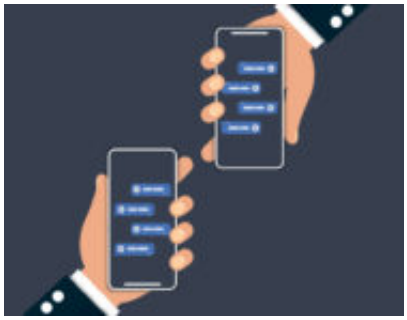
Messaggistica istantanea: quanto è sicura?

Author : Giorgio Sbaraglia

Date : 10 Febbraio 2020



La diffusione della Messaggistica istantanea (IM)

Oggi è cambiato il modo con il quale comunichiamo: sempre meno si usa il telefono (inteso come chiamata vocale) e sempre di più le **app per la messaggistica istantanea** (IM: *instant messaging*). Queste stanno - in parte - sostituendo anche le email, perché più veloci e pratiche.

I precursori della messaggistica istantanea sono stati - come tutti ricordiamo - gli SMS (sigla in inglese che significa *Short Message Service*). Comparvero negli anni Novanta (1993) quando la rete cellulare passò da ETACS al GSM (noto anche come 2G). Usavano infatti la rete cellulare, perché internet sui telefonini era ancora qualcosa di molto “rudimentale” e poco fruibile. E i nostri “telefonini” erano “feature phone[1]”, con caratteristiche e funzionalità molto basiche, ancora non erano diventati gli “smartphone” di oggi, potenti come veri computer.

L'uso dei messaggi SMS si è diffuso molto velocemente in tutto il mondo. Nel 2004 furono inviati, in tutto il mondo circa **500 miliardi di SMS**, che sono cresciuti nel 2008 fino circa 4.100 miliardi di SMS in un anno.

Ma alla fine del primo decennio del XXI secolo, la supremazia degli SMS come strumento di messaggistica istantanea viene messa in crisi – irreversibile - dalla comparsa di nuove applicazioni. **Nel 2009 nasce WhatsApp Messenger**, un'applicazione di messaggistica istantanea per smartphone multipiattaforma (cioè disponibile per i differenti sistemi operativi). A differenza degli SMS utilizza la rete internet e questo ha rappresentato un decisivo abbattimento del costo per l’utilizzatore.

Oggi WhatsApp (che nel 2014 fu acquistata da Facebook) è l’applicazione di messaggistica più diffusa nel mondo, con oltre un miliardo e mezzo di utenti attivi in 180 nazioni ed assieme alle applicazioni simili (Telegram, iMessage, WeChat, Signal, Facebook Messenger e molte altre) ha demolito il monopolio degli SMS, sempre meno utilizzati.

Infatti, già nel 2015, secondo uno studio dell'*Economist*, sono stati inviati mediamente ogni

giorno nel mondo circa 20 miliardi di SMS e **30 miliardi di messaggi** tramite WhatsApp.

Secondo un'indagine Audiweb, nel 2018 in Italia WhatsApp è stata usata da 31 milioni e 700 mila persone (+22% rispetto all'anno precedente).

Al secondo posto troviamo Facebook Messenger con poco più di 23 milioni di utenti mensili (+28% rispetto al 2017).

Seguono poi Telegram (9 milioni di utenti italiani, oltre 200 milioni nel mondo), Skype (3,5 milioni in Italia), Viber (840.000) ed iMessagge, l'app di Apple, utilizzabile solo sugli iPhone.

In grande crescita infine WeChat, l'app della cinese Tencent che nel mondo è utilizzata da oltre 1 miliardo di persone e che in Italia è particolarmente diffusa nella comunità cinese. Si differenzia dalle altre perché offre servizi molto avanzati che vanno oltre la semplice messaggistica (pagamenti diretti, prenotazioni, ecc.).

WhatsApp e sistemi di messaggistica istantanea: quanto sono sicuri?

