



• -:عدة الأمن الإلكتروني لحماية حسابك في شبكة التواصل الاجتماعي تويتر



- 1- وأنه الموقع مشفر في بداية [Twitter.com](https://twitter.com) عند الدخول لشبكة تويتر من خلال المتصفح تأكد دوماً من أنك تدخل للموقع الصحيح - HTTPS الرابط بالعلامة الخضراء، وإنّبه من أي علامات (خطأ) بالإنترنت أو ظهور صفحة لشهادة مزيفة تطلب "القبول" أو HTTPS الرابط بالالتحويل لموقع آخر يتطلب أي صلاحيات أو دخول على حسابك.
- 2- عند استخدام تويتر من هاتفك سواء "الأندرويد" أو الآيفون فيفضل استخدام التطبيق الرسمي لتويتر لما قامت به تويتر من جهد في فقط وليس من المواقع والمنشآت Google Play تشفير تطبيقاتها، وقم بتحميلها من متجر آبل الرسمي أو تأكد من أن حسابك في تويتر مرتبط فعلياً بإيميلك الخاص، وتأكد من قدرتك للدخول على الإيميل، وذلك حتى تستطيع إسترجاع -3 الحساب في حالة إختراقه أو توقيفه.
- 4- تأكد من استخدام كلمة مرور صعبة ومعقدة، ويجب أن تكون مختلفة عن كلمة المرور الخاصة بالإيميل.
- 5- "Request Personal" قم بتفعيل خيار " طلب معلومات شخصية عند طلب إستعادة كلمة المرور " أو ما يسمى "Information" من قسم الإعدادات في تويتر، وذلك لوضع عقبة أمام محاولات إختراق حسابك.
- 6- من الإعدادات الخاصة بالحساب ثم "Login Verification" عند استخدامك تطبيق تويتر الرسمي في الهاتف يفضل تفعيل خيار "الأمان" وذلك لإيقاف الهاكر من استخدام حسابك حتى لو حصل فعلاً على كلمة المرور، لأنه بتفعيل هذا الخيار سيطلب منك تويتر التصريح بالدخول في كل مرة تدخل فيها تويتر من جديد، تذكر أيضاً حفظ الأكواد الاحتياطية التي سيعطيكها لك تويتر ، وإلا لن تستطيع حتى أنت دخول حسابك في حال ضياع جهازك أو لو كان مغلق.
- 7- لا تجعل لأي تطبيقات غير مرغوب فيها من القدرة لاستخدام حسابك، كتطبيقات التغريد الآلي والإحصائيات والقرآن والأذكار وهكذا -8 لا تدخل أي روابط مشبوهة أو روابط يرسلها لك أشخاص قد يستهدفوك، تأكد دائماً أن الرابط صحيح بالنظر إليه والتأكد من سلامة الحروف والكلمات.
- 9- قد يستهدفك الهاكر بواسطة البريد عن طريق إرسال إيميل يبدو كأنه من "تويتر" ويطلب تغيير كلمة المرور أو إعادة الدخول -10 للحساب، إنتبه من ذلك.
- 10- أعط كلمة المرور لشخص تثق فيه، حتى يغير كلمة المرور في حال إعتقالك أو مصادرة جهازك، أو حتى يقوم بإعلام متابعيك -10 في حال أي مكروه قد يصيبك.

- 11- عند التقاط الصور وعند نشرها في مواقع التواصل فإنها ستدل عليك وعلى مكانك GPS Tagging إننتبه من تفعيل خاصية -11 بالضبط وقد يتم إستهدافك
- 12- تعتبر الرسائل الخاصة في تويتر آمنة ومشفرة، بشرط إستخدامها بالشكل الصحيح وقد نشرنا في سايركوف تقريراً خاصة بذلك -12 وبعنوان [\(رسائل الخاصة ليست خاصة، كيف تحافظ على سرية رسائل الخاصة في تويتر\)](#).

• :-عدة الأمن الإلكتروني عند التقاط ونشر الصور



- لم تعد الصورة التي تخرج اليوم من هاتفك المحمول مجرد صورة، بل تحتوي على العديد من المعلومات حولك، يمكن إستخراج -1 المعلومات الموجودة بالصور، ومنها قد تكون معلومات "موقعك الجغرافي" تأكد دائما من تعطيل Exif Data هذه المعلومات بواسطة معلومات "خدمات الموقع الجغرافي" في كاميرا هاتفك من خلال إعدادات الكاميرا في الأندرويد، أو إعدادات الخصوصية في الأيفون
- 2- يمكنك أيضا نشر معلومات مزيفة "لموقعك الجغرافي" بحيث تظهر الصورة بأنه تم التقاطها في المكان الفلاني وهو موقع مزيف، أيضا [Photo GPS Editor](#) للأيفون لتزيف موقع الصورة الجغرافي، أو تطبيق [Mappr](#) يمكنك إستخدام تطبيق
- وهنا لقاء قصير بخصوص حفظ خصوصيتك في تطبيق الإنستغرام والذي لا ينصح بإستخدامه لإتباعه سياسية الفيسبوك في جمع المعلومات وصيت سيء في حماية الخصوصية

