنقروا على OK؛ ستتم إضافة مفاتيحكم تلقائياً إلى قاعدة بيانات البرنامج.



في النافذة الأخيرة بإمكانكم اختيار «لا أريد ظهور مرشد الإعدادات مرة أخرى أو I don't want to see the wizard again»، حددوا هذا الخيار إذا انتهيتم من إنشاء مفاتيحكم أو استيرادها.

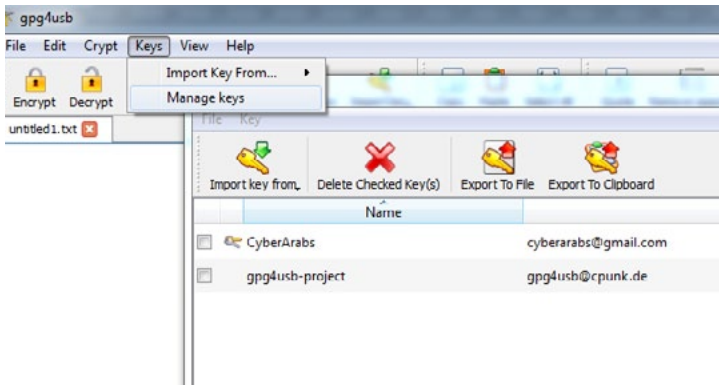
بعد إغلاق نافذة مرشد الإعدادات، انتقلوا إلى نافذة البرنامج. تتألف الشاشة من عدة أزرار، وحقل نصي، وقائمة بجهات الاتصال التي تملكون مفاتيحها العامة. إذا كانت هذه المرة الأولى التي تستخدمون البرنامج فيها، ستلاحظون وجود مفتاح واحد فقط، وهو المفتاح العام العائد إلى مطور البرنامج. الخطوة الأولى التي يجب عليكم اتباعها هي مشاركة مفتاحكم العام مع أصدقائكم وإضافة مفاتيحهم العامة، ويتم ذلك (إضافة إلى كل عمليات إدارة المفاتيح) عبر النقر على «إدارة المفاتيح» أو Manage keys.



بعد الذهاب إلى نافذة «إدارة المفاتيح» تستطيعون استيراد المفاتيح، أو حذفها، أو تصديرها. تأكدوا من أنكم لا تقومون بحذف مفتاحكم الخاص، ومن المفضّل أن تصدّروا مفاتيحكم لإنشاء نسخ احتياطية منها، وتخزينها في مكان ما على

حاسوبكم أو في مكان آمن، حتى لا تضطرون إلى إنشاء زوج مفاتيح جديد في كل مرة تودون تشفير رسالة فيها.

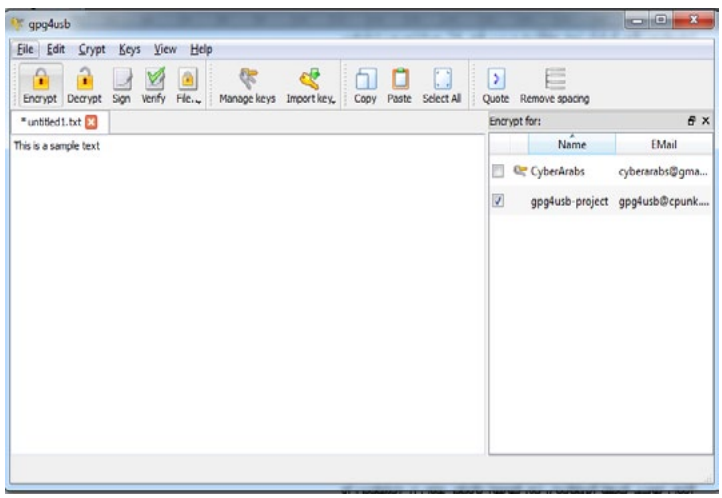
لتصدير مفاتيحكم انقروا على «تصدير إلى ملف» أو Export to file، وثم اختاروا مكان تصدير المفتاح.



أما لاستيراد مفاتيح أصدقائكم أنقروا على Import keys from > File

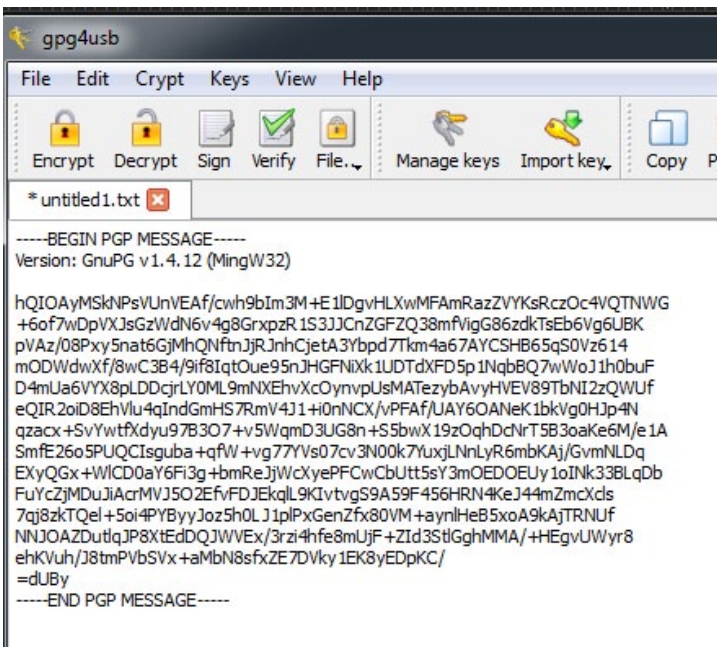
ولأن المفاتيح هي عبارة عن نص فقط، فبإمكانكم أيضاً مشاركة مفاتيحكم عبر نسخ المفتاح العام ولصقه في رسالة إلكترونية. المفتاح العام ليس سرياً، لذا بإمكانكم مشاركته أو وضعه في أي مكان.

بعد الحصول على مفاتيح جهات الاتصال لديكم، تبقى عملية إرسال رسالة مشفرة، وهي في غاية السهولة الآن.



اطبعوا الرسالة في الحقل النصي المخصص لها (أو انسخوها والصقوها من مكان آخر إذا أردتم)، ثم اختاروا الأصدقاء الذين تودون توجيه الرسالة إليهم عبر القائمة الجانبية التي توجد فيها المفاتيح، وانقروا على زر «تشفير» أو «Encrypt». سيتحول نص الرسالة إلى شكل يشبه هذا:

هذا هو نص الرسالة المشفر. انسخوا هذا المحتوى وشاركوه مع أصدقائكم عبر البريد الإلكتروني، أو قد تودون وضعه في ملف نصي وإرساله.



إذا استقبلتم رسالة مشابهة، أي مشفرة بالشكل التالي، بكل بساطة انسخوا المحتوى المشفر وضعوه في حقل النص في البرنامج ثم انقروا على زر «فك التشفير» أو «Decrypt». إذا كانت الرسالة المشفرة موجهة إليكم، سيطلب منك البرنامج إدخال كلمة المرور المرتبطة بمفتاحكم الخاص. بعد إدخالها تستطيعون قراءة الرسالة بعد فك تشفيرها.

كيف يتم اختراقكم؟

يصل فريق «سايبر آرابز» من القراء العديد من الأسئلة المتعلقة باحتمال اختراقهم. الاختراق هو عملية اقتحام جهاز حاسوب أو موقع إلكتروني أو خدمة بريد إلكتروني أو هاتف نقال.

تتم غالباً سرقة معلومات حساسة خلال عملية الاختراق، ما يشكل خطراً على المستخدمين الذين تم اختراقهم أو يضر بأعمالهم. ولأن العديد من الأشخاص يتعرضون للاختراق اجمالاً، سنلخص كيف تتم عملية الاختراق وكيف يمكننا تجنبها.

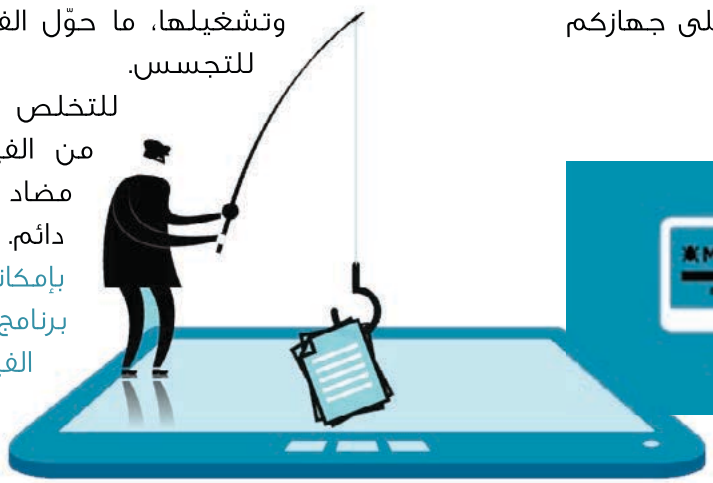
أجهزة الحاسوب المكتبية والمحمولة

إذا كنتم متصلين بشبكة الإنترنت، هناك العديد من الطرق التي يستطيع بها المخترق الوصول إلى جهاز الحاسوب الخاص بكم، ويتضمن ذلك الملفات المخزّنة على جهازكم والأجهزة المتصلة بالجهاز كالطابعات والكاميرات مثلاً.

من أسهل الطرق التي يلجأ إليها المخترقون هي الفيروسات أو ملفات التجسس.

غالباً ما يصاب جهاز المستخدم بهذه البرامج عبر النقر على رابط خبيث أو تحميل ملف من مكان غير موثوق به. تتراوح هذه الأماكن غير الموثوقة بين أقراص الـ USB ورسائل سكايب والمواقع المصابة.

على سبيل المثال، تم تصميم فيروس يستهدف النشطاء السوريين، وانتشر هذا الفيروس ليصل إلى العديد من الأجهزة في العالم العربي، وقد كان غير مكتشف من قبل مضادات الفيروسات لفترة طويلة. انتشر هذا الفيروس عبر رسائل من حسابات سكايب وبريد إلكتروني مخترقة، وأتاح للمخترق الوصول إلى جهاز الحاسوب الخاص بالضحية، بالإضافة إلى ذلك كان بإمكان المخترق الوصول إلى الميكروفونات والطابعات والكاميرات الموصولة بالجهاز وتشغيلها، ما حوّل الفيروس إلى أداة للتجسس.



للتخلص من هذا النمط من الفيروسات، نصّبوا مضاد فيروسات بشكل دائم.

بإمكانكم استخدام برنامج «أفيرا» لرصد الفيروسات والملفات الخبيثة الأخرى.

إحدى الطرق الأخرى التي يعتمدها المخترقون للوصول إلى حاسوبكم هي شبكة انترنت «وايرلس» (Wi-Fi) التي تتصلون بها

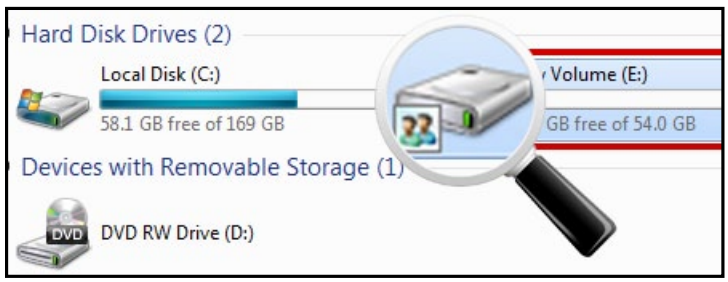
حيث يمكن لكل الأجهزة المتصلة بالشبكة ذاتها الاتصال بجهازكم مباشرة، لذلك عليكم التأكد من أنكم أغلقتم كافة «الأبواب» في أجهزتكم. وفي لغة علم الشبكات، يطلق على الأبواب «منفذ» أو Port، وبإمكان المخترق إجراء فحص على الشبكة لمعرفة ما هي الأجهزة المتصلة، والمنافذ المفتوحة في كل جهاز.