L'Instant Messaging è diventato il sistema di comunicazione più diffuso e viene usato spesso anche per le comunicazioni aziendali, in alternativa all'email. Questo non è sbagliato, in termini di sicurezza, perché oggi tutti i sistemi IM implementano nativamente la crittografia *end-to-end* e ciò li rende **intrinsecamente più sicuri dell'e-mail**, che utilizza ancora protocolli di trasmissione come l'SMTP (Simple Mail Transfer Protocol) sviluppati negli Anni 80 e notoriamente insicuri.

Tuttavia, proprio a causa della loro enorme diffusione, sono diventate un **obbiettivo appetibile** anche per il *cybercrime*.

Non solo: si pone anche un problema di libertà, perché la vulnerabilità di queste applicazioni può mettere a rischio la libertà, la **privacy** e la sicurezza delle persone.

Le parole di Sherif Elsayed-Ali, direttore del programma «Tecnologia e diritti umani» di Amnesty International, ci fanno ben comprendere l'importanza del problema:

«Chi pensa che i servizi di messaggistica istantanea (IM) siano privati, si sbaglia di grosso: le nostre comunicazioni sono sotto la costante minaccia della cybercriminalità e dello spionaggio di stato. Sono soprattutto i giovani, i più inclini a condividere fotografie e informazioni personali su app di messaggistica, quelli più a rischio».

Per questo, Amnesty International ha redatto nel 2016 un rapporto denominato "FOR YOUR EYES ONLY[2]", dove ha esaminato le 11 aziende produttrici delle più popolari applicazioni di messaggistica. Ha assegnato valutazioni su una scala di punteggio da 0 a 100 rispetto a cinque parametri, fra cui il riconoscimento delle minacce online e l'utilizzo di default della crittografia end-to-end.

Il rapporto di Amnesty è rivolto soprattutto agli aspetti dei diritti umani e della **libertà di**

espressione, ma i risultati di questo studio ci devono far riflettere, perché riguardano anche l'utilizzo che ne facciamo noi tutti.

Anche EFF (Electronic Frontier Foundation, associazione che si occupa della difesa dei diritti della rete) ha analizzato le app di messaggistica. Questo studio è stato realizzato a novembre 2014 ed aggiornato fino ad aprile 2016, quindi oggi è da considerarsi superato (perché le app vengono continuamente aggiornate), ma è comunque un documento interessante che può essere consultato a questo link: https://www.eff.org/node/82654.

Non c'è solo WhatsApp

Sono molte le applicazioni IM presenti sul Play Store di Google e sull'AppStore di Apple e questa possibilità di scelta permette a chi è per davvero attento alla propria privacy di trovare interessanti soluzioni alternative a WhatsApp.

Questa rimane la più diffusa ma non certo la più sicura: non possiamo dimenticare che **WhatsApp appartiene a Facebook** (che l'ha acquistata nel febbraio 2014 per circa 19 miliardi di dollari!), il cui modello di business è basato sulla profilazione degli utenti, non certo sulla protezione della loro privacy…

WhatsApp è un'app pensata più per la praticità che per la sicurezza e la sua stessa grande diffusione la rende un obbiettivo da parte di ricercatori e cyber attaccanti che continuamente ne ricercano vulnerabilità da sfruttare. A maggio 2018 è stata scoperta una grave **vulnerabilità** di WhatsApp[3] che ha permesso alla società israeliana NSO Group[4] di spiare i cellulari di almeno 1.400 utenti tra il 29 aprile 2019 e il 10 maggio 2019.

Le vittime erano giornalisti, attivisti per i diritti umani, esponenti politici, dissidenti, diplomatici e alti funzionari governativi.

Questo caso ci fa capire che chiunque debba trattare informazioni delicate, non dovrebbe farlo usando un'applicazione commerciale e senza particolari requisiti di sicurezza qual è WhatsApp.