• :-للإتصالات GSM عدة الأمن الإلكتروني عند إستخدام شبكة الهواتف



1- مشفرة عن المستخدم العادي فقط وتشفيرها ضعيف لدرجة سهولة إختراقها والتتصت على GSM من المعلوم أن شبكات الهواتف المحادثات باستخدام أدوات لا تتجاوز قيمتها \$3000 دولار، لذلك يفضل عدم إستخدامها بواسطة المراسلين والصحفيين والإعلاميين وإستخدام هواتف مشفرة لحماية المحادثات الحساسة

2- الألمانية التي تشفر المحادثات، ولكن يجب على الطرفين إستخدام نفس [CryptoPhone](#) إستخدام هواتف مشفرة من شركة -الهاتف لإتمام مكالمات آمنة

3- [silent](#) الذي يعمل بنظام أندرويد والذي يحتوي على تطبيقات للحفاظ على أمن إتصالاتك مثل [BlackPhone](#) إستخدام هاتف -وغيره [circle](#)

4- وقد فصلناها في قسم خاص من هذا المقال GSM مشفرة بديلة عن شبكات الـ VOIP إستخدام تطبيقات صوتية -

• -عدة الأمن الإلكتروني عند قطع الإتصالات والإنترنت



- تتجه بعض الدول عند إشتداد الإحتجاجات الى قطع الإتصالات والإنترنت عن الحشود أو المتجمهرين او الدولة بالكامل وهنا بعض الحلول للإستمرار في التواصل في حالة قطعت الإنترنت والإتصالات:
- 1- إستخدام الهواتف المتصلة بالساتلايت لإجراء المحادثات أو الإنترنت
 - 2- إستخدام الإنترنت الفضائي للوصول للإنترنت بمعزل عن المزود المحلي للإنترنت
 - 3- يجب ضبط إعدادات حسابك (في حال حجب شبكة تويتر أو قطع الإنترنت وبقاء الإتصالات SMS إستخدام التغريد بواسطة ال- SMS بتويتر للتغريد بواسطة الرسائل النصية)
 - 4- خاصة داخلية وبعيدة المدى للتواصل بين المجموعات حتى لو قطعت الإنترنت والإتصالات Wifi إنشاء شبكات وإيرلس
 - 5- الموجود [للأيفون](#) و [للأندرويد](#) لمشاركة الصور والمحادثات في محيط 200 متر وبدون الحاجة للإنترنت FireChat إستخدام تطبيق
 - أو الإتصال أو حتى شريحة هاتف، حيث يقوم بفتح (غرف دردشة للصور والمحادثات) تستوعب حتى 80 شخص في شبكة داخلية بينهم فقط، ويجب الإنتباه أن التطبيق لا يستعمل التشفير في الوقت الحالي، فيجب إستخدامة فقط عند قطع الإنترنت والإتصالات وليس بشكل دائم
 - 6- [للأيفون](#) و [للأندرويد](#) للتواصل الكتابي بدون الحاجة للإنترنت أو شبكات الإتصال Tin-Can app إستخدام تطبيق
 - 7- [للأجهزة الأندرويد](#) وهو تطبيق يجعل جهازك عبارة عن محطة للاتصال مع أطراف أخرى [The Serval Project](#) إستخدام تطبيق
 - تستخدم نفس التطبيق وفي محيط 200 متر وكلما زاد عدد المستخدمين زاد محيط عمل التطبيق، ويتم التواصل بواسطة أرقام داخلية "مثل نظام" البدالة
 - 8- "قصيرة المدى للتواصل عبر موجات الراديو " لكنها غير مشفرة Walkie Talkie إستخدام أجهزة ال-

- عدة الأمن الإلكتروني في تشفير كافة نشاطاتك عند الإتصال بالإنترنت



يعد الإتصال بالإنترنت بواسطة الهواتف هو العامل الأكثر أهمية في جمع معلوماتك، حيث يقوم جهازك بنشر العديد من البيانات التي تعمل بالخلفية وكذلك عند تصفحك للأنترنت لمواقع غير مشفرة، مع الأخذ بعين الإعتبار أن اغلب "الترافيك" الذي تستخدمه بالإنترنت هو غير مشفر ويمكن من خلال تحليله ومراقبته الوصول لكم كبير من المعلومات حولك، والوصول للمكان التقريبي لتواجدك بكشف

بشكل دائم عند إتصالك بالإنترنت حتى تخفي VPN الخاص بك مثلاً، لذلك ينصح دائماً بتشفير الإتصال بإستخدام شبكات الـ IP رقم الـ وأجهز الأمن والمخابرات وغيرهم ISP موقعك ونشاطاتك بالكامل عن مزود الخدمة.

