

[Informàtic](#)

5 aplicacions de missatgeria instantània segura



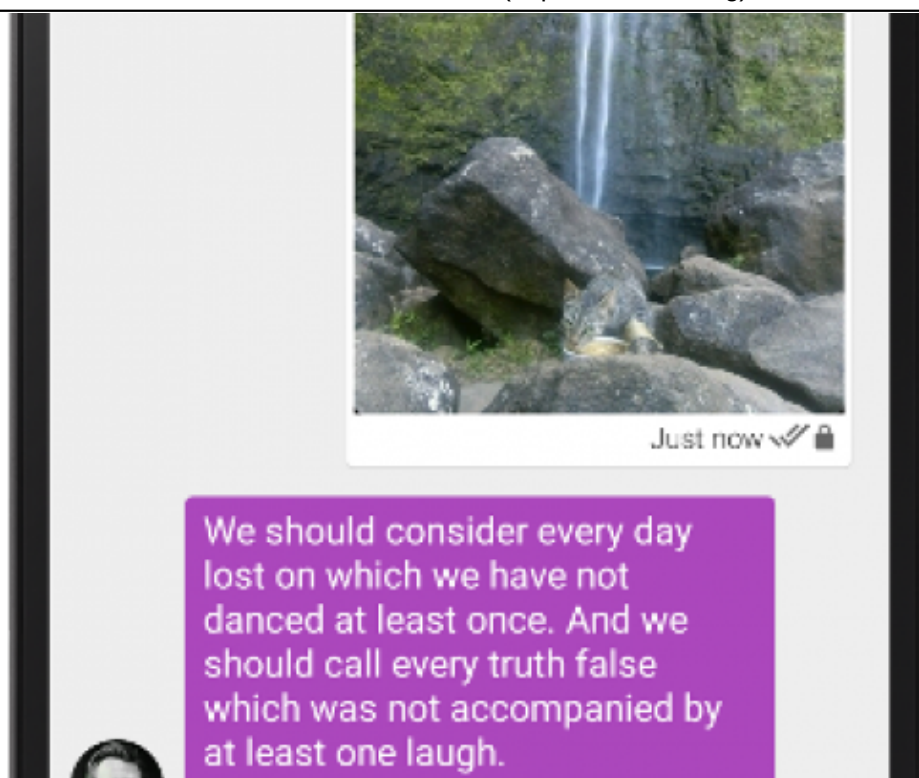
13/10/2017

Associació per a Joves TEB - Informàtic

Autor/a: Associació per a Joves TEB



Telegram permet obrir canals de comunicació secrets, que són encriptats punt a punt.



Signal és molt poc utilitzat i és una de les eines més segures que hi ha al moment.



Briar és una aplicació que de moment té fase beta, però que també és molt segura.



Whatsapp no és codi lliure i utilitza una criptació pròpia.



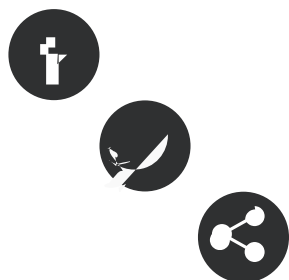
Firechat és una eina que permet enviar missatges sense tenir connexió Internet.

5 aplicacions de missatgeria instantània segura

13/10/2017

Autor/a: Associació per a Joves TEB

Associació per a Joves TEB - Informàtic



Resum:

Moltes aplicacions de missatgeria instantània no fan servir protocols de xifratge, el qual significa que la comunicació pot ser captada molt fàcilment. Les següents aplicacions poden enviar missatgers segurs.

Actualment vivim temps d'organització ciutadana, de participació en mobilitzacions i d'accions pacífiques al carrer. Tot això requereix molta organització i **molta comunicació**, que sigui realment efectiva. Les mobilitzacions de l'11 de març del 2004 van ser un èxit [gràcies als missatges SMS](#) que la ciutadania va anar enviant a tots els seus contactes del seu telèfon mòbil. Avui en dia, el SMS **gairebé no es fa servir** i ha deixat pas a les aplicacions de missatgeria instantània. Però són segures aquestes aplicacions?

La informació que circula per ones, com les connexions Wifi, o per cable, **poden ser captades i interpretades molt fàcilment**. Hi ha molts programes a la xarxa que ho poden fer i milers de manuals que ho expliquen. Aquesta informació pot ser desvirtuada i generar confusió. Per això és necessari **enviar els missatges amb aplicacions de missatgeria que siguin segures**.