Vediamo dunque quali sono le **alternative** di IM più sicure che possiamo utilizzare per gestire comunicazioni riservate. Le scelte non mancano anche se molte di queste hanno come principale limite la loro scarsa diffusione.

Le principali applicazioni di messaggistica istantanea: caratteristiche e differenze

1. La crittografia end-to-end (E2E)

Oggi tutte le applicazioni di IM implementano la crittografia end-to-end (E2E), con la parziale eccezione di Telegram, come vedremo in seguito.

La crittografia end-to-end (letteralmente “da un estremo all'altro”) è un sistema di comunicazione cifrata dove solo il mittente ed il destinatario possono leggere i messaggi.

Serve ad impedire l’attacco *“man in the middle”* (MITM). Questi attacchi puntano a rubare dati e informazioni personali, intercettando *“in the middle”* la comunicazione tra due utenti.

La crittografia end-to-end si basa sulla **crittografia asimmetrica** (detta “a chiave pubblica”), realizzata mediante la generazione di una coppia di chiavi, una “privata” ed una “pubblica” che sono differenti, ma legate tra loro da un algoritmo che è stato inventato nel 1976 da Whitfield Diffie e Martin E.Hellman (si parla infatti di algoritmo Diffie-Hellman per lo scambio delle chiavi).

Il doppio paio di chiavi crittografiche (ognuno dei due utenti che si scambia il messaggio avrà due chiavi) è necessario per cifrare e decifrare i messaggi in partenza e in arrivo. Ogni utente utilizzerà una propria chiave pubblica e una propria chiave privata, La chiave privata è destinata a rimanere sul dispositivo di ciascuno dei due “endpoint” e servirà a decrittare i messaggi in arrivo; la chiave pubblica, invece, sarà condivisa con l’interlocutore e verrà utilizzata per crittografare i messaggi in uscita.

Grazie a questa tecnica le comunicazioni, pur viaggiando attraverso canali “aperti” e potenzialmente intercettabili, saranno leggibili solo dal dispositivo che ospita la chiave privata legata alla chiave pubblica utilizzata nel processo di crittografia.

Quindi, se una comunicazione è crittografata end-to-end è sicura. Ma questo **non significa che qualcuno non possa riuscire a leggerla**. Significa solamente che i suoi contenuti sono criptati nel percorso da un’estremità all’altra.

Ma se una delle due “estremità” viene compromessa, se il nostro telefono viene violato (per esempio con uno spyware, o captatore informatico, come quelli realizzati da NSO Group) o fisicamente confiscato dalla polizia e sbloccato, la crittografia non serve più a nulla.

Vediamo ora quali sono quali sono le app di messaggistica più diffuse e quali le più sicure.

2. WhatsApp

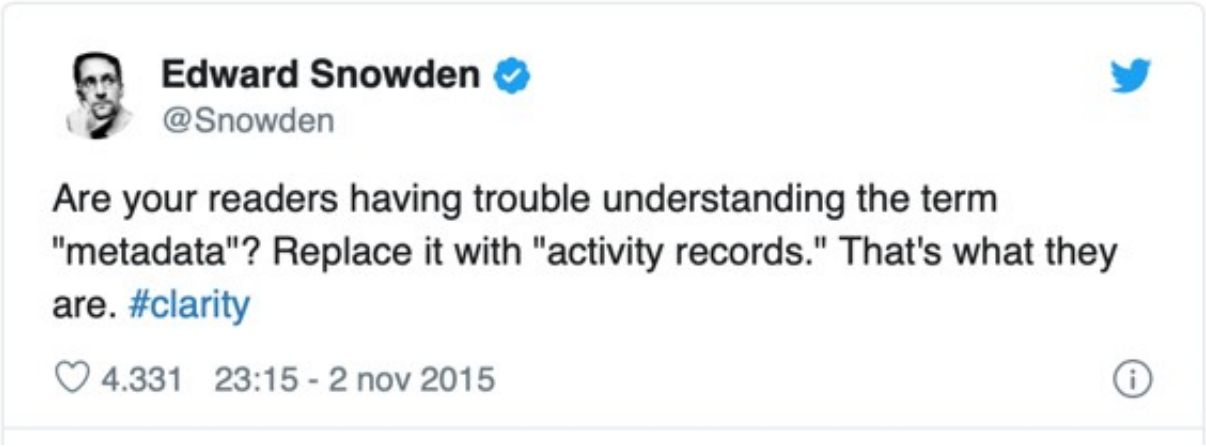
WhatsApp ha implementato la crittografia end-to-end (E2E) solo nel 2016 quando ha acquistato l’algoritmo di crittografia da Open Whisper Systems, la fondazione non-profit sulla quale torneremo in seguito a proposito di Signal.