ويفضل الابتعاد عن الخدمات الأمريكية أو العربية في هذا المجال VPN قم بإستخدام خدمات الـ 1-

F- للهواتف للآيفون [من هنا](#) و للآندرويد [من هنا](#) ، وهي خدمة من شركة الأمن الفنلندي VPN الـ [Freedom](#) قم بإستخدام خدمة -2 وهي ليست مجانية، ولكنها سريعة وتحميك من الرقابة والتجسس والمواقع المزورة وغير ذلك Secure

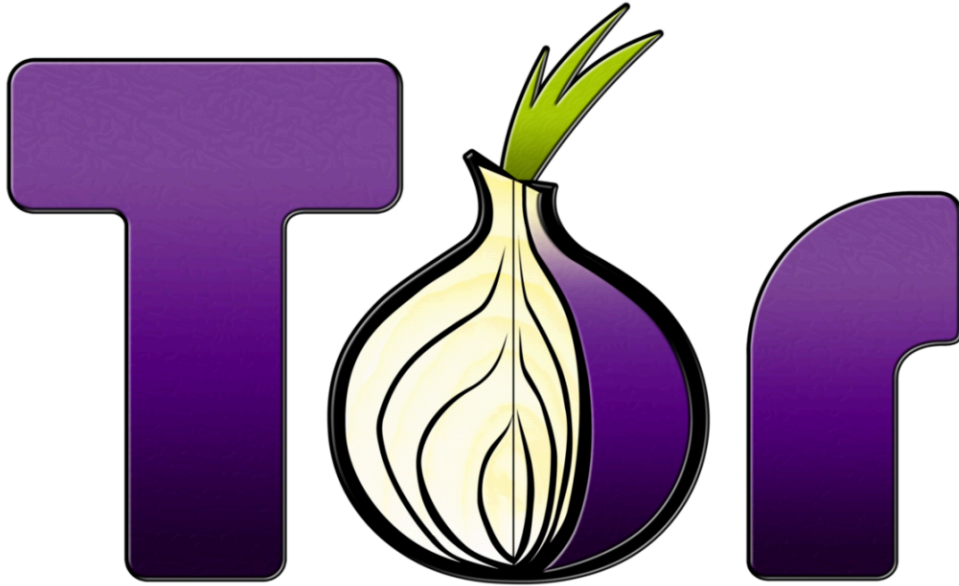
يمكن تحميل تطبيقها للآيفون [من هنا](#) ، وللآندرويد [من Avast](#) من شركة الأمن Avast SecureLine! أو قم بإستخدام تطبيق -3 [هنا](#) ، كما يمكن إستخدامة لأنظمة الوندوز [من هنا](#)

هناك أيضاً برامج أخرى ولكن من مميزات البرامج السابقة أنها تقوم بتتصيب شهادة تشفير وتحكم بإتصالك، وفي حال إنقطاعه بشكل مفاجئ يتم الإتصال بشكل أوتوماتيكي بالبرنامج مما يعطيك حماية إضافية يجب التنبيه أيضاً : لإيقاف عمل البرنامج يجب إزالة شهادة التشفير من الإعدادات في الآيفون

• -:عدة الأمن الإلكتروني في التصفح الآمن في الإنترنت

يعتبر المتصفح هو بوابتك الى الإنترنت، تستخدمه مواقع الإنترنت في جمع كم هائل من المعلومات التي يتم تحليلها فيما بعد لمراقبة سلوكك، فيما يلي متصفحات تحمي خصوصيتك وتشفر بياناتك لتبتك بعيداً عن أعين الرقابة

يخفي هويتك ويحميك من التتبع ويمكنك من مشاركة المعلومات بشكل سري ومشفر وخفي ينصح به **TorBrowser متصفح -1** دائماً عند الرغبة في اخفاء هويتك اثناء القيام بنشاطاتك عبر الإنترنت بشكل مجهول لا يدل عليك



[لتحميل النسخة الإنجليزية من هنا](#)

[لتحميل النسخة العربية من هنا](#)

للآندرويد يخفي هويتك ويحميك من التتبع ويمكنك من مشاركة المعلومات بشكل سري ومشفر وخفي وهو نسخة Orweb متصفح -2
"لكنها لنظام "آندرويد TorBrowser مماثلة لـ

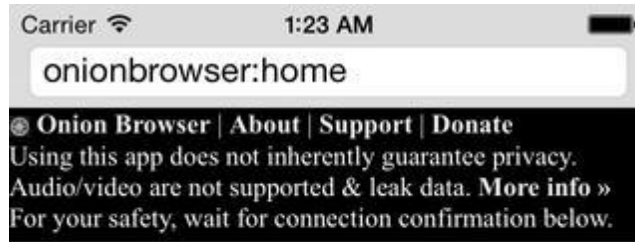


Browse Privately

للتحميل من المتجر الخاص بنظام أندرويد [من هنا](#)

لإخفاء الهوية قبل التصفح (وقد Tor حتى يستطيع بدوره من الدخول على شبكة Orbot **ملاحظة:** هذا المتصفح يتطلب تنصيب برنامج يحتاج عمل روت للجهاز)

للآيفون: يخفي هويتك ويحميك من التتبع ويمكنك مشاركة المعلومات بشكل سري ومشفر **Onion Browser متصفح -3**
TorBrowser في أندرويد و Orweb وخفي وهو مماثل لـ



Congratulations. Onion Browser has successfully connected over Tor.