بإمكانكم إغلاق هذه المنافذ عبر تفعيل جدار الحماية على جهازكم، يوجد واحد ملحق مع الويندوز بإمكانكم تفعيله عبر الذهاب إلى لوحة التحكم > النظام والأمان > جدار الحماية أو Control panel > System and Security > Firewall

ملاحظة: معظم الأحيان يأتي جدار الحماية ملحقاً مع برامج مضاد الفيروسات (أفيرا مثلاً) لذلك من الأفضل تفعيل جدار حماية واحد فقط.

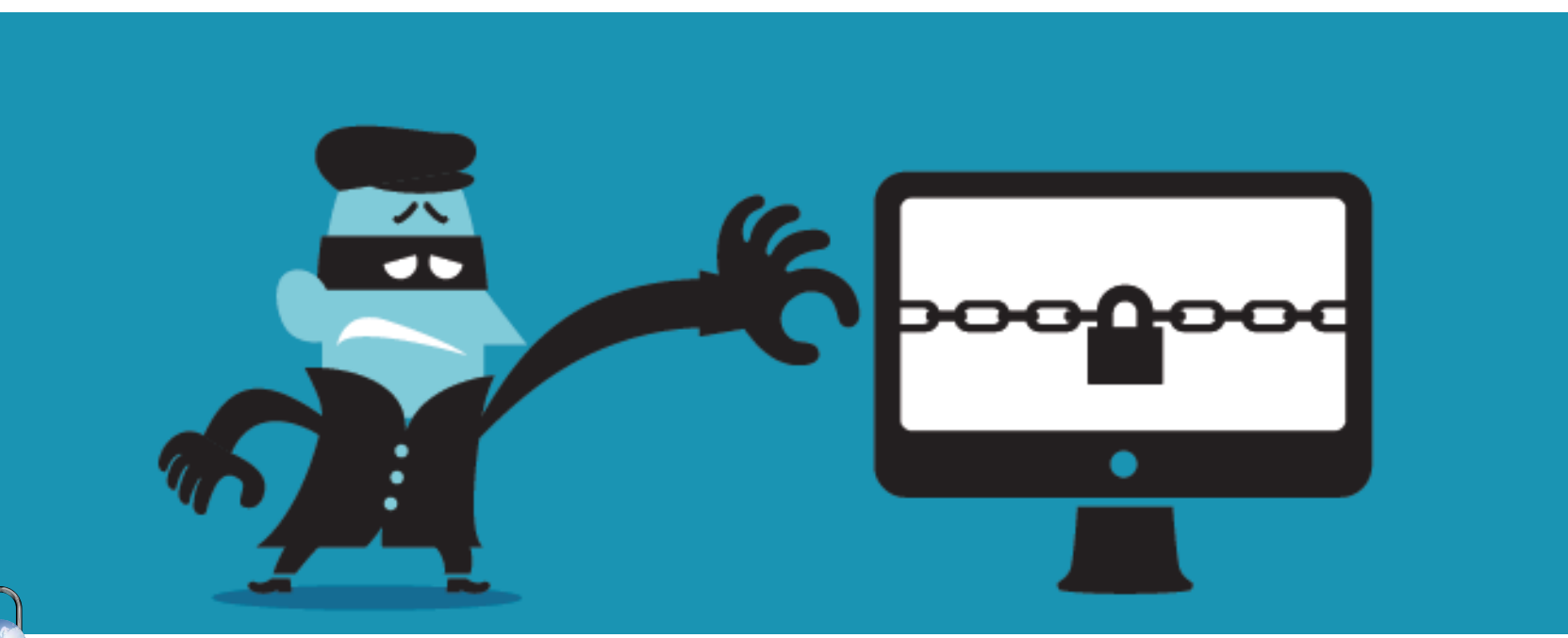
أيضاً قد يتم اختراقكم بسبب ضعف إعدادات الأمن في «راوتر» الإنترنت الذي تستخدمونه. لمعرفة كيفية زيادة الأمان في الـ«راوتر» لديكم بإمكانكم قراءة مقالنا هنا.

خطأ آخر يقع فيه المستخدمون، هو مشاركة سواقات الأقراص أو المجلدات عبر الشبكة. بإمكانكم التأكد بسهولة من الملفات التي تشاركونها عبر مشاهدة رمز يد تحمل المجلد الذي تفحصونه. إذا صادفتم مجلداً كهذا انقروا بالزر الأيمن عليه واختاروا خصائص > مشاركة. من هنا، بإمكانكم إيقاف مشاركة هذا المجلد.



البريد الإلكتروني... وخدمات الويب الأخرى

تشكل خدمات الويب، مثل البريد الإلكتروني والشبكات الاجتماعية، أهداف شائعة جداً بالنسبة إلى المخترقين، والقليل منكم يعرف أن هذه المواقع تساعد المخترق على الوصول إليكم. الخطأ الأول الذي يقع به المستخدم هو مشاركة قدر كبير من المعلومات الشخصية على الصفحات مثل فيس بوك أو تويتر. فعملية إعادة ضبط كلمة المرور غالباً ما تتطلب بعض المعلومات الشخصية. وبالعودة إلى مشاركة الكثير من



إحدى الطرق الشائعة أيضاً للحماية من المخترقين، هي اختيار كلمة سر قوية والتأكد من عدم مشاركتها مع أي شخص.
للقراءة عن كيفية اختيار كلمة سر قوية وحمايتها يرجى قراءة هذا المقال

المعلومات الشخصية، هذه العملية تسهل على المخترق إعادة ضبط كلمة المرور كما لو كنتم أنتم من يقوم بذلك.
لذا، تفادوا مشاركة تفاصيل عن حياتكم الشخصية كتاريخ الميلاد، واستخدموا عنوان بريد إلكتروني لا تعتمدونه عادةً للاشتراك في المواقع الأخرى.

KeyLogger، ملفات خبيثة صغيرة تقوم بتسجيل كافة الضربات على لوحة المفاتيح، وهي تعد في رأس القائمة للطرق التي يتبعها المخترق لمعرفة كلمات سر الضحية. تنتشر هذه النوعية من الملفات عبر تشغيل ملف تم تحميله من البريد الإلكتروني أو من أماكن أخرى على الإنترنت، حيث يتم تسجيل كل الضربات على لوحة المفاتيح وإرسالها للمخترق دون معرفتكم، ثم يقوم المخترق باستخدام هذه البيانات للدخول إلى حساباتكم وبريدكم الإلكتروني.

حالما يقوم المخترق بولوج الشبكة التي تتشاركونها (مقهى إنترنت مثلاً) يصبح بإمكانه مراقبة كافة بياناتكم على الإنترنت، إلا أن المواقع التي تبدأ بـ https مشفرة ولا أحد يستطيع معرفة ماذا تفعلون خلالها سواكم، لذا من الجيد التأكد من الدخول إلى مواقع مثل فيس بوك وجيميل وتويتر عبر بروتوكول HTTPS والمعروف أيضاً بتشفير SSL، وإذا لم يكن ذلك ممكناً فبإمكانكم تشفير بيانات الإنترنت التي تقومون بإرسالها واستقبالها عبر استخدام VPN أو SSH. لمعرفة المزيد عن كيفية حماية الشبكة لديكم بإمكانكم مراجعة هذا المقال.

وتأكدوا من الدخول إلى المواقع باستخدام HTTPS، أو الاتصال عبر VPN أو SSH. بإمكانكم معرفة المزيد عن إعداد بروكسي آمن على هاتفكم الذكي هنا وهنا.

الهواتف الذكية

يمكن اعتبار الهواتف الذكية الحديثة أجهزة حاسوب صغيرة، ومعظم المخاطر التي ذكرناها أعلاه تنطبق أيضاً على الهواتف الذكية. لذا، توخوا الحذر أثناء تحميلكم التطبيقات على أجهزتكم.
على كل حال، معظم الأشخاص سيئو النوايا يقومون بالوصول إلى هاتفكم عبر سرقته أو مصادرته، في هذا الحال الطريقة الوحيدة لحماية بياناتكم هي تشفير هاتفكم الذكي (لمعرفة المزيد قوموا بقراءة المقال التالي) وأيضاً بإمكانكم تنصيب تطبيق حماية الهاتف «SOPHOS» من هنا.

نظام التشغيل "تايلز"

ما هو "تايلز" (TAILS):

"تايلز" هو نظام تشغيل مباشر مبني على لينكس (Linux) يمكن تشغيله تقريباً على أي جهاز كمبيوتر من قرص DVD أو جهاز تخزين USB. يهدف "تايلز" إلى الحفاظ على الخصوصية وإخفاء هوية المستخدم ويساعدكم على تنفيذ ما يلي:

1. **إستخدام شبكة الانترنت بتخفٍ والتغلّب على الحجب:**

يفرض "تايلز" على كافّة الاتصالات بالانترنت المرور من خلال شبكة "تور" (Tor)، وهي شبكة تخفٍ مفتوحة تحمي خصوصيّتكم على الإنترنت، عن طريق تمرير اتصالاتكم عبر شبكة خوادم موزّعة عبر العالم ويديرها متطوعون. يمنع "تور" من يراقب اتصالاتكم بالانترنت من معرفة المواقع التي تزورونها ويمنع تلك المواقع من تحديد أماكن تواجدكم. إنّ جميع البرمجيات في "تايلز" معدة للإتّصال بشبكة الإنترنت عبر "تور" وإذا حاول أحد البرامج الاتصال بشبكة الإنترنت مباشرةً، وليس من خلال "تور"، يتم حظر الاتصال تلقائياً لدوافع أمنية.

2. **عدم ترك أي أثر على جهاز الكمبيوتر المستخدَم إلا إذا طُلب ذلك من "تايلز" بوضوح:**

تم إعداد "تايلز" بحرص للاستغناء عن القرص الصلب (Hard Disk) والتشغيل الكلّي على ذاكرة الوصول العشوائي (RAM) في الكمبيوتر التي يتم محوها تماماً عندما يُطفأ الجهاز. يعني هذا أنّ استعمال "تايلز" لا يعتمد على نظام التشغيل المثبّت في الكمبيوتر ولا يعدّل جهازكم بأي شكل من الأشكال إلّا إذا طُلب منه ذلك. إذاً يمكنكم استعمال "تايلز" بالطريقة نفسها على جهازكم، أو جهاز أصدقائكم، أو على جهاز عمومي، فبعد فصل قرص الـ DVD أو جهاز تخزين USB لن يبقى أي أثر لاستخدام "تايلز" ويمكنكم إعادة تشغيل الكمبيوتر على نظامه المعتاد. ويمكّنكم هذا من العمل على وثائق حسّاسة من أي كمبيوتر ويحميكم من محاولات استعادة البيانات بعد الإغلاق.

بطبيعة الحال، يبقى بإمكانكم حفظ الوثائق على جهاز تخزين USB آخر أو قرص صلب خارجي إذا اخترتم ذلك.

3. **استخدام أدوات التشفير للملفات الخاصة والبريد الإلكتروني والتراسل الفوري:**

يحتوي "تايلز" على العديد من البرامج المهيأة مسبقاً للحفاظ على الأمن: متصفح الانترنت، برنامج دردشة، برنامج البريد الإلكتروني، برامج مكتبية، محرر للصور، محرر للصوت، إلخ...
ويحتوي أيضاً على مجموعة مختارة من أدوات الحماية للبيانات الخاصة الّتي تستخدم التشفير القوي وتمكّنكم من:

- تشفير جهاز تخزين USB أو قرص ثابت خارجي باستخدام نظام تشفير لينكس (Linux) الأكثر استعمالاً "LUKS".
- التبديل التلقائي إلى HTTPS الآمن عند تصفح مواقع تدعم إستعمال "HTTPS Everywhere"، وهو إضافة لفيرفوكس (Firefox) طوّرتها "مؤسسة الحدود الإلكترونية" (Electronic Frontier Foundation).
- تشفير وتوقيع بريدكم الالكتروني ووثائقكم باستخدام "Open PGP" إما من مرسل البريد الالكتروني أو محرّر النصوص أو متصفّح الملفّات لدى "تايلز".

- حماية محادثات رسائلكم الفوريّة باستخدام أداة OTR للتشفير والتّصديق والإنكار.