Tuttavia WhatsApp presenta alcune caratteristiche che ne indeboliscono la sicurezza: quanto questo sia voluto, tenuto conto che parliamo di Facebook, non è facile saperlo…

I **Metadati**: il messaggio non è leggibile grazie alla crittografia E2E, ma WhatsApp ne conserva i metadati in forma non criptata. Questi metadati vengono salvati sui server di WhatsApp, che dichiara di farlo per migliorare la qualità del servizio.

Per capire cosa sono i metadati e perché non sono da sottovalutare, citiamo un tweet di Edward

Snowden[5]: *“Are your readers having trouble understanding the term "metadata"? Replace it with "activity records." That's what they are”.*



Dunque, nel caso di un messaggio i metadati sono, per esempio: data e ora di invio, i numeri di telefono del mittente e del destinatario, la loro localizzazione, ecc. Si tratta quindi di una “fingerprint” (impronta digitale elettronica) che aggiunge automaticamente dati identificativi che possono fornire ad un soggetto terzo informazioni importanti.

Backup delle chat: per impostazione predefinita, WhatsApp memorizza i messaggi in modo da consentirne il backup nel cloud di iOS o Android. Questo può essere comodo, nel caso un utente cambi smartphone. Tuttavia, se i nostri messaggi contengono informazioni riservate è consigliabile disattivare il backup della chat: WhatsApp permette di farlo sia in iOS che in Android, attraverso il menù delle impostazioni.

Consigliamo di farlo, perché - a differenza dei messaggi, che sono crittografati - i backup di WhatsApp sono in chiaro. Lo sono sicuramente in Android, mentre nel caso di iOS la crittografia ai backup in iCloud “dovrebbe” essere stata implementata alla fine del 2016, secondo quanto dichiarato da un portavoce di WhatsApp a *Forbes*[6].

Vedremo successivamente che le app considerate più sicure trattano i backup in modo migliore o - addirittura - non li permettono neppure, proprio per ragioni di sicurezza (come Wickr, Signal e Confide).

La formula dubitativa sulla forma dei backup in iCloud è motivata dal fatto che WhatsApp ha un codice proprietario (non *open source*) che non è accessibile per analisi da parte di terze parti. La non conoscenza del codice sorgente limita la trasparenza del prodotto e delle sue caratteristiche. In altre app (quali Telegram o Signal) abbiamo invece codice open source, che chiunque può esaminare.

Collegamento a Facebook: come detto, WhatsApp è stata acquisita da Facebook. Già nel 2016 era stato annunciato che i metadati degli utenti WhatsApp sarebbero stati condivisi con Facebook per vari scopi tra cui l'invio di pubblicità più mirata[7]. L’operazione è poi in parte

rientrata, per le proteste (e per le sanzioni dai garanti privacy europei), ma ben difficilmente Facebook rinuncerà ai suoi piani.

3. Facebook Messenger

Valgono le stesse considerazioni - e perplessità! - già espresse per il “fratello maggiore” WhatsApp. É anche possibile che Facebook intenda far convergere le due app in una sola.