This page at onionbr5zulufnuj.onion is only accessible over Tor.

You may now browse the Internet anonymously. You can visit check.torproject.org for further connection confirmation; note that this site only checks for the official PC/Mac/Linux client, so an **orange** confirmation is expected.

Warning: JavaScript is enabled and may affect your anonymity.

Note: Onion Browser users are advised to avoid using the "Define" function when selecting text, as this will leak traffic outside of Tor.

Please note that Onion Browser is still experimental software; check [the Onion Browser website](#) for the latest caveats and security information. For help, [check the built-in help page](#).

[Donate to Support Onion Browser](#)

And donate to support these other free speech and online rights organizations:

[The Tor Project](#)

[Freedom of the Press](#)

[Electronic Frontier Foundation](#)

This page based on check.torproject.org, available at <https://github.com/torproject.org/check.git> under the MIT license.



[للتحميل من المتجر الخاص بالآيفون من هنا](#)

متصفح آمن وسهل الاستخدام ويحمي خصوصيتك ويحميك من سكربتات المراقبة في المواقع المختلفة ولكنه لا **Aviator** متصفح -4
يخفي هويتك ولا يشفر إتصالاتك



[للتحميل من هنا](#)

للايفون والاندرويد: يقوم هذا المتصفح بالدخول على المواقع باستعمال بروكسي خاص بالشركة ومنها يتم **Opera Mini** متصفح -5
الخاص بك ويظهرك من دولة أخرى، كما يفتح حجب المواقع IP اخفاء هويتك اثناء التصفح ويخفي رقم الـ



[للتحميل لأجهزة أندرويد من هنا](#)

[للتحميل لأجهزة آيفون من هنا](#)

ومنها السعودية، OperaMini ملاحظة: هناك بعض الدول قامت خاطبت شركة أوبرا حتى تلغي التشفير والتخفي الموجود في متصفح. لذلك لا تعتبر استخداماً آمناً بالسعودية

وهو يقوم بتشفير الإتصال ويفتح المواقع المحجوبة وهو نفس تطبيق Yandex OperaMini وعوضاً عنه يفضل إستخدام متصفح الروسية الشهيرة بإضافة بعض التحسينات عليه yandex الأصلي ولكنه قامت شركة OperaMini

من هنا Yandex OperaMini لتحميل تطبيق

[للآيفون من هنا](#)

[للأندرويد من هنا](#)

- عدة الأامن الإلكتروني في حماية الملفات و تشفير الأجهزة بالكامل



بعد تشفير كامل الجهاز أحد أهم الخيارات بالنسبة للمراسلين من مناطق النزاع خاصة عند فقد الأجهزة أو مصادرتها أو ضياعها، أجهزة الآيفون تكون مشفرة بمجرد وضع قفل للشاشة ويفضل أن تكون كلمة سر طويلة وليست ذات الأربعة حروف، أما أجهزة الأندرويد فالتشفير فيه إختياري من الإعدادات الخاصة بالأمان، ويفضل تفعيلها للجهاز بالكامل وللذاكرة الداخلية، ولكن بعد أخذ نسخة احتياطية لمحتويات جهازك تحسباً لحدوث أي خطأ أثناء التشفير

فيما يلي أدوات تشفير لأجهزة اللابتوب بالكامل أو الفلاش ميموري

يقوم بتشفير كامل جهازك أو جزء منه أو مجموعة من ملفاتك في أجهزتك ويحافظ على سريتها ويمنع TrueCrypt برنامج -1 الحصول عليها في حال ضياع الجهاز أو مصادرته أو الحصول عليه قسراً

[للتحميل من هنا](#)

فقط ولا تقم بتحميل النسخ الجديدة (7.2) لوجود تغييرات فيها وتوقف TrueCrypt ملاحظة: قم بتحميل النسخة (7.1) من برنامج خصائص التشفير من قبل المطورين لأسباب مجهولة

غير أنه تم تطويره من قبل شركة فرنسية TrueCrypt وهو برنامج تشفير ملفات مبني على برنامج VeraCrypt برنامج -2 TrueCrypt وزيادة آلية عمل التشفير فيه وهو يعمل بشكل مماثل وبنفس طريقة