- محو ملفّاتكم وتنظيف مساحة القرص في جهازكم باستخدام Nautilus Wipe.

الحدود والاخطار:

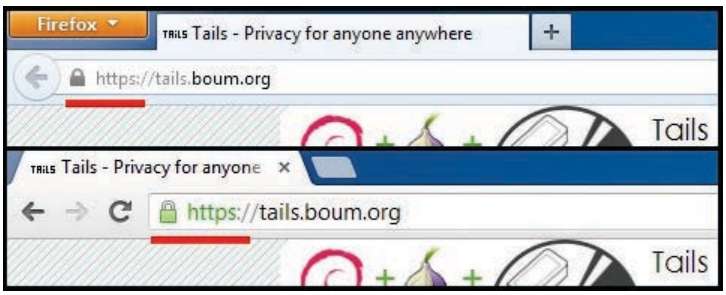
رغم أنّ "تايلز" يستخدم شبكة "تور" (TOR) ليخفي موقعكم وهويتكم ويمنع مراقبة نشاطاتكم على شبكة الانترنت، فلا يزال عليكم التأكد من تشفير أي بيانات حسّاسة ترسلونها ومسح أي حقائق تعريف ومعلومات وصفية (Metadata) بأنفسكم. فحتى ولو لم يكن بإستطاعة أحد التَعرّف على المكان الذي أتت منه البيانات، فالبيانات بذاتها يمكن أن تُعترض. وبالإضافة إلى ذلك، فإنّ مزود خدمة الإنترنت والخادم الذي تحاولون الاتصال به بإمكانهما معرفة أنّكم تستخدمون "تور".

إذا كنتم ترغبون في إجراء مهمتين مختلفتين أو إستخدام هويتين في سياقين منفصلين، فلا تستعملوا الجلسة ذاتها من "تايلز". مما يعني أنه عليكم إطفاء جهازكم وإعادة تشغيله مرة أخرى مع "تايلز" للتأكد من عدم وجود برامج قيد التشغيل أو ملفات مؤقتة أو إتصالات منشأة على شبكة "تور" يمكنها الكشف أن المستخدم نفسه قام بالمهمتين.

وأخيراً، تذكروا دوماً أن تستخدموا أحدث نسخة من "تايلز"، لأنّ "تايلز" وجميع البرمجيّات التي يشملها هي في تطّور مستمر، وبإمكانها أن تحتوي على أخطاء برمجية أو ثغرات أمنية.

التحميل، التثبيت، والإقلاع:

لتحميل "تايلز"، زوروا موقع tails.boum.org وتحققوا من صحّة العنوان وأنه يُعرض من خلال بروتوكول HTTPS عن طريق التأكّد من أنّ العنوان يبدأ بـ "https" بدلاً من "http" والبحث عن رمز قفلٍ أو منطقة ملونة تحتوي على اسم الموقع يعرضهما المتصفح إلى جانب العنوان.



ثمّ قوموا بتحميل أحدث نسخة من «تايلز».

قد ترغبوا في التحقق من سلامة الملف بعد تنزيله. التعليمات للقيام بذلك متوفرة على موقع «تايلز».

الآن وقد أصبح لديكم ملف «تايلز» الذي ينتهي بلاحقة ISO.، أصبح بامكانكم حرقه على قرص DVD أو تثبيته على جهاز تخزين USB. الفائدة من حرق «تايلز» على قرص DVD غير قابل لإعادة الكتابة هي طمأنتكم لعدم وجود تغييرات دائمة وربّما خطرة يمكن إدخالها على نظام «تايلز» الخاص بكم، سواء عن طريق الخطأ أو من خلال أحد المهاجمين. من ناحية أخرى، من الأسهل حمل جهاز تخزين USB ولكن عندها يصبح بإمكان فيروس أو مهاجم يملك وصول فعلي إلى جهاز التخزين إجراء تغييرات على نظامكم. إذا كنتم ترغبون في تقليل هذه المخاطر فيمكنكم مسح جهاز تخزين USB وإعادة تثبيت «تايلز» عليه بشكل منتظم.

واعلموا أيضا أن بعض أجهزة الكمبيوتر القديمة قد لا تدعم الإقلاع من جهاز تخزين USB.

لحرق «تايلز» على قرص DVD من خلال «ويندوز 7» (Windows 7) أنقروا بزر الفأرة الأيمن على على ملف الـ ISO واختاروا «Burn disc image». قد تحتاجون إلى تثبيت برنامج حرق DVD مثل Infra Recorder المجاني من infrarecorder.org على إصدارات قديمة من ويندوز. عند تثبيته، أُدخلوا على البرنامج وانقروا على «Actions» ثم «Burn Image» وحددوا ملف « تايلز» ISO.

بإمكانكم الحصول على المزيد من التعليمات هنا.

لتثبيت «تايلز» على جهاز تخزين USB أو على بطاقة الذاكرة SD، يجب أن تكون سعة أي منهما 1 جيغابايت (GB) على الأقل وقوموا بتثبيت برنامج مثل «Linux Live USB Creator» أو Unetbootin على ويندوز. اعلموا أنّ تثبيت «تايلز» على جهاز تخزين USB سيمحي محتوياته. كل ما عليكم فعله مع كل من هذه البرامج هو اختيار جهاز تخزين USB وتحديد ملف ISO ثم التثبيت.

عندما يجهز القرص أو جهاز التخزين الذي يحتوي على «تايلز»، أدخلوه في جهاز كمبيوتر ثم أعيدوا تشغيل الجهاز. يجب أن تروا شاشة الترحيب التي تسمح لكم برؤية المزيد من الخيارات وبتغيير اللغة.

إذا لم يقلع جهازكم انطلاقاً من نظام التشغيل «تايلز»، قد يتوجب عليكم تعديل إعدادات نظام الإدخال والإخراج الأساسي (BIOS). إذا عرض الكمبيوتر خيار يسمّى «Boot Options» عند تشغيله، قوموا بإدخاله واختاروا الإقلاع من محرك الأقراص (DVD Drive) أو جهاز الـ USB الذي قد يسمى «USB media» أو «Removable Drive». إن لم ينجح ذلك، أعيدوا تشغيل الكمبيوتر، وابحثوا عن رسالة تخبركم أي مفتاح تضغطون للدخول إلى إعدادات BIOS. وعادةً تكون واحدة من F1, F2, DEL, ESC أو F10. انقروا على هذا المفتاح أثناء إقلاع الكمبيوتر لتعديل إعدادات BIOS. يجب تعديل اعدادات «Boot Order» ووضع محرك الأقراص (DVD Drive) أو جهاز الـ USB على رأس القائمة. احفظوا التغييرات ثمّ أعيدوا تشغيل الكمبيوتر.

للمزيد من المعلومات حول الإقلاع من قرص DVD و جهاز الـUSB يمكن الاطّلاع على الروابط التالية:

- الإقلاع من قرص DVD: من الوثائق الرسمية لأوبونتو لينكس

الإقلاع من جهاز الـUSB: من الوثائق الرسمية لأوبونتو لينكس و من pcsupport.about.com

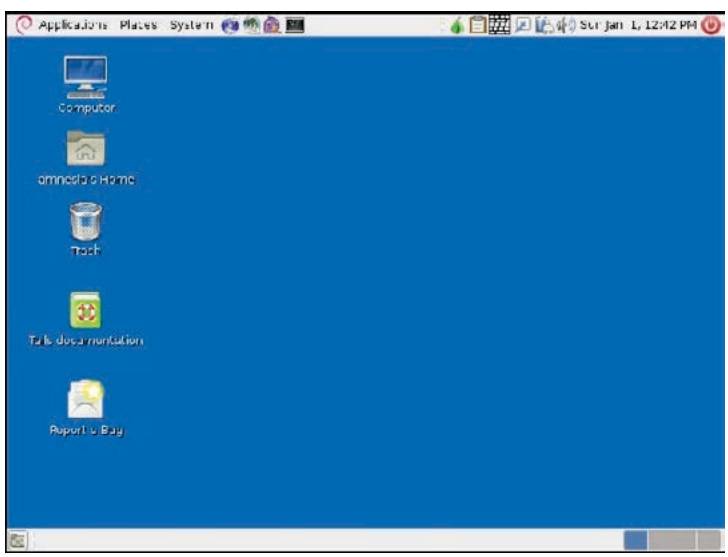
الدخول إلى إعدادات الـBIOS : من pendrivelinux.com

تأكدوا من الحصول على أحدث نسخة متوفرة من «تايلز» لكي لا يكون نظامكم عرضة للثغرات الأمنية المعروفة. يمكنكم الإشتراك في القائمة البريدية لـ«تايلز» هنا.

سطح المكتب:

عندما تشغّلون «تايلز»، سترون شاشة ترحيب تسألكم إن كنتم تريدون رؤية المزيد من الخيارات، وتسمح لكم بتغيير لغة نظام التّشغيل في أسفل الشّاشة. إن اخترتم عرض المزيد من الخيارات، ستتمكنون منّ تعيين كلمة سرّ خاصة بالإدارة، وستحتاجونها إن كنتم تريدون تنفيذ مهام إدارية كالوصول إلى الأقراص الصلبة الداخلية للحاسوب. عادة، تكون كلمة السر الخاصة بالإدارة معطّلة للحصول على أمنٍ أفضل. كما سيتم إعطاؤكم الخيار لتفعيل «التمويه كويندوز إكس بي» (Windows Camouflage) الذي يجعل «تايلز» يبدو مثل «ويندوز إكس بي» وهذا يفيد في تجنّب الإشتباه في الأماكن العامّة.

إن سجلتم الدخول مع الخيارات الاعتيادية سترَون سطح المكتب هذا، وينبغي أن يبدو مألوفاً بعض الشّيء لمستخدمي «ويندوز» و«ماك» (Mac).



الأيقونات الموجودة على سطح المكتب تؤمّن الوصول إلى:
– أجهزة التخزين المتصلة بالكمبيوتر (Computer)
– مجلد المنزل للمستخدم (Home Folder)
– وسيلة للتبليغ عن المشاكل أو الأخطاء التقنية في تيلز (Report bugs)
– وثائق «تايلز» الكاملة (Tails Documentation)
– المهملات (Trash)

تشمل اللوحة الموجودة في الأسفل طريقة مختصرة لتصغير جميع النوافذ المفتوحة واظهار سطح المكتب وتليها أزرار لفتح النوافذ، وعلى الجهة اليسرى، توفّر مجموعة من أربعة مستطيلات صغيرة الوصول إلى أربع مساحات عمل مختلفة (أو أسطح المكتب) يمكنها ان تحتوي نوافذ مفتوحة خاصة بها. ويمكن أيضاً تبديل مساحات العمل باستخدام الاختصار (Ctrl + Alt + مفتاح السهم). وتغيير عدد مساحات العمل بالنقر على هذه المستطيلات بزرّ الفأرة الأيمن واختيار «تفضيلات».

يحتوي شريط التنقل في الأعلى على ثلاثة قوائم على الجانب الأيسر (أو الأيمن إذا كنتم تستخدمون تيلز باللغة العربية):

– تحتوي قائمة «التطبيقات» (Applications) على اختصارات لتطبيقات مثبّتة تم تجميعها حسب الفئة.
– تحتوي قائمة «الأماكن» (Places) على اختصارات لملفّات وأجهزة تخزين ومواضع شبكة الاتّصال.
– تخوّلكم قائمة «النّظام» (System) من تعديل النّظام ومظهره.

بعض الخيارات المفيدة في قائمة «النظام» هي:

– ضبط لوحة المفاتيح
– ضبط الشاشة حيث يمكنكم تغيير ميزاتها
– التحكم بكلمات السر ومفاتيح التشفير حيث يمكنكم إدارة مفاتيح تطبيقOpenPGP.