Aggiungiamo che nel caso di Messenger la crittografia E2E non è di default e deve essere attivata dall’utente: è l’opzione "Conversazioni segrete” che Facebook ha reso disponibile nel 2016.

Quindi i messaggi inviati senza questa funzionalità vengono criptati solo per l'invio al server di Facebook e quindi una seconda volta per l'invio al destinatario (mentre la crittografia end-to-end avviene direttamente tra il mittente e il destinatario). Ciò significa che sui server di Facebook **rimane archiviata una copia dei messaggi**, quindi, se richiesto dalla legge, Facebook potrebbe consegnare i vostri messaggi. É lecito avere dei dubbi…

4. Telegram

Telegram rappresenta per diffusione uno dei principali concorrenti di WhatsApp, con oltre 200 milioni di utenti su iPhone e Android. È stata creata nel 2013 dai fratelli russi Durov, ma oggi è bandita in Russia, perché non ha voluto consegnare le chiavi di crittografia alle autorità russe. Telegram inoltre ha acquisito la fama (non certo positiva) di essere l’app di messaggistica preferita dall'ISIS.

Ha alcune funzioni molto pratiche, in particolare la possibilità di creare chat di gruppo con un massimo di 10.000 membri.

Per contro è una delle poche che non ha la crittografia E2E impostata di default: deve essere abilitata dall’utente, attivando le “chat segrete”[8]. In caso contrario, se non si utilizza una chat segreta, i dati vengono salvati sui server di Telegram e questa è un’opzione senz’altro meno sicura.

Inoltre Telegram utilizza un algoritmo di crittografia proprietario, MTProto[9], sul quale molti esperti hanno espresso scetticismo.

Telegram ha spiegato questa sua scelta[10], che considera più sicura delle chat di WhatsApp (*“La nostra roadmap è piena di funzionalità impossibili da costruire su un'architettura obsoleta come quella di WhatsApp”*).

Sicuramente ha il vantaggio, essendo basata sul proprio cloud integrato, di permettere l’accesso alla cronologia dei messaggi Telegram da diversi dispositivi contemporaneamente, perché sono salvati nei server.

Il codice sorgente comunque è open source e chiunque lo può esaminare.

In conclusione: è sicuramente un prodotto di messaggistica molto pratico e ricco di funzionalità, che non è sottoposto alle logiche commerciali che caratterizzano WhatsApp. Non può essere considerato però il migliore in termini di sicurezza.

5. Apple iMessage

iMessage è il sistema IM proprietario di Apple, che funziona solo in iOS.

É crittografato E2E e si affida ad Apple iCloud per memorizzare la cronologia dei messaggi degli utenti e prevenire la perdita di dati nel caso in cui questi perdano il loro smartphone. I messaggi criptati rimangono archiviati nei server di Apple per sette giorni prima di essere eliminati.

É importante sapere che vengono crittografati solo i messaggi tra gli utenti di iOS (quelli con il fumetto blu). Un messaggio ad un utente di Android verrà inviato come SMS normale (in verde) senza crittografia.

Il codice sorgente è segreto.

iMessage esegue il backup in iCloud, ma lo fa in forma crittografata (e l'esecuzione di questo backup può essere disattivato nelle impostazioni di iOS).

6. Signal: consigliata da Edward Snowden

Signal[11] è l'applicazione di messaggistica che gode della miglior reputazione tra gli esperti di sicurezza. È quella preferita da Edward Snowden, che ha affermato: *"Use anything by Open Whisper Systems"*. È consigliata anche dal famoso crittografo americano Bruce Schneier.

Signal è stata creata da da **Moxie Marlinspike** con Open Whisper Systems, una fondazione non profit che sviluppa software open source per la sicurezza delle comunicazioni.