[للتحميل من هنا](#)

وهو متاح بعدد من إصدارات نظام مايكروسوفت ويندوز ويمكنك من تشفير الجهاز **BitLocker** التشفير بواسطة نظام ويندوز -3
بالكامل أو تشفير فلاش ميموري أو هاردسك خارجي أيضاً، وهو مناسب لحماية بياناتك

[من هنا](#) BitLocker للتعرف أكثر على نظام التشفير

السريعة [integral CryptoSSD](#) استخدام أقراص صلبة (هاردسكات) مشفرة بذاتها وبدون تدخل البرامج مثل أقراص شركة -4
الفلاش ميموري المشفير، ولشك هناك أنواع أخرى كثيرة [Storage datAshur](#) والتي تحتوي شريحة تشفير مدموجة بها، أو شركة
منها الغالي ومنها متوسط السعر، وعند الحديث في هذا القسم رأيت من المناسب الحديث عنه في مقال جديد مستقل يشرح كافة هذه
الأنواع وقيمها، وأكتب ذلك حين يتيسر الأمر بإذن الله



• عدة الأمن الإلكتروني في التراسل الآمن عبر البريد الإلكتروني:

يعد البريد الإلكتروني اليوم من احد اهم وسائل التواصل الخاص، وارسال التقارير وعمل اللقاءات والمقابلات او نشر التسيريات وغير ذلك، ويستخدم العديد بريد إلكتروني من شركة (جوجل و مايكروسوفت وياهو) وإن كان جديدين من ناحية الأمن ضد هجمات الهاكرز ولكنه لا يحميك من تلصص الحكومة الأمريكية أو شركة جوجل و مايكروسوفت، والتي قد تستغل ضدك يوم من الأيام، لذلك يفضل استخدام شركات ليست أمريكية وكذلك تحافظ على خصوصيتك وأمنك الشخصي

خدمة بريد إلكتروني آمنة ومجانية يمكن من خلالها فتح حساب والبدء بالمراسلات حيث تتكفل الخدمة بتشفير **Hushmail** خدمة -1
الرسائل دون تدخل من المستخدم تكمن سیرفرات الخدمة في كندا، وهي أحد أشهر خدمات البريد الآمن

[للتسجيل من هنا](#)

خدمة بريد إلكتروني آمنة ومجانية ولكنها جديدة لذلك يجب عليك طلب دعوى لفتح حساب جديد في **ProtonMail** خدمة -2
الخدمة، مشفرة تشفير عالي وتكمن سیرفرات الخدمة في سويسرا، ويشرف عليها علماء في الفيزياء والتشفير من جامعة هارفرد
والوكالة الأوروبية للأبحاث النووية، وشركة سايبيركوف لها شراكة خاصة بالمشروع وقد أشرفت على فحصها والتأكد من MIT و
تشفيرها، وحصلت على شهادة تركية وتقدير من المؤسسات المذكورة

[للتسجيل من هنا](#)

بريد إلكتروني مشفر بالكامل وآمن وسهل الاستخدام ويحافظ على الخصوصية ويمكن فتح حساب بالمجان. **خدمة Tutanota -3**
ولكنه يطب رقم هاتف عند التسجيل لأغراض إستعادة الحساب عند NSA تكمن سيرفراته في ألمانيا ويقول مطوره أنه محمي من ال
فقدانه.



[للتسجيل من هنا](#)

• عدة الأمان الإلكتروني في التراسل الكتابي الآمن:

تعد برامج وتطبيقات التواصل الكتابي من أشهر وسائل التواصل المباشر الذي يستخدمه الملايين حول العالم في التواصل العائلي والتجاري والإعلامي والعديد من المجالات، والحفاظ على أمن هذه المراسلات والمحادثات يجب أن يكون ذو أولوية قصوى لكل أفراد المجتمع وبخاصة النشطاء والإعلاميين والمراسلين لما عليهم من مسؤولية في حفظ مصادر معلوماتهم، لذلك لا يجب أن يستخدموا برامج وغيره من البرامج التي لاتحمي بياناتهم ولا خصوصياتهم وتسمح لأجهزة الأمان (Line أو WhatsApp الواتساب) غير آمنة مثل والمخابرات والهاكرز بالتجسس عليهم وإختراقهم، وفيما يلي قائمة بأفضل برامج التواصل الكتابي الذي يحمي خصوصيتك وسرية محادثاتك.

متوفر للآندرويد والآيفون فقط ولا يجبرك على استخدام رقم End-to-End برنامج للتراسل الكتابي المشفر: **Threema برنامج -1**
فريد لكل مستخدم، كما يمكن إستخدام رقم هاتفك أيضاً وسيقوم بعمل (ID الهاتف للدخول والمحادثه حيث يعتمد البرنامج على توليد تزامن) حتى تعرف من من أصحابك يستعمله، وتكمن سيرفرات البرنامج في سويسرا، وهو آمن ومشفر بشكل كبير وآمن من العديد من أنواع الهجمات وينصح به أن يكون برنامج الأول في التواصل كما يوفر المجموعات، والتخابر الصوتي وتبادل الصور والفيديو بشكل مشفر أيضاً.