يوجد على الجانب الأيمن من هذه القوائم الثلاث اختصارات لبعض التطبيقات المستخدمة بشكلٍ متكررٍ:

– IceWeasel هو متصفح مؤسس على فَيرفوكس.
– ClawsMail هو عميل بريد إلكتروني
– Pidgin هو برنامج دردشة فورية
– GNOME Terminal يخولكم إستخدام سطر الأوامر

أخيراً، توجد منطقة الإشعارات في الزاوية العليا اليمنى وتحتوي على أيقونات لبعض التطبيقات المشغلة وملامح النظام:

– Vidalia هو واجهة تحكم لـ«تور»
– gpgApplet يشفر ويفك تشفير لوحة القطع واللصق (clipboard) باستخدام OpenPGP
– Florence هو لوحة مفاتيح افتراضية
– مدير الشبكة يعالج إتصالات شبكتكم
– مدير الطاقة يظهر معلومات عن البطارية إن كنتم تستخدمون حاسوب نقّال
– متحكّم الصوت
– زرّ إعادة التّشغيل أو الإغلاق

بعض التّطبيقات المفيدة التي تأتي مع «تايلز» هي:

OpenOffice: هو مجموعة برامج مكتبية تشبه Microsoft Office
GIMP وInkscape: برنامج تحرير رسوميات
Scribus: برنامج تخطيط لتصميم منشورات للطّبع
Audacity: محرّر الصوت
– نظام الطّباعة CUPS وSimple Scan: لطباعة البيانات ومسحها ضوئياً

استعمال «تايلز» على الانترنت:

للاتصال بالإنترنت، إمّا اشبكوا كابل شبكتكم أو انقروا على مدير الشبكة (Network Manager) واختاروا شبكة

الـ Wifi. يفترض أن يعمل Vidalia تلقائيًا عند اتصالكم بشبكة ما. انتظروا حتى تصبح ايقونة Vidalia خضراء لتتأكدوا من اتصالكم بشبكة «تور» (Tor) وبعدها إنتظروا ليعمل المتصفح تلقائيًا. يمكنكم أيضًا تشغيل Vidalia ومتصفح IceWeasel يدويًا من خلال قائمة التطبيقات.

إن لم تتمكّنوا من الاتّصال بشبكة «تور» بعد الانتظار لوقتٍ طويل، قد يكون الوصول إلى «تور» محجوب من قبل مزوّد الانترنت أو أطراف أخرى. يكون الحل في هذه الحالة إستخدام «جسور تور» (Tor Bridges) وهي خوادم موزّعة غير مدرجة علناً. كل ما عليكم فعله هو زيارة bridges.torproject.org والنقر على «Getbridges» وبعدها إدخال الكلمات التي تظهر في الصورة ثمّ النقر على زر الادخال. إن لم تتمكنوا من الدّخول إلى تلك الصفحة يمكنكم أيضاً إرسال بريد إلكتروني إلى «bridges@bridges.torproject.org» من عنوان Gmail أو Yahoo تكتبون فيه هذا السّطر فقط «get bridges». عند تلقي اللائحة، افتحوا Vidalia وانقروا على «Settings» ثم «Network» واختاروا «مزودي بخدمة الانترنت يحجب الاتصال بشبكة تور». وبعد ذلك أضيفوا أسطر من اللّائحة واحد تلو الآخرة.

يمكنكم أن تجدوا المزيد من المعلومات عن «جسور تور» ومشاكل الاتصال هنا و هنا.

يمكنكم إستخدام التطبيقات المتعلقة بالإنترنت التي تأتي مع «تايلز» عندما تصبحون على إتصال كلي.

متصفح IceWeasel مبني على موزيلا فيرفوكس (Mozilla Firefox) مما يعني أنه يعمل بالطريقة ذاتها ويدعم إضافات فايرفوكس نفسها، وتم اعداده مسبقاً لإستخدام «تور» وبضع الإضافات التي تشمل:

- HTTPS Everywhere: يتأكد من أنكم تستعمل «https» بدلاً من «http» متى كان الأمر متاحاً.
- TorButton: يعنى ببضعة أشياء متعلقة بالأمن والخصوصية في فيرفوكس على مستوى التطبيقات.
- NoScript: يُعطي المستخدم الخيار لتعطيل Javascript على مواقع الانترنت. تم تعطيل هذا الخيار بشكل افتراضي لأنه يمنع العديد من المواقع من الظهور بشكل صحيح.

Pidgin هو برنامج للرسائل الفورية. لدى استعماله مع «تايلز»، يتيح هذا البرنامج الدردشة على الخدمات التي تستخدم IRC أو XMPP. عند تشغيل Pidgin، يتم وصلكم تلقائياً مع اسم مستخدم عشوائي بـ irc.oftc.net حيث يمكنكم العثور على قنوات الدردشة الرسمية لـ«تايلز» و«تور» (#tails و #tor). إن بعض الحسابات الأخرى مشمولة إفتراضياً ويمكنكم تفعيلها أو إضافة حسابكم الخاص بالنقر على «Accounts» ثم «Manage Accounts».

يدعم Pidgin برتوكول OTR مما يعني أنه يمكنكم التراسل من دون تسجيل أو حفظ الرسائل. يؤمن OTR التشفير والتصديق والإنكار وسريّة أماميّة مثاليّة.

يمكنكم أن تجدوا تعليمات حول استعمال OTR في هذا الفيديو وهذه المقالة. يمكنكم أيضاً معرفة المزيد عن OTR هنا.

ويسمح لكم «تايلز» بإستخدام I2P وهي شبكة تخفٍ مغلقة وتكون عموماً منفصلة عن شبكة الإنترنت العادية. تنتهي مواقع I2P بلاحقة «i2p.» ويمكنكم الوصول إليها فقط إن كنتم متصلين بشبكة الـ«I2P». بإمكانكم الاتصال بهذه الشبكة من قائمة «Applications» ثم «Internet» وبعدها الضغط على «I2P». ستفتح صفحة محلية اسمها «I2P Router Console» في IceWeasel وعاجلاً ما تصلكم بشبكة «I2P». يمكنكم إختبار الإتصال بزيارة موقع i2p. مثل www.i2p2.i2p (احرصوا على تحديد «www»).

للمزيد من المعلومات عن I2P زوروا www.i2p2.de .

يستخدم «تايلز» الجدار الناري لنواة لينوكس ليمنع التطبيقات من الاتصال المباشر بشبكة الانترنت إلا إذا عبَر من خلال «تور». لكن يأتي «تايلز» مع متصفح غير آمن «Unsafe Web Browser» موجود في قائمة «التطبيقات» تحت فئة «Internet». يُسمح لهذا المتصفح غير الآمن بالإتصال مباشرةً بالإنترنت دون العبور من خلال «تور» وهو لا يقدم أي حماية من حيث التخفي أو حماية الخصوصية إطلاقاً. قد يكون هذا المتصفح ضرورياً في حالات تتطلّب منكم الوصول إلى صفحة دخول ما، قبل الوصول إلى الانترنت، مثلاً في مقاهي الانترنت، مكتبات، مطارات، فنادق، جامعات...

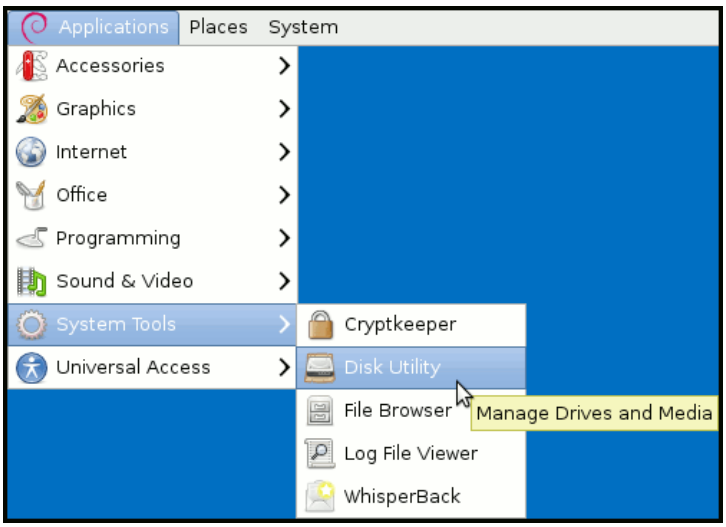
في هذه الحالات، لا تستخدموا إلا المتصفح غير الآمن لتنفيذ الدخول الأولي، بعدها أغلقوا المتصفّح واستخدموا تطبيقات أخرى مثل متصفّح IceWeasel. عدا عن ذلك، لا يجدر بكم إستخدام المتصفح غير الآمن في الحالات العاديّة.

إستخدام ملامح الخصوصيّة والتشفير في «تايلز»:

يأتي «تايلز» مع بضع الأدوات للخصوصية والأمن والتشفير التي تحميكم في حالات عديدة.

مسجلات ضربات المفاتيح أو «Keyloggers» هي برمجيات أو أجهزة تسجّل كل مفتاح يُضغط على لوحة مفاتيح الحاسوب. يمكن لمسجل ضربات المفاتيح أن يكون مثبتاً فعلياً من قبل مهاجمين على الحواسيب العامة أو حاسوبكم الخاص، ومن المعروف أن ذلك يحدث.

ولحمايتكم من مسجّل ضربات المفاتيح، يأتي «تايلز» مع لوحة مفاتيح افتراضية اسمها «Florence». تسمح لكم هذه اللوحة بإدخال معلومات حساسة كأسماء المستخدمين وكلمات السر باستخدام الفأرة من أجل التقليل من مخاطر سرقة هذه المعلومات. استخدموا لوحة مفاتيح «Florence» كلّما تشكّون في الجهاز الذي تستخدمونه، وخاصةً في مقاهي الإنترنت.
إذا ضاع أو سُرق جهاز مثل جهاز تخزين USB يحتوي على معلومات خاصة أو حساسة، يمكن أن تصبح هذه المعلومات متوفرة لكل من يجد الجهاز.



من أجل حماية معلوماتكم الحساسة، يسمح لكم «تايلز» بإنشاء أقسام مشفرة من القرص بإستخدام معيار تشفير LUKS. لإنشاء قسم مشفر، اذهبوا إلى «تطبيقات» (Applications) ثم «أدوات النظام» (System Tools)، وبعدها «Disk Utility». سترون لائحة بأجهزة التخزين الموجودة. عندها، إشبكوا جهاز التخزين الذي تريدون إستخدامه وسيظهر على اللائحة. انقروا على جهاز التخزين وتحققوا من أن إسم النموذج والسعة يتوافقان مع جهاز التخزين الخاص بكم، ثم انقروا على «Format Drive» واختاروا «Format» في النوافذ التي تظهر. إعلموا أن هذا سيمسح جميع المعلومات عن الجهاز.

الآن يجب أن يكون جهازكم فارغاً. انقروا على «Create Partition» واختاروا حجم المساحة ونوع نظام الملفات وإسماً للقسم الجديد. مثلاً، يمكنكم ضبط الحجم إلى الحدّ الأقصى لإستخدام الجهاز بأكمله أو ترك مساحة لإنشاء قسم عادي في ما بعد. اختاروا Ext4 كنوع نظام الملفات إن كنتم فقط تريدون أن

تكونوا قادرين على إستخدام القسم المشفر على «تايلز» أو أنظمة لينوكس أخرى لديها أدوات LUKS. في المقابل، اختاروا FAT إن كنتم تريدون استخدام جهاز التخزين على أنظمة تشغيل أخرى لديها أدوات تتلاءم مع LUKS، مثلاً أداة «FreeOTFE» الخاصة بـ«ويندوز».

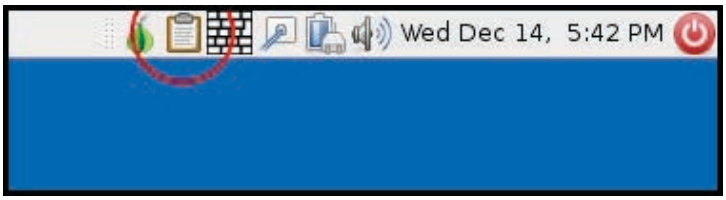
حددوا إسماً للقسم الخاص بكم وسيظهر فقط أثناء الاستخدام من بعد فك التشفير عن الجهاز. أخيراً، قوموا بتحديد الخانات التالية «Take Ownership of filesystem» و«Encrypt Underlying device» وانقروا «Create».