Marlinspike è tra i maggiori esperti mondiali di crittografia e sicurezza informatica oggi viventi. Dopo essere stato a capo della sicurezza Twitter, ha creato Open Whisper System, che si finanzia esclusivamente con donazioni, non richiede alcun pagamento ed è priva di pubblicità. Oggi è finanziata anche da **Brian Acton** (co-fondatore nel 2009 di WhatsApp assieme a Jan Koum). Acton è uscito dal gruppo Facebook-WhatsApp nel 2017 per fondare la **Signal Foundation**[12] e nel 2018, dopo lo scandalo di Cambridge Analytica, ha dato vita al movimento **#DeleteFacebook**.

Signal utilizza un protocollo di crittografia E2E denominato **Signal Encryption Protocol** ideato da Marlinspike e considerato più sicuro anche del protocollo PGP (Pretty Good Privacy).

Questo stesso protocollo è stato implementato da aprile 2016 anche in WhatsApp e successivamente in Skype.

Ma Signal garantisce un livello di privacy e sicurezza superiore a WhatsApp, per i motivi che

andiamo a illustrare:

- **metadati**: Signal - a differenza di WhatsApp - memorizza solo i metadati necessari per il suo funzionamento, quindi il numero di telefono, la data di creazione dell'account e l'ora dell'ultima connessione ai server di Signal; non salva alcuna informazione relativa alla conversazione. Inoltre non salva questi metadati dei messaggi sui propri server (come fa invece WhatsApp). I numeri di telefono vengono trasmessi al server in forma crittografata.
- **Backup**: sempre per ragioni di sicurezza, in Signal i messaggi sono memorizzati localmente sul dispositivo e non vengono neppure salvati nel backup di iCloud (nel caso di iPhone). Solo in Android è disponibile una funzione di esportazione che può essere utilizzata esclusivamente per trasferire i messaggi da uno smartphone ad un altro. Per questo, se qualcuno chiedesse a Open Whisper di fornirgli i dati di un utente, questa non potrebbe darglieli, semplicemente perché non li ha.
- **Codice sorgente**: quello di Signal è pubblico, secondo la logica dell'open source, quindi accessibile per analisi, mentre quelli di WhatsApp e di iMessage - in quanto prodotti commerciali - non lo sono.
- **Audit**: Signal è stato sottoposto, già nel 2016, ad un audit di sicurezza da parte di un team indipendente[13].

Signal si basa su un software open source ed ha ora sviluppato anche una versione desktop che - come l'app - può essere utilizzata per inviare e ricevere messaggi privati, di gruppo, allegati e messaggi multimediali.

Si tratta ancora di un'app di nicchia, con una diffusione piuttosto limitata. Non ci sono dati relativi ad iOS, ma si stima che nel mondo Android sia stata scaricata nel Play Store da non più di cinque milioni di utenti nel mondo.

L'approccio di sicurezza di Signal (che non permette il backup della chat) ne rappresenta una barriera di ingresso per quei tanti utenti che non vogliono perdere tutta la loro storia di messaggi quando/cambiano i loro telefoni.

Quindi le applicazioni di questo tipo non diventeranno mai molto popolari, perché l'utente medio continuerà a preferire la praticità d'uso e la diffusione rispetto alla sicurezza (purtroppo!)

7. Le altre applicazioni di messaggistica

Esistono altre applicazioni IM che sono considerate tra le più sicure, ma che hanno una diffusione ancora minore di Signal.

Citiamo le migliori, che sono:

Wire[14] (di Wire Swiss GmbH): è gratuita e disponibile anche in versione desktop (per Windows e macOS). Ha anche le versioni Pro ed Enterprise a pagamento con funzionalità aggiuntive.

Wire si distingue per la qualità delle chiamate vocali e video e la possibilità di uso simultaneo su 8 dispositivi. Il codice è open source.

Threema[15] (di Threema GmbH): ha un software proprietario ed è a pagamento. Non salva metadati e non comunica le informazioni relative al messaggio (mittente, destinatario, ora di invio e ricezione, ecc.). I server di Threema si trovano in Svizzera e sottostanno alle rigide regole di protezione dei dati vigenti sul territorio svizzero. Diffusione: 4,5 milioni di utenti (dati aggiornati al 2018).