[للتحميل لأجهزة آيفون من هنا](#)

[للتحميل لأجهزة أندرويد من هنا](#)

مشفرة من النهاية "Secret Chat" برنامج "تلغرام" روسي المنشأ يحتوي على ميزة المحادثات السرية: **Telegram برنامج -2** بينك وبين من ترسل كما تحتوي على ميزة "التدمير الذاتي" بعد فترة يتم تحديدها في المحادثة. وقد تم "End-to-End" الى النهاية كتابة موضوع تفصيلي وشرح ممل لمن يريد الاستزادة [اقرأ هنا](#). ولاننصح باستخدامه للقروبات، حيث يمكن استرجاع المحادثات بسبب ميزة "التزامن" لو تم مصادرة جهازك.



Telegram

taking back our right to privacy

[لتحميل برنامج تيليجرام للأندرويد من هنا](#)

[لتحميل برنامج تيليجرام للآيفون من هنا](#)

برنامج آمن ومشفّر للتراسل الكتابي عبر الهواتف الذكية. لا يتطلب أي رقم هاتف أو أي إيميل عند التسجيل: **SureSpot برنامج -3** وبدأ الاستخدام.

[للتحميل في أجهزة أندرويد من هنا](#)

[للتحميل في أجهزة آيفون من هنا](#)

يدعم التراسل الكتابي الآمن ويدعم القروبات ويحافظ على خصوصية المستخدم ويحتوي على ميزة "التدمير الذاتي" للرسائل. متوفر للآيفون والأندرويد: **Wickr برنامج -4**



[للتحميل في أجهزة أندرويد من هنا](#)

[للتحميل في أجهزة آيفون من هنا](#)

يمكن استخدام خدمة "كربتوكات" للتراسل الكتابي الآمن ويمتاز كربتوكات بتوفير إضافة في المتصفح: **Cryptocat خدمة -5** وتوفير برامج في الماك والآيفون للتراسل المشفر عبر قنوات يتم انشاؤها في السيرفر، وهو ليس كباقي التطبيقات، وإنما يتم عبر إنشاء غرفة مشفرة للدردشة تعتمد على الأسماء الوهمية او (ال نيك نيم) يتم عبرها التواصل بين الأعضاء.

CRYPTOCAT Cryptocat Documentation Blog

Cryptocat lets you chat with privacy.
We're developing an easy to use web app that encrypts your conversations. It's open-source, translated into 32 languages and you already know how to use it.

[Download Cryptocat for Chrome](#)

Encrypted IM can be easy and accessible.

Cryptocat is free software that aims to provide an open, accessible Instant Messaging environment that encrypts your conversations and works right in your browser. [Download Cryptocat for Chrome.](#)

Cryptocat is an open source experiment – the goal is to provide the easiest, most accessible way to chat while maintaining your privacy online, because we believe in Internet privacy.

[من هنا](#) Firefox لتحميل إضافة متصفح

[من هنا](#) Chrome لتحميل إضافة متصفح

[من هنا](#) Safari لتحميل إضافة متصفح

[من هنا](#) لتحميل البرنامج لنظام ماك

[من هنا](#) لتحميل البرنامج في آيفون

و Viber وهو تطبيق سويسري مشفر وآمن ويقدم خدمات التواصل الكتابي والصوتي مثل : **IO SwissCom تطبيق 6-**

وستحدث عنه أكبر في قسم (التواصل الصوتي الآمن) Tango

لشركة بريطانية يقدم تشفير عالي المستوى ويدعي مطورينه أن حتى شبكات الحاسب العملاقة لا تستطيع كسر : **PQChat تطبيق 7-**

تشفيره، وهو عند تنصيبه على الجهاز يجبر المستخدم على تفعيل المميزات الأمنية مثل (الماستر باسورد) و رقم سري آخر للدخول للبرنامج، كما يحتوي على مميزات (توثيق إضافي) حتى تتأكد بالفعل أنك تحدث الطرف الآخر الصحيح، وأنه لا يتحدث اليك شخص آخر أو تحت الماكراه

PQChat About Technology Enterprise FAQ Contact us

Your Post-Quantum Secure Messenger

PQChat is the world's first commercially available post-quantum messenger based on our "Never The Same" technology. Every message you send has a different encrypted output.