سيطلب منكم إدخال عبارة مرور/كلمة سر للقسم الجديد. اختاروا عبارة مرور وأدخلوها في كلا المربعين وانقروا «Create». الآن، سيتم إنشاء القسم المشفر الجديد.

بعد أن يتم ذلك، سيُسمح لكم بإنشاء قسم عادي في المساحة المتبقية على جهاز التخزين إذا اردتم.
لإظهار الكيفية التي يعمل بها القسم المشفر، إفصلوا جهاز التخزين واشبكوه مرةً أخرى. سيظهر في قائمة الأماكن (Places).

إن قمتم بالنقر عليه وأدخلتم عبارة مرور خاطئة سيبقى مقفلاً. حالما تدخلون عبارة الدخول الصحيحة، سيفتح القسم وسيسمح لكم باستخدامه كأنه جهاز تخزين عادي. عند الإنتهاء، انقروا على «الأماكن» (Places) وبعدها «الحاسوب» (Computer) وانقروا بزر الفأرة الأيمن واختاروا «Safely Remove».

يمكن للنّصوص غير المشفرة التي تُرسل عبر الإنترنت أن تُخترق و تُقرأ. لتشفير النصوص، يأتي مع «تايلز» تطبيق «Tails gpgApplet» الذي يعطيكم خيار التشفير باستخدام كلمة سر أو مفاتيح PGP.
للإستفادة منه، افتحوا محرر نصوص مستقل واكتبوا نصكم داخله. لا تكتبوا نصاً سرياً داخل المتصفح لأنه عرضة لهجمات Javascript. إذا نقرتم على قائمة «التطبيقات» (Applications) وبعدها على «ملحقات» (Accessories) ستجدون محرر النصوص «gedit». اكتبوا نصاً داخله ثمّ حددوا النص وانسخوه بإستخدام الإختصار «Ctrl+C» أو بالضغط عليه بزرّ الفأرة الأيمن واختيار «إنسخ» (Copy). بعد ذلك، انقروا على gpgApplet واختاروا وسيلة للتشفير.

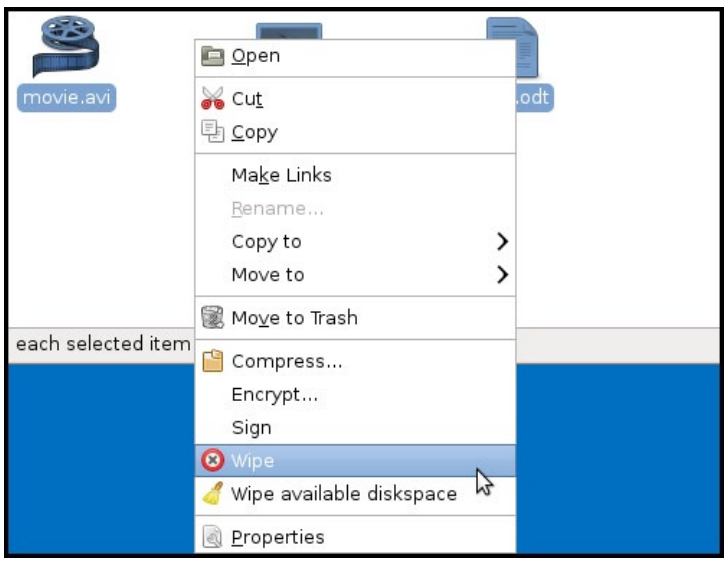


إن اخترتم التشفير بإستخدام كلمة سر (Passphrase) سيسألكم gpgApplet أن تدخلوا العبارة وبعدها أن تؤكدوا الإدخال. وستظهر الآن أيقونة gpgApplet قفلاً مما يعني أنه أصبح بإمكانكم لصق النص المشفر بإستخدام الإختصار Ctrl+V أو بالنقر على زر الفأرة الأيمن وإختيار «لصق» (Paste).

مثلاً بإمكانكم الآن لصق النص المشفر في المتصفح لإرساله ببريد إلكتروني. وليس بإمكان أي أحد فك التشفير وقراءة النص إلا أولئك الذين يعرفون عبارة المرور. اننا ننصحكم بمشاركة عبارة المرور هذه مع المرسل اليهم شخصياً.

على سبيل المثال، بإمكانكم تشفير نصاً منسوخاً بإستخدام المفاتيح الـ PGP التي تخص المرسل اليه (ومفتاحكم الخاص إن كنتم تريدون توقيع رسائلكم أو فك التشفير من الرسائل التي ارسلت اليكم) بالضغط على gpgApplet وتحديد «Manage Keys». حالما تضيفون جميع المفاتيح الضرورية، انقروا على gpgApplet واختاروا التشفير بالمفاتيح العامة (Public Keys). بعدها، حددوا مرسل إليه أو أكثر واختاروا إن كتنتم تريدون إخفاء المرسل اليهم بمفتاحكم الخاص أم لا، ثم انقروا على «OK». قد يظهر إطار منبثق يسألكم إذا كنتم تثقون بالمفتاح، أجيبوا على السؤال. بإمكانكم الآن لصق هذا النص بالطريقة ذاتها في رسالة بريد إلكتروني. لا يمكن لأحد أن يقرأ النص إلا المرسل اليهم الذين استخدمتم مفاتيحهم العامة.
عندما تقومون بمسح ملف ما، لا تُمسح المحتويات الفعلية لهذا الملف حتى بعد إفراغ المهملات.

عوضاً عن ذلك، يزيل نظام التشغيل الوصول المباشر إلى الملف. تبقى البيانات الفعلية على وسائط التخزين إلى أن يستخدم نظام التشغيل المساحة لبيانات جديدة. وهذا يعني أنه غالباً ما يمكن استعادة الملفات الممسوحة.



لمسح الملفات بشكلٍ آمن، يمكنكم أن تستعملوا إضافة «Nautilus Wipe» وهي إضافة لمدير ملف الـ Nautilus تأتي مع «تايلز». يقوم «Nautilus Wipe» بالكتابة فوق البيانات الممسوحة ليمنع استعادتها.

لاستخدامه، حددوا الملفات التي تريدون ازالتها وأنقروا عليها بزر الفأرة الأيمن وحددوا «Wipe» أو «المسح».

قد يستغرق الأمر بضع ثوانٍ أو دقائق بينما يتم مسح الملفات والكتابة فوقها. بالإضافة إلى ذلك، تسمح لكم إضافة «Nautilus wipe» بتنظيف كل المساحة الخالية على القرص لمنع عمليات إستعادة الملفات التي تم محوها مسبقاً.

كل ما عليكم فعله هو الدخول إلى الملف الموجود على ذلك القرص والنقر بزر الفأرة الأيمن وتحديد «Wipe available diskspace» أو «مسح مساحة القرص الموجودة».

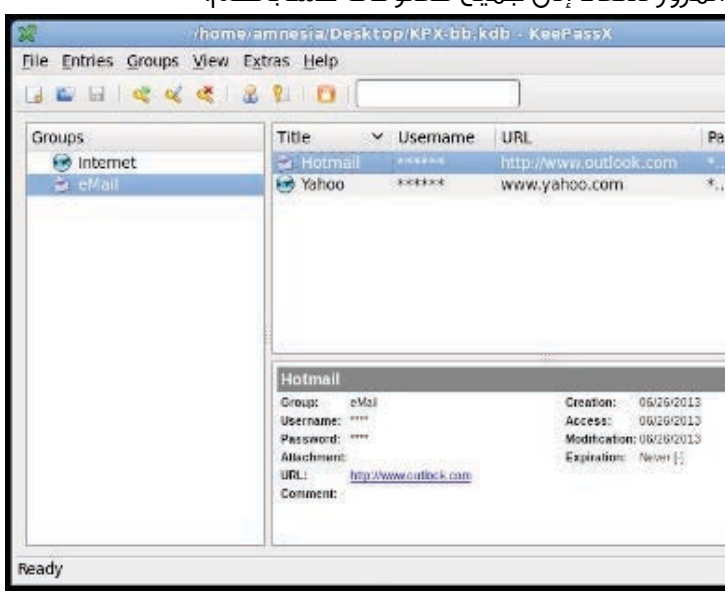
لن يمسح ذلك البيانات الموجودة على القرص ويمكن أن تأخذ العملية بضع دقائق أو ساعات لتتم. لاحظوا أن وسيلة الأمن هذه لمسح الملفات تعمل بشكلٍ أفضل على الأقراص الصلبة التقليدية.

ولكن عندما يتعلق الأمر بجهاز تخزين USB أو أقراص جامدة (Solid–state drives)، لن تكون هذه الوسيلة بالفعالية نفسها، فلذلك من الضرورة إجراء تشفير كلّي لأجهزة كهذه بهدف منع قراءة أي نوع من البيانات.

تكون كلمات السر القوية طويلة وتحتوي على أنواع مختلفة من الأحرف، ولا تكون كلمات معجمية ولا تُستخدم في أماكن عديدة. قد يصعب تذكر عدد كبير من كلمات السر هذه.

يوجد في «تايلز» KeePassX لإدارة كلمات السر.

KeePassX هو مدير لكلمات السر يسمح لكم بتخزين جميع تفاصيل حساباتكم في قاعدة بيانات تكون محمية بعبارة مرور واحدة. باستخدام KeePassX، لا يكون عليكم سوى حفظ عبارة المرور للنفاذ إلى جميع معلومات حساباتكم.



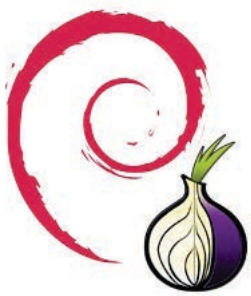
للوصول إلى KeePassX، انقروا على «التطبيقات» أو «Applications» ثم على «الملحقات» (Accessories) وانقروا على KeePassX.

لإنشاء قاعدة بيانات جديدة لكلمة سر ما، انقروا على «File» وبعدها على «New Database».

ادخلوا عبارة المرور التي سيتم استخدامها لتشفير قاعدة البيانات هذه وانقروا على «OK».
الآن، انقروا على «File» وعلى «Save Database» وبعدها اختاروا مكان لحفظ القاعدة، مثل جهاز تخزين خارجي.
يمكنكم أيضاً رفع قاعدة البيانات على الإنترنت من أجل الوصول إليها في المستقبل بما أنها مشفرة ولايمكن فتحها سوى باستخدام عبارة المرور.
من السهل إستخدام KeePassX، يمكنكم إنشاء مجموعات وإضافة ادخالات ضمن هذه المجموعات لحسابات مختلفة. يمكنكم إستخدام مولد كلمات السر (Password Generator) في KeePassX لتوليد كلمات سر قوية جداً.
عندما تحتاجون إلى معلومات حساباتكم في وقتٍ لاحق، شغلوا KeePassX، وافتحوا قاعدة بيانات كلمة السر وقوموا بفك التشفير عنها بعبارة المرور، ثم، انسخوا إسم المستخدم وكلمة السر اللذين تحتاجون اليهما.
بإمكانكم أيضاً إستخدام ميزة «Autotype» لجعل KeePassX يُدخّل كلمة سرّكم آلياً.

استفيدوا من هذه الأدوات عند استخدام «تايلز» من أجل تحسين أمنكم وحماية خصوصيتكم.