La seguretat en aquestes aplicacions es calcula, sobretot, en com s'envia la informació. Moltes aplicacions de missatgeria instantània, **envien la informació sense encriptar**. Això significa que el missatge, surt del dispositiu mòbil, idènticament com la persona l'ha escrit. Amb qualsevol programa es pot captar aquest missatge.

Perquè el missatge sigui segur, cal que **el programa encripti el missatge just abans d'enviar-lo**. Així, quan el missatge surt del dispositiu mòbil, surt en forma de números i caràcters indescriptibles. Si el missatge és escoltat per algú, no pot ser interpretat, ja que **no pot descriure correctament el contingut del missatge**. Quan el missatge arriba al destinatari, l'aplicació desencripta el missatge i la persona que el rep, el pot llegir, tal com l'emissor l'ha escrit. Això és l'encriptació punt a punt.

Hi ha algunes aplicacions que **no encripten el missatge quan surt de l'aplicació de l'emissor**. Aquest missatge pot ser captat i interpretat perfectament. Quan arriba al servidor de l'aplicació, aleshores sí que s'encripta el missatge. Aquest missatge s'envia al receptor, i l'aplicació del receptor, desencripta el missatge.

A continuació us descrivim **5 eines de missatgeria instantània** en els quals podreu comunicar-vos entre tots els vostres conciutadans. Algunes d'aquestes eines estan descrites a la [Guia d'Autodefensa digital de Softcatalà](#), la qual us recomanem la lectura.

[Telegram](#)

[Telegram](#) ja té uns quants d'activitat i és l'alternativa real a Whatsapp. Els clients (l'aplicació) de Telegram, **són codi lliure**. La part de servidor, no és codi lliure. Telegram disposa de canals de difusió unidireccionals que **han ajudat a posar una mica de calma als missatges no verificats**. Per defecte, Telegram no xifra els missatges punt a punt. Per a fer-ho, cada vegada que voleu escriure un missatge, **heu d'activar l'opció de «Xat secret nou»**. No queda clar, però, si els grups de Telegram, **utilitzen comunicació xifrada punt a punt**. Moltes d'aquestes converses, **queden guardades en servidors descentralitzats** en forma xifrada, però no es pot saber si s'ha enviat de forma xifrada.

[Signal](#)

[Signal](#) és una aplicació de missatgeria instantània, **totalment lliure i de codi obert**. [Signal](#) utilitza diversos protocols de comunicació que són **molt segurs i que preserven la privacitat**. Permet comunicacions xifrades punt a punt, és a dir, que el missatge es desxifra quan arriba al destinatari. [Signal no guarda cap missatge a cap dels seus servidors](#). De moment, [Signal](#) no s'utilitza molt i hi ha molt pocs usuaris i usuàries. [Signal](#) només es pot utilitzar des d'un dispositiu.

[Briar](#)

[Briar](#) és una aplicació de missatgeria instantània, de [programari lliure](#), en fase de proves. [Briar](#) utilitza **comunicacions xifrades punt a punt**. Tots els missatges que s'envien a través de [Briar](#), no passen **per cap servidor central**. Són guardats directament al dispositiu mòbil. Una de les particularitats que té [Briar](#), és que per enviar el missatge a una persona, primer heu de firmar un consentiment en mode [codi QR](#). [Briar](#), també pot enviar missatges **sense connexió Internet**.

[Whatsapp](#)

[Whatsapp](#) és una aplicació de missatgeria instantània que **no és codi lliure**. Utilitza comunicacions xifrades punt a punt, **però aquests protocols són propis**, i per tant no es poden estudiar per saber realment el grau de

seguretat. D'ençà que Facebook va comprar Whatsapp, moltes de les dades que s'obtenen de les converses, s'utilitzen per promocions i estudis a Facebook. Això és degut perquè les comunicacions **passen per un servidor central**.

[Firechat](#)

Sense voler-ho ser, [Firechat](#) es va convertir en una de les eines de comunicació que es van utilitzar [en les protestes civils de Honk Kong del 2014](#). [Firechat](#) té la particularitat d'utilitzar **un sistema de comunicació que no necessita Internet**. Mitjançant xarxes wifi o connexions Bluetooth, es poden **enviar missatges a altres usuaris de Firechat**. Firechat utilitza encriptació punt a punt.

Per a saber-ne més: [Guia d'autodefensa digital](#)

Etiquetes: [missatgeria instantània](#), [firechat](#), [WhatsApp](#), [telegram](#), [programari lliure](#), [aplicacions i programari](#)

URL d'origen: <https://xarxanet.org/informatic/noticies/5-aplicacions-de-missatgeria-instantania-segura>