[Watch the Video](#)

AVAILABLE ON [Download on the App Store](#) COMING SOON ON [GET IT ON Google play](#)

متوفر حاليا فقط لأصحاب الآيفون ويمكن تحميله [من هنا](#)

لألمانيا من مستشارتها ميركل الى أصغر NSA الماني جاء للرد على التجسس الأمريكي الموسع بواسطة الـ **Sicher** تطبيق -8 مواطن فيها، يستخدم التشفير بشكل أساسي ويحمي الخصوصية، وبه العديد من الميزات وينقل الملفات والصور بشكل مشفر ويمكن التحكم بحذف ماتم مشاركته



متوفر لأجهزة الآيفون [من هنا](#)

ومتوفر لأجهزة الأندرويد [من هنا](#)

التابعة لشركة آبل، وهي خدمة مشفرة من (النهاية الى النهاية) وآمنة ولا يمكن للحكومات ولشركات **iMessage** استخدام خدمة -9 الاتصالات وحتى لشركة آبل مراقبتها والتنصت عليها، وقد ذكرت ذلك في [دليل التعامل مع جهات تنفيذ القانون](#)، ولكن الخدمة مقتصرة حيث أن (iMessage) عند فشل الـ SMS إعادة الإرسال بالـ (على منتجات آبل فقط، وعند تفعيلها يجب الانتباه على إغلاق خاصية مكشوفة ومراقبة SMS رسائل الـ



• Encrypted VOIP :- عدة الأمن الإلكتروني في التواصل الصوتي الآمن

و Viber يعتبر التواصل الصوتي من أكثر أنواع التواصل فعالية وسرعة وكثيراً ما يستعمل النشطاء او عموم الناس برنامج مثل غير مشفر أصلاً، ولا يجب عليك استخدامهم، ويستخدم الناس أيضاً بكثرة خدمة وبرامج سكايب Tango وهما إسرائيليان والـ Tango وهي مشفرة عن الحكومات المحلية ولكن ليست عن الإستخبارات الأمريكية والروسية والصينية والإسرائيلية كما أظهرت Skype العديد من التقارير، كما انه تمت إضافة خدمات التزامن للمحادثات الكتابية فيه مما يشكل خطر، كما يقوم بتخزين المحادثات في -مايكروسوفت وفي الأجهزة بدون تشفير، لذلك لا ننصح به وننصح باستخدام البدائل التالية

وهو تطبيق مفتوح المصدر ويوفر التواصل الآمن والمشفّر الكتابي والصوتي بشكل ممتاز ولا يعتمد على **Linphone برنامج -1** رقم الهاتف وإنما على " إسم المستخدم " الذي تقوم بإنشاءه وقت تشغيل البرنامج وتسجيل حساب خاص بك، ولكن يجب الإنتباه انه وهو تفعيل للتشفير في محادثات الفيديو والصوت **SRTP** عليك الدخول للإعدادات وتفعيل خيار التطبيق يعمل على كافة المنصات مثل الآيفون والآنرويد والوندوز ولينكس مما يتيح لك حرية كاملة في الاختيار

[لتحميل التطبيق للآيفون من هنا](#)

[لتحميل التطبيق للآنرويد من هنا](#)

ولكنه مشفر Tango والـ Viber وهو تطبيق سويسري رائع للمحادثات الصوتية والكتابية شبيه بالـ **IO Swisscom تطبيق -2** ولا يمكن التجسس على محادثاتك الصوتية فيه، كما يحتوي على محادثات كتابية مشفرة **SRTP** بالكامل للصوت باستخدام تقنيات أيضاً، ويعتمد على رقم الهاتف في التفعيل وتزامن جهات الإتصال وسهل الإستخدام وكل سيرفراته في سويسرا، وهو غير مشهور بالعالم العربي.



[لتحميل التطبيق للآيفون من هنا](#)

[لتحميل التطبيق للآندرويد من هنا](#)

الآمنة والمشفرة بشكل عالي، ولكن بإشترك شهري ويجب على الطرفين إمتلاك البرنامج، **Silent Circle** تطبيق وخدمات شركة -3 Silent Contacts و Silent Text و Silent Phone وهو فعال وسريع وآمن، ويتكون من 3 تطبيقات وهم

[للتحميل للآيفون من هنا](#)

[للتحميل للآندرويد من هنا](#)

ويعمل على نظام أندرويد فقط في ZRTP وهو تطبيق مفتوح المصدر ومشفّر بالكامل ويستخدم تشفير **RedPhone** تطبيق -3 الوقت الحالي، من إنتاج شركة [وسير سستمز](#) لمجموعة من النشطاء في مجال الخصوصية وأمن المعلومات



[للتحميل للآندرويد من هنا](#)

Encrypted VOIP للاتصالات المشفرة Signal **تحديث:** تم الإعلان من الفريق المطور بيوم 30/7/2014م عن إنطلاق خدمة بالآندرويد RedPhone للآيفون وهي تعمل ومتطابقة للعمل مع من يمتلك تطبيق