الخاتمة:



وهكذا نكون قد قمنا بتغطية أهم ميزات «تايلز» وقمنا بشرح كيفية التنزيل، والتثبيت، والتشغيل، واستخدام نظام تشغيل «تايلز» بشكلٍ فعال لتحسين خصوصيتكم والحفاظ على أمنكم على الانترنت وعلى أجهزة حاسوب غير موثوقة.
يمكنكم العثور على المزيد من المعلومات عن «تايلز» و«تور» على موقعيهما:
موقع «تايلز»
موقع «تور»

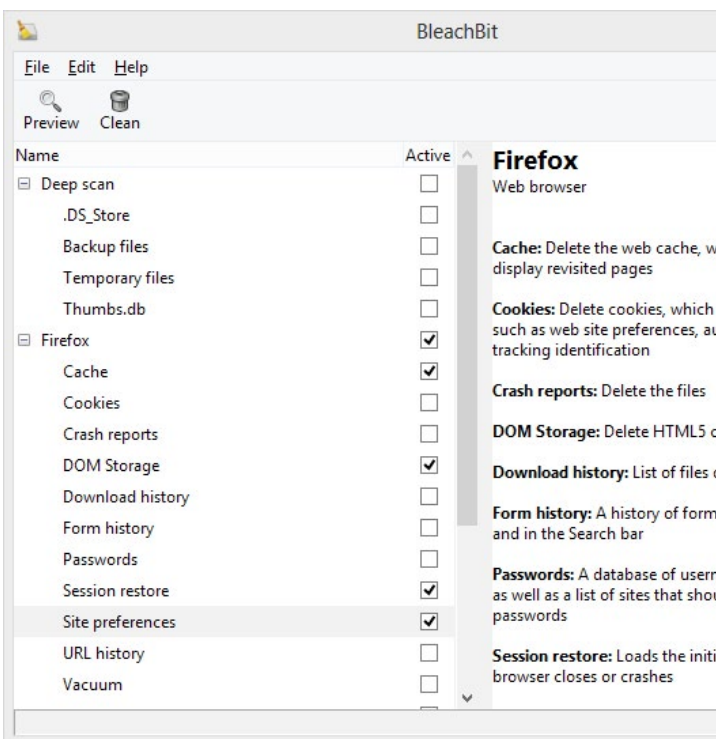
بإمكانكم مشاهدة الفيديوهات التالية لشرح أكثر عن طريقة استعمال تيلز

BleachBit «بليتشبت» لحذف الملفات

BleachBit («بليتشبت») برنامج مفتوح المصدر يقوم بإزالة الملفات الغير الضرورية من أنظمة تشغيل Windows وLinux، كالملفات المؤقتة وتاريخ التصفح على الويب وغيرها من مخلفات تتركها البرامج على حاسوبكم بالإضافة إلى إزالة الملفات بشكل آمن ونهائي.

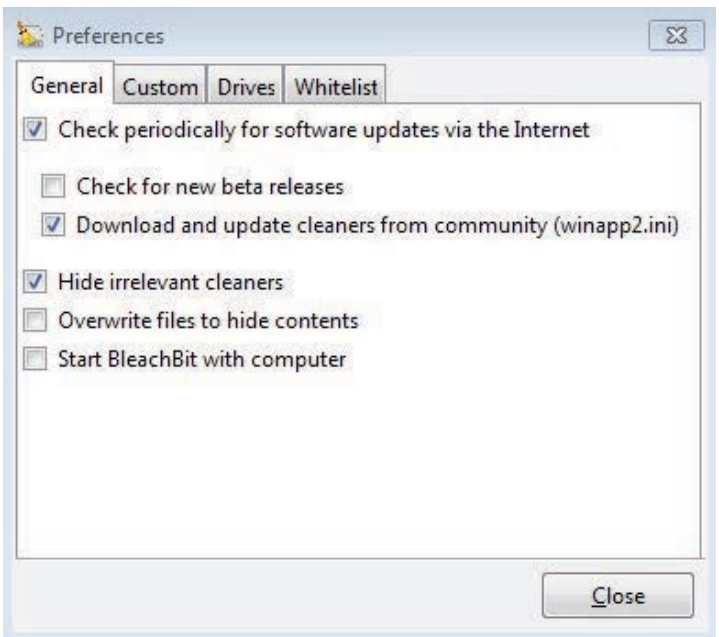
بذلك، يمكن القول أن BleachBit شبيه بمزيج من CCleaner وEraser، لكنه يمسح عدداً أكبر من الملفات مقارنةً بـ CCleaner، وكيفية حذف البيانات نهائياً أبسط من تلك التي في Eraser.

ولقد ازدادت شعبية BleachBit مؤخراً بعد ذكر أحد الشخصيات الشهيرة في عالم الأمن الرقمي بروس شناير أنه يستخدم BleachBit (بالإضافة إلى GPG، OTR، TrueCrypt، Tails، وغيرها) عندما يتعامل مع ملفات حساسة.



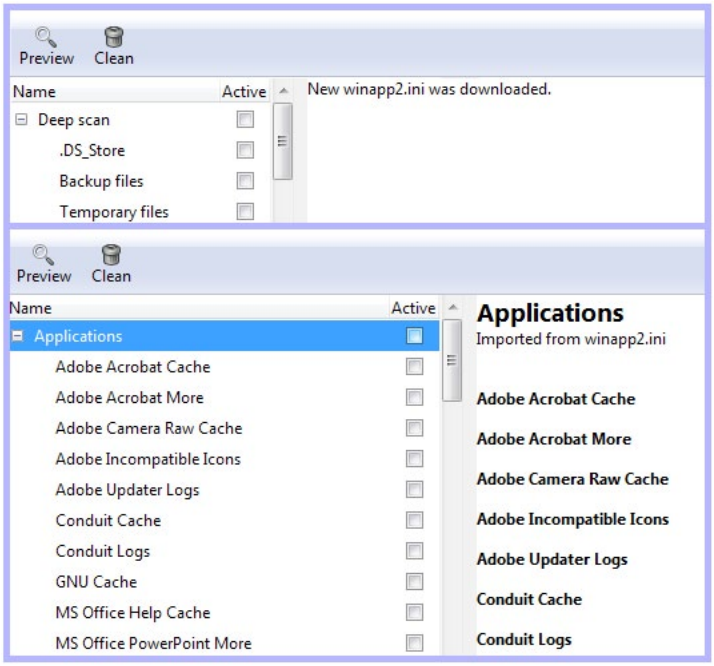
BleachBit سهل الإستخدام، فمظهره بسيط وليس لديه إعدادات كثيرة. لتجربته، قوموا بتنزيله من موقعه الرسمي وتثبيته. عندما تقومون بتشغيله، ترون على اليسار لائحة لأنواع الملفات التي يستطيع BleachBit أن يزيلها، وعند النقر على احدها، يعرض BleachBit معلومات عنها.

بعد إختياركم من تلك اللائحة، يمكنكم عرض الملفات التي سيقوم BleachBit بحذفها، دون حذفها فعلاً، بواسطة النقر على «Preview». وبعد المراجعة، يمكنكم المباشرة بالإزالة بالنقر على «Clean».

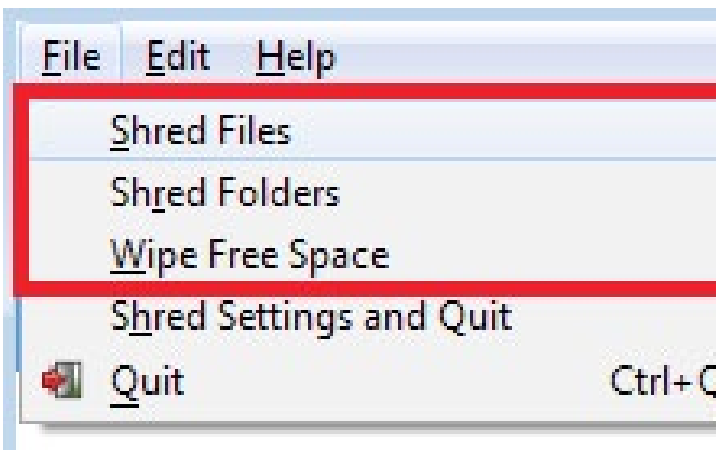


بعض الإعدادات المفيدة في BleachBit موجودة في Edit > Preferences، تحت صفحة «General»، وهي:

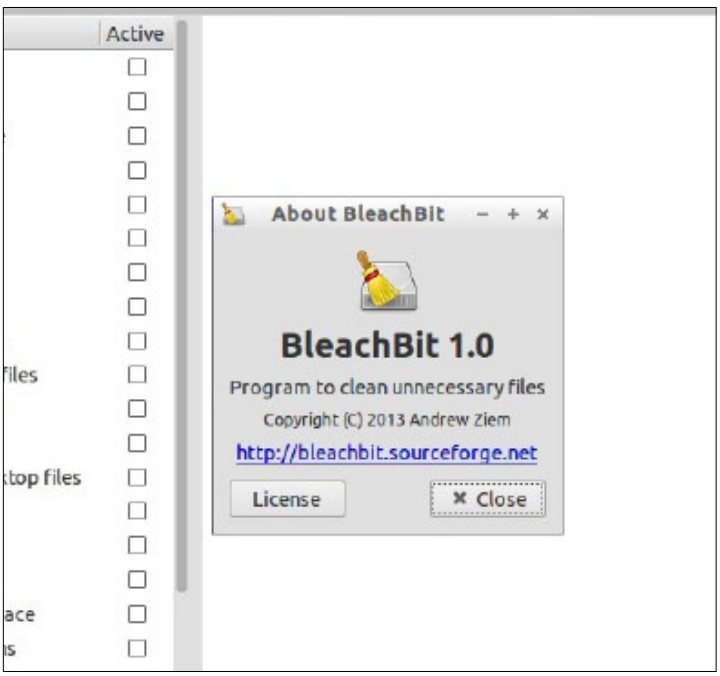
– «Download and update cleaners from community» يخولكم الإستفادة من أكثر من 1200 منظف إضافي من تقديم مجتمع مستخدمي BleachBit.



بعد إختيار تلك الإعدادات، أعيدوا تشغيل BleachBit كي يقوم بتنزيل ملف «winapp2.ini» تحضيراً لتنزيل المنظفات الإضافية، ثم قوموا بإعادة تشغيله ثانيةً كي يقوم بتنزيل المنظفات.



أخيراً، يمكنكم الوصول إلى وسيلة حذف البيانات نهائياً بالنقر على «File» والاختيار بين «Shred Files» لحذف الملفات أو «Shred Folders» لحذف مجلدات بكاملها أو «Wipe Free Space» لحذف بيانات محذوفة مسبقاً عن جهاز التخزين بشكل نهائي، ولكن الرجاء الانتباه إلى أنّ استخدام «Shred» لحذف ملفات «مايكروسوفت أوفيس» لن يغنيكم عن تشغيل خيار «Wipe Free Space» لاحقاً وذلك لأن «مايكروسوفت أوفيس» يترك نسخاً مخبأة من الملفات على الأقراص.



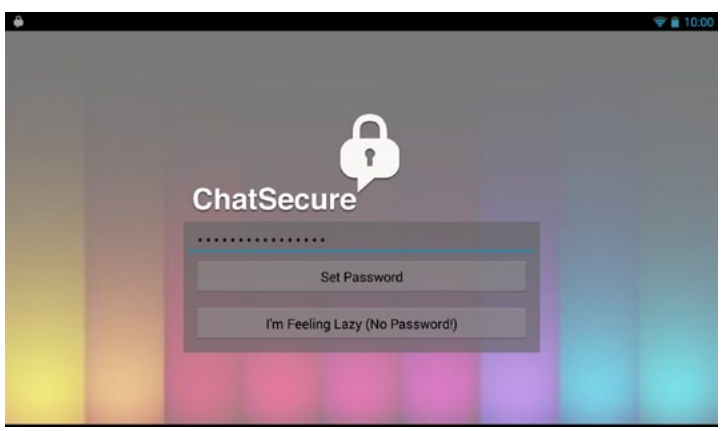
(يرجى الملاحظة أن حذف الملفات بشكل نهائي، أياً كانت الوسيلة المستخدمة، لا يعمل بشكل صحيح إلا على الأقراص الصلبة التقليدية (HDD) وليس على أجهزة USB Flash أو SSD)

«تشات سيكيور» ChatSecure
تطبيق للدردشة الآمنة

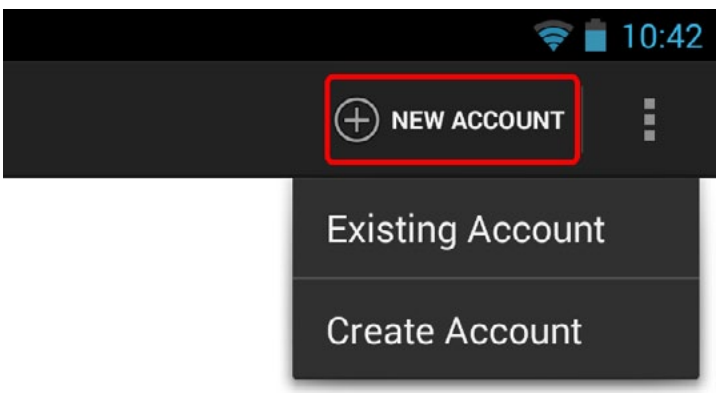
ChatSecure هو تطبيق تراسل فوري مجاني ومفتوح المصدر، يدعم تشفير OTR ويتيح لكم إدارة حساباتكم المختلفة عبر واجهة استخدام موحّدة. يعمل ChatSecure مع جميع خدمات الدردشة التي تستخدم بروتوكول XMPP، ما يعني أنه يعمل مع Facebook Chat و GoogleTalk/Hangouts وJabber وDukgo.com والعديد غيرها، كما أنه يمنحكم فرصة إنشاء حسابات XMPP جديدة مباشرةً داخل التطبيق. بالإضافة إلى ذلك، يعمل ChatSecure على Android وiOS ويمكنكم أيضاً من التواصل مع متصلين يستخدمون أنظمة التشغيل Windows أو Mac أو Linux من خلال برنامج تواصل ملائم مثل Jitsi.