وهي تابعة [Whisper Systems](#) أنشأته شركة Encrypted VOIP وهو تطبيق للاتصالات الآمنة **Signal: تطبيق -4** لمجموعة من النشطاء في مجال الخصوصية وأمن المعلومات، والتطبيق خاص بالآيفون ويعمل بشكل متطابق لمن يمتلك تطبيق الغير قابل للتجسس، وهو مجاني ومفتوح المصدر ZRTP لنفس الشركة، حيث يوفر إتصالات آمنة ومشفرة بتشفير Redphone

[لتحميل التطبيق للآيفون من هنا](#)

وهي (FaceTime Audio/ FaceTime Video) لأجهزة آبل سواء الصوتية أو الفيديو **FaceTime** استخدام خدمات -5
آمنة ومشفرة من (النهاية الى النهاية) وإستخدامها للناس العاديين او المراسلين والإعلاميين أفضل من استخدام الإتصالات العادية التي
حيث أنها مراقبة في الغالب، ويعتبر الفيس تايم آمن ومشفر بحيث لا تستطيع شركات الإتصالات والإنترنت وأجهزة GSM بواسطة الـ
الأمّن مراقبته، وذكرت شركة آبل بدليل ([قواعد التعامل مع قوى تنفيذ القانون](#)). أنها لا تستطيع تزويد القضاء الأمريكي بمحتوى
المكالمات او المحادثات لأنها لا تمتلك سلطة عليها.

• عدة الأمن الإلكتروني في التخزين السحابي للملفات:

يستخدم الكثير خدمات "الكلود" او الخدمات السحابية لتخزين ملفاتهم وصورهم أو عمل نسخة احتياطية من ملفاتهم الهامة والغير هامة،
دروب بوكس، والتي إنضمت كوندليزا رايس لمجلس إدراتها مؤخراً وهي Dropbox ولعل أكثر خدمة شهيرة بهذا المجال هي خدمة
المعروف عنها محاربتها للخصوصية وتأييدها المطلق للتجسس الإلكتروني، لذلك نصح إدراور سنودن بعدم إستخدام الخدمة وإعتبرها
خطرة على الأمن الشخصي والخصوصية.

وهنا نضع خدمات بديلة وآمنة ولاتقل عن دروب بوكس من ناحية المساحة والمميزات بل أفضل منها بكثير.

خدمة تخزين سحابي آمنة جدا ومجانية توفر مساحه 50 جيجابايت بالمجان وتقوم بتشفير الملفات اثناء انتقالها **MEGA خدمة -1**
كما توفر برامج للهواتف الذكية، أندرويد وآيفون، Windows واثاء تخزينها في سيرفرات الخدمة. توفر الخدمة برامج لنظام
وصاحبها معروف بحماية الخصوصية ودعم ويكيليكس.



[لتحميل البرنامج في نظام أندرويد من هنا](#)

[لتحميل البرنامج في آيفون من هنا](#)

[للتسجيل وفتح الحساب من هنا](#)

خدمة تخزين سحابي مشفرة تشفير عالي جدا تحافظ على سرية ملفاتك حيث لا يمكن لأحد ولا لموظفي **SpiderOak خدمة -2**
الشركة الإطلاع على محتويات ملفاتك



[لتحميل البرنامج في أندرويد من هنا](#)

[لتحميل البرنامج في آيفون من هنا](#)

[للتسجيل وفتح حساب من هنا](#)

3- خدمة لتخزين الملفات بسيطة وسهلة الاستخدام وتوفر برامج للهواتف الذكية، أندرويد وآيفون، هذه الخدمة: SugarSync خدمة -3
مدفوعة. يمكن استئجار مساحته بسعر 7 دولار شهرياً تقريباً



[للتحميل في أندرويد من هنا](#)

[للتحميل في آيفون من هنا](#)

4- خدمة لتخزين الملفات سحابياً مشفرة وتوفر 15 جيجابايت بالمجان. تحافظ على سرية ملفاتك وتحميها وتحمي: copy.com خدمة -4
خصوصيتك. توفر برامج لجميع الأنظمة تقريباً



[لتحميل البرنامج في أندرويد من هنا](#)

[لتحميل البرنامج في آيفون من هنا](#)

[للتحميل في نظام وندوز أو ماك من هنا](#)

يجب عليك دائماً الحذر ومعرفة طرق الجواسيس والهكرز وتفاديها وقد نشر سايبركوف تقريراً خاصاً بذلك بعنوان [\(وجهاً لوجه مع جواسيس دمشق | كيف تقوم المخابرات الإلكترونية السورية بالابتلاع بنشاط الإنترنت؟\)](#) فراجع

هذا دليل مختصر نسأل الله بالإخلاص فيه، ونتمنى أن يتم نشره ومشاركته على أوسع نطاق، وسنسعى في سايبركوف لتقديم مواضيع مماثلة بشكل أكثر تفصيلاً في المستقبل والله من وراء القصد وفوق كل ذي علم عليم

خالد من غزة