سوف نشرح في هذا المقال عن تطبيق ChatSecure لنظام «أندرويد»، الذي يطوره «The Guardian Project» والذي يختلف مظهره عن ذلك الذي يعمل على iOS (إذا كان عندكم اسئلة عن ChatSecure على iOS، يمكنم طرحها على صفحتنا على فيس بوك).

يمكنكم تنزيل ChatSecure على أندرويد من خلال Google Play أو هذا الرابط.



في أول مرة تشغلون ChatSecure، يطلب منكم التطبيق وضع كلمة مرور اختيارية، تمنع الدخول إلى التطبيق في حال خرجتم منه بواسطة إختيار «Exit» من قائمته.



بعد ذلك يمكنكم البدء بإضافة حساباتكم. إذا لم يكن لديكم حساب Jabber/XMPP مسبقاً، يمكنكم إنشاء حساب جديد من خلال التطبيق بإختيار «New Account» ثم «Create Account».

هنا تختارون إسم مستخدم جديد، ومزود خدمة. مثلاً إذا اخترتم إسم مستخدم «user123» والمزود «dukgo.com»، يصبح حسابكم «user123@dukgo.com».

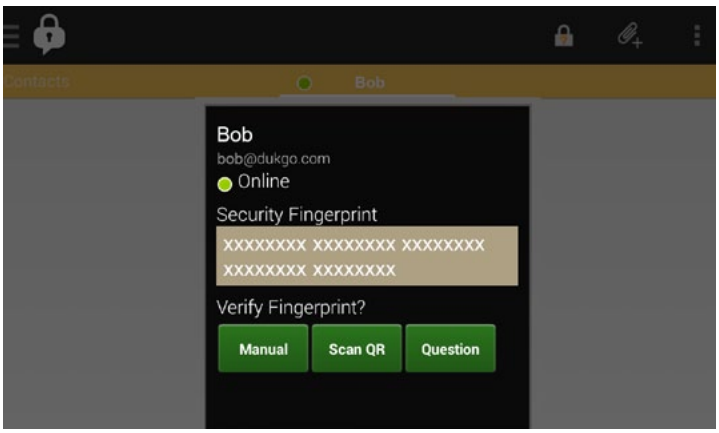
بالطبع يمكنكم إستخدام حساب «Google» أيضاً من خلال إختياركم «Existing Account»،

لكن قد تريدون توقيف تطبيق «Google Hangouts» على جهازكم كي لا يبلغكم عن الرسائل نفسها التي تصلكم على ChatSecure (ففي حال بدأتم بإستخدام التشفير داخل ChatSecure، ستصل تلك الرسائل إلى Google Hangouts بشكلها المشفر).

بعد إضافة الحساب، يعرض ChatSecure جهات الإتصال الخاصة بكم في حال قمتم بإضافتها مسبقاً. يمكنكم إضافة جهات إتصال جديدة من خلال الضغط على الأيقونة في أعلى اليسار وإختيار «Add Contact» وإدخال إسم حسابهم.

لبدء المحادثة، اختاروا جهة إتصال ليعرض ChatSecure شاشة دردشة. إذا كان الطرف الآخر يستخدم برنامج ملائم مع تشفير OTR، يمكنكم تشغيل التشفير من خلال الضغط على أيقونة القفل المفتوح في أعلى الشاشة وإختيار «Start Encryption».
قد يتطلب الأمر المحاولة أكثر من مرة واحدة أو القول للطرف الآخر أن يشغل التشفير في حال لم تنجحوا بعد عدة محاولات.

يشير تغير صورة الأيقونة إلى قفل مغلق إلى نجاح التشفير، لكن لاحظوا إشارة الاستفهام عليها واللون الأصفر على الشريط الموجود تحتها، فذلك يعني أن بالرغم من وجود التشفير، لم يجرِ التأكد من هوية الطرف الآخر، أي انكم لم تتأكدوا انكم لستم تتعرضون لهجوم «Man-In-The-Middle» أو «رجل في الوسط»، حيث يقوم المهاجم بتلقي معلومات من الطرفين وإيهام كل طرف بأنه الطرف الآخر. للتأكد من هوية الطرف الآخر، اضغطوا على أيقونة القفل واختاروا «Verify» ثم وسيلة للتأكد.



الخيار «Manual» يتيح لكم التأكد من صحة رمز البصمة للطرف الآخر، وذلك من خلال تبادل رموز البصمات من خلال وسيلة إتصال أخرى. الرمز الموجود تحت جملة «Fingerprint for you» هو رمز بصمتكم الخاصة التي يجب أن ترسلوها للطرف الآخر.

والرمز الموجود في أسفلها تحت جملة «Fingerprint for xxx*xxx» هو رمز البصمة للطرف الأخر والذي يجب أن يطابق ما أرسله لكم ذلك الطرف. بعد التأكد من صحة رمز البصمة العائدة لذلك الطرف، يمكنكم إختيار «OK» والعودة إلى شاشة الدردشة.

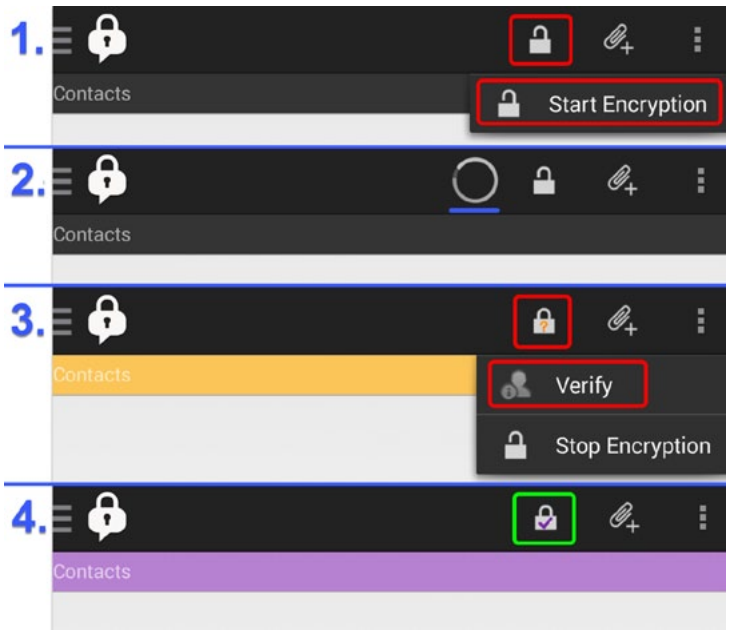
أما الخيار «Scan QR»، فيمكنكم من استخدام كاميرا جهازكم للقيام بمسح ضوئي لصورة QR (الشبيهة بالباركود) التي تحتوي على رمز بصمة الطرف الآخر. يطلب هذا الخيار تثبيت تطبيق «Barcode Scanner» من خلال Google Play أو هذا الرابط.

يطلب هذا الخيار تثبيت تطبيق «Bacode Scanner» من خلال Google Play أو هذا الرابط.

لإرسال صورة QR لرمز بصمتكم الخاصة، عودوا إلى نافذة الدردشة وإضغطوا على أيقونة ChatSecure في أعلى اليسار وإختاروا «Fingerprint»، ثم اختاروا «Share» من

أعلى اليسار لإرسال الصورة من خلال وسيلة إتصال مختلفة عن ChatSecure. عند تلقيكم صورة الـ QR من الطرف الآخر، إضغطوا مجدداً على الشريط الأصفر واختاروا «Scan QR» ووجهوا كاميرا جهازكم نحو شاشة الجهاز الذي يعرض الصورة.

أخيراً، يمكنكم الخيار «Question» من إدخال سؤال والإجابة المتوقعة له للتأكد من هوية جهة الإتصال.



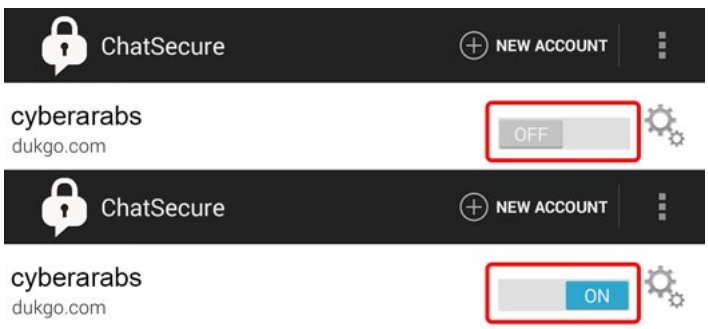
والآن، بعد التأكد من هوية جهة الإتصال، يجب أن تصبح صورة أيقونة القفل صورة قفل مغلق عليه إشارة «صح»، وأن يزول اللون الأصفر عن الشريط الموجود تحتها، ما يعني أن المحادثة أصبحت مشفرة وآمنة.

أخيراً، يجدر ذكر الخيار «Panic». إذا ضغطتم على أيقونة ChatSecure في أعلى اليسار، ستجدونه في أسفل القائمة، وعند اختياره، سيسألكم ChatSecure إن كنتم تريدون إزالة التطبيق فوراً.

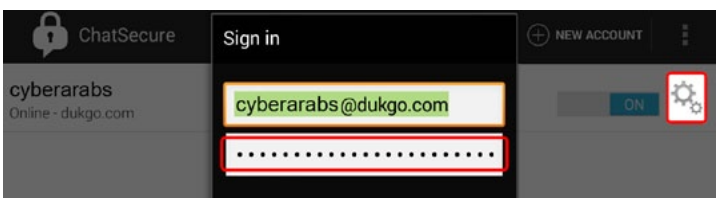
وهكذا يمكنكم إستخدام ChatSecure للقيام بمحادثات آمنة مع جهات الإتصال الخاصة بكم. نرجو الملاحظة، أن ChatSecure كان قيد التطوير وقت كتابة هذا المقال، ولا زال يحتوي على العديد من العلل. إذا واجهتم أية مشاكل في استخدامه، لا تترددوا في سؤالنا عنهم على صفحتنا في فيس بوك.
وما يلي بعض المشاكل التي قد تواجهونها عند استخدام التطبيق وطريقة التعامل معها:

خروج التطبيق فور الدخول إليه حتى بعد عدة محاولات:
قوموا بإزالة ChatSecure وإعادة تثبيته

عدم ظهور دعوات جهات إتصال جديدة:
أعيدوا تسجيل الدخول إلى حسابكم



فشل تسجيل الدخول:
تأكدوا من كلمة السر للحساب عبر الضغط على أيقونة إعدادات الحساب



فشل تسجيل الدخول بعد تسجيل الحساب من التطبيق:
في حال فشل تسجيل الدخول إلى حسابكم بعد التسجيل في أحد مزودات الخدمة، قوموا بتسجيل الحساب عبر موقع الخدمة (dukgo.com مثلاً)

تعطيل حساب فيس بوك

النتيجة: حساب فيس بوك معلق ولا يمكن الوصول إليه

قبل الحالة الطارئة:

ضرورة مشاركة بيانات تسجيل الدخول مع شخص موثوق به أو إضافة عنوان بريد إلكتروني إضافي (هنا). في حالة الاعتقال، حيث لا يمكنكم الوصول إلى الإنترنت، سيقوم الشخص الموثوق به بتسجيل الدخول إلى حسابكم (باستخدام اسم المستخدم وكلمة المرور الخاصين بكم أو إعادة تعيين كلمة المرور باستخدام البريد الإلكتروني البديل) والقيام بالإجراءات التالية عنكم. أجروا ترتيبات واضحة مع الشخص الموثوق به عن وقت التصرف (مثلا عندما لا تعودون بعد الساعة العاشرة). يمكنكم التراجع عن التعطيل عن طريق تسجيل الدخول باستخدام بيانات اعتماد جديدة.

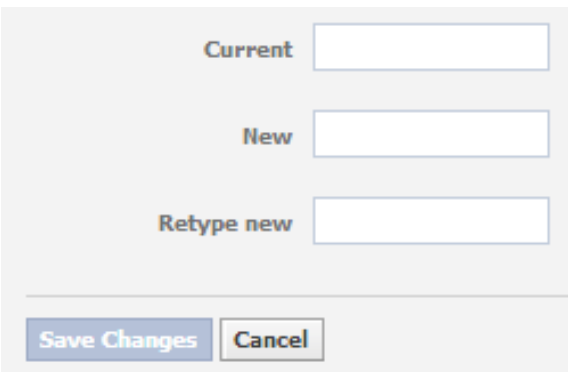
الخطوة ١:

تسجيل الدخول و تغيير كلمة المرور

١- تسجيل الدخول إلى حساب فيس بوك مثلما تفعلون عادة.

٢- النقر على رمز الدولاب الموجود في اليمين الأعلى والذهاب إلى: إعدادات الحساب› عام › كلمة المرور ، أو ببساطة النقر هنا.

٣- كتابة كلمة المرور، كلمة المرور الجديدة، و كلمة المرور الجديدة مرة أخرى.



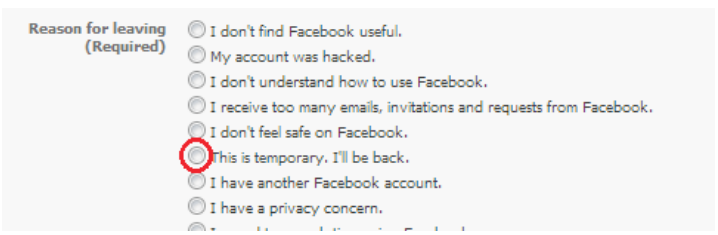
٤- النقر على «حفظ التغييرات»

الخطوة ٢ :

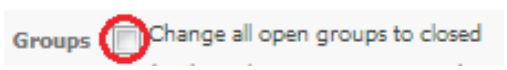
تعطيل حساب فيس بوك

١- النقر على رمز الدولاب أعلى اليمين والذهاب إلى: إعدادات الحساب› الأمن › إلغاء تنشيط الحساب (في أسفل الصفحة)، أو ببساطة النقر هنا.

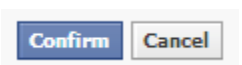
٢. إختيار « هذا هو مؤقت. سأعود » من القائمة.



٣- إذا كان لديك مجموعات، إختر «تغيير كل المجموعات مفتوحة إلى مغلقة»



٤- النقر على تأكيد.



٥- كتابة كلمة السر الخاصة بكم والنقر على «إلغاء التنشيط الآن»

٦- في بعض الأحيان سوف يطلب منكم نسخ نوع من التسلسل الإلكتروني العشوائي. افعلوا ذلك وانقر على «إرسال».

٧- تم تسجيل الخروج وتم إيقاف حسابكم

فقدان الهاتف المحمول

النتيجة بعد التطبيق: سوف يحظر وصول أطراف ثالثة (اللصوص والشرطة و الأجهزة الأمنية) إلى بياناتكم وحساباتكم على الانترنت

قبل فقدان الهاتف المحمول:

اعلموا أن على الرغم من كون الهواتف المحمولة أجهزة عملية فإن وقوعها في أيدي أفراد سيئي النية خطر جداً. تجنبوا أخذ هاتف يحتوي على بيانات حساسة إلى مناسبات قد يكون خطر الاعتقال أو الخسارة ممكن. وعلاوة على ذلك، إطلعوا على مخاطر الهواتف المحمولة والاخطاء الشائعة عند استخدام الهاتف المحمول، وقوموا بتشفير هاتفكم، وتثبيت برمجية للحفاظ على أمن الأجهزة المحمولة مثل سوفوس أو اعدوا مدير جهاز الأندرويد Android Device Manager للقفل والمسح عن بعد(شرح).

شاركوا كلمة سر «الرسالة النصية» لـ«سوفوس» مع شخص موثوق به واجروا ترتيبات واضحة معه عن وقت التصرف (مثلاً عندما لا تعودون بعد الساعة العاشرة) وعما يجب القيام به. بالإضافة إلى ذلك، إذا قمتم بربط رقم هاتفكم بأي حساب على الانترنت مثل «فيس بوك»، أو غوغل يسمح لكم بإعادة تعيين كلمة السر عن طريق استخدام رمز يرسل عبر رسالة نصية. أزيلوا رقم هاتفكم من الحساب في أقرب وقت ممكن لأنه بإمكان أي شخص لديه بطاقة SIM الخاصة بكم، أو حتى جهازكم المحمول، الوصول إلى حساباتكم.

الخطوة ١: أزيلوا البطارية

في حالة الاعتقال، إذا كنتم قد شفرتم هاتفكم بشكل صحيح ويمكنكم الوصول إليه قبل تسليمه، حاولوا إطفائه أو حتى إزالة البطارية منه ورميها بعيداً. بهذه الطريقة، لن تتمكن الجهة التي تعتقلكم من تشغيل الهاتف دون كلمة السر، حتى إذا استعادت البطارية.

الخطوة٢: استخدام البرمجيات الأمنية المحمولة مثل «سوفوس» لمسح جميع بياناتكم و إنهاء جلسات عمل «فيس بوك»

لبرنامج «سوفوس»، قوموا بإرسال رسالة نصية إلى رقم الهاتف الخاص بكم تتضمن كلمة «wipe» تليها كلمة السر، على سبيل

المثال: «wipe 12345678». يمكنكم أيضاً استخدام مدير جهاز «أندرويد» (https://google.com/android/devicemanager) إذا كنتم قد أعددتموه مسبقاً.

الخطوة ٣: إنهاء جلسات عمل «فيس بوك» وإلغاء ربط رقم هاتفكم من الحسابات على الانترنت

١. إذا كان لديكم «فيس بوك» على هاتفك النقال، انقروا على رمز الدولاب في أعلى اليمين واذهبوا إلى: إعدادات الحساب› الأمن› جلسات الموقع، أو ببساطة انقروا هنا.

٢. انقروا من خلال القائمة على «نهاية النشاط» لكل دورة على الهاتف المحمول.

٣. إذا كنتم قد نسيتم إلغاء ربط رقم هاتفكم من الحسابات على الانترنت التي تسمح إعادة تعيين كلمة المرور باستخدام SMS («فيس بوك»، و«جوجل»، الخ) أزيلوا رقم هاتفكم من تلك الحسابات في أقرب وقت ممكن.

الخطوة ٤: إبلاغ جهات الاتصال لديكم عن فقدان هاتفكم

إذا قمتم بحفظ أرقام هواتف لأشخاص مثل أرقام النشطاء قوموا بإبلاغهم عن فقدان هاتفكم ومحتوياته. بهذه الطريقة، يكون لهؤلاء الأشخاص القدرة على اتخاذ الاحتياطات المناسبة. وأكّدوا عليهم ألا يقومو بالرد على الاتصالات الواردة من الهاتف المفقود.

«أوستل» لإجراء المكالمات المشفّرة

أوستل، هو تطبيق قام «مشروع غارديان» بإنشائه ضمن مجموعة من التطبيقات للهواتف النقالة، كتبنا عن معظمها على موقعنا. تهدف هذه التطبيقات إلى توفير الحماية والأمان أثناء استخدامكم الإنترنت أو الاتصالات والرسائل، أو حتى التصوير، وتتوفّر هذه الأدوات بشكل مجّاني ومفتوح المصدر.

أوستل ليس تطبيقاً مستقّلاً، بل شبكة تعتمد في عملها على تطبيق CSIPSimple بإمكانكم تحميله من متجر غوغل للتطبيقات هنا، أو في حال كان الموقع محجوباً من هنا.

عمله ليس محصوراً بنظام التشغيل أندرويد، بل بالإمكان إجراء اتصالات على كافة أنظمة التشغيل، فهناك العديد من التطبيقات والبرامج التي تدعم شبكة أوستل.

هنا قائمة بأنظمة التشغيل والبرامج التي تدعم الاتصال عبر شبكة أوستل

ويندوز:	Jitsi أو LinPhone
ويندوز٨:	LinPhone
ماك:	Jitsi
لينوكس:	Jitsi
آيفون:	LinPhone
بلاك بيري:	PrivateGSM
أندرويد:	CSIPSimple

سنقوم في مقالنا هذا بشرح طريقة استعمال أوستل عبر الأجهزة التي تعمل بنظام التشغيل أندرويد، ولكن إن كنتم تريدون استعمالها على أحد الأجهزة أو أنظمة التشغيل الأخرى وواجهتم مشاكل أثناء ضبط الإعدادات، فبإمكانكم التواصل معنا عبر صفحتنا على فيس بوك وسنقوم بمساعدتكم.

للبدء باستخدام أوستل نقوم أولا بتحميل التطبيق الخاص به عبر الذهاب إلى متجر غوغل والبحث عن .CSIPSimple

في حال كان الموقع محجوباً بإمكانكم تحميله عن طريق التوجه إلى موقع «مشروع غارديان» ثم النقر على Download Apps ثم اختيار Direct Download APK

بعد الانتهاء من عملية التنصيب يتوجب علينا الآن القيام بتسجيل حساب «أوستل» خاص بنا.

توجهوا إلى موقع الشبكة ostel.co
اختاروا Sign me up
أدخلوا بريدكم الإلكتروني ثم اضغطوا على sign up

في الصفحة التالية سيقوم الموقع باقتراح اسم مستخدم بناء على عنوان بريدكم الإلكتروني؛ بإمكانكم تغييره.
الحقل الثاني هو بريدكم الإلكتروني

أدخلوا كلمة السر في الخانة الثالثة، وأعيدوا إدخالها من جديد ثم اضغطوا على Create my account.

الآن افتحوا تطبيق CSIPSimple
قوموا بالنقر على Accounts ثم Add account
ثم اختيار OSTN
أدخلوا اسم المستخدم وكلمة السر وعنوان السيرفر ثم اختاروا save

ننتظر حتى يتغير لون الأيقونة إلى الأخضر، ما يعني أنه تم تسجيل الدخول الآن وبإمكانكم إجراء المكالمات واستقبالها.

للبدء بإجراء المكالمات قوموا أولاً باختيار txt ثم ضعوا عنوان الشخص الذي تودون الاتصال معه ca@ostel.co ثم النقر على زر الاتصال

بعد بدء المكالمة تظهر شاشة فيها رمز التحقق؛ تأكدوا من الشخص الذي تتصلون به من أن هذا الرمز متطابق كما هو ظاهر.

بإمكانكم أيضاً تسجيل المكالمة عبر النقر على الخيارات ثم اختيار Record.
لإضافة جهة اتصال توجها إلى تبويب سجل المكالمات ثم انقروا على اسم الشخص واختاروا Add to contacts ثم انقروا على أيقونة الإضافة وأضيفوه.

بإمكانكم أيضاً إرسال الرسائل واستقبالها مع جهات الاتصال لديكم عبر النقر على تبويب الرسائل ثم النقر على Compose.

بإمكانكم مشاهدة الفيديو التالي الذي يشرح طريقة استعمال أوستل