Wickr[16]: disponibile per iPhone e Android (non esiste la versione desktop), offre una versione per uso personale (Wickr Me) e una per professionisti e aziende (Wickr Pro). Wickr Me è gratuita, mentre Wickr Pro è un servizio a pagamento.

Implementa la crittografia E2E anche sulle chiamate e sulla messaggistica vocale.

Ha la funzione di Rilevamento degli screenshot e la funzionalità Secure Data Shredder per accertarsi che i file già eliminati non siano recuperabili con strumenti o tecnologie particolari (in

pratica un “distruggi- documenti”).

Il codice sorgente è stato reso disponibile su GitHub[17].

Confide[18]: disponibile per iPhone e Android. Esiste anche la versione desktop per Windows.

Oltre ad usare la crittografia E2E, ha una caratteristica che la contraddistingue: una volta letto, il messaggio si autodistrugge e con esso tutti gli allegati, comprese le registrazioni vocali. Inoltre il messaggio non viene visualizzato per intero, ma solo per singola parola, che viene resa visibile trascinando il dito sopra, mentre le altre parole rimangono oscurate. Questa è un’efficace protezione contro gli screenshot, suggestiva ma in realtà abbastanza poco pratica.

Silent Phone[19]: disponibile per iPhone e Android (non esiste la versione desktop), ma a pagamento. Chiamate crittografate con qualsiasi dispositivo iOS, Android o Silent OS.

Messaggistica di gruppo, videochiamate e videoconferenza. Condivisione sicura di file, foto, video all'interno di gruppi.

Line[20]: creata nel 2011 in Giappone dalla Naver Corporation, permette di fare chiamate vocali (anche di gruppo) e videochiamate. Ha caratteristiche che la rendono un’alternativa a WhatsApp, con funzioni simili a quelle dei social network. Dal punto di vista della sicurezza non è considerata tra le migliori, ma è tra le più diffuse (l’azienda ha dichiarato che sono stati raggiunti i 700 milioni di utenti attivi in tutto il mondo nel 2015).

Viber[21]**:** rispetto alle altre app, si contraddistingue per un alto numero di utenti (circa un miliardo), risultando così un'alternativa a WhatsApp.

Permette di effettuare chiamate vocali di alta qualità, videochiamate, inviare messaggi di testo, foto e condividere luoghi con altri utenti Viber. È gratuita, ha anche la versione desktop. Il codice è proprietario. Conserva i metadati ed anche per questo non è considerata tra le più sicure in termini di privacy.

Note

[1] Con questo termine si intendono i telefoni cellulari privi delle funzionalità avanzate degli smartphone.

[2] https://www.amnestyusa.org/reports/for-your-eyes-only/

[3] https://www.cybersecurity360.it/nuove-minacce/spiare-whatsapp-le-tecniche-per-sbirciare-nelle-chat-altrui-e-i-consigli-per-metterle-in-sicurezza/

[4] https://www.nsogroup.com

[5] https://twitter.com/Snowden/status/661305566967562240

[6] https://techcrunch.com/2017/05/08/whatsapp-quietly-added-encryption-to-icloud-backups/

[7] https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp

[8] https://telegram.org/faq#q-how-do-i-start-a-secret-chat

[9] https://core.telegram.org/mtproto

[10] https://telegra.ph/Why-Isnt-Telegram-End-to-End-Encrypted-by-Default-08-14

[11] https://signal.org

[12] https://signal.org/blog/signal-foundation/

[13] https://www.cyberscoop.com/signal-security-audit-encryption-facebook-messenger-whatsapp/

[14] https://wire.com/en/

[15] https://threema.ch/en

[16] https://wickr.com

[17] https://github.com/WickrInc/wickr-crypto-c

[18] https://getconfide.com

[19] https://www.silentcircle.com/products-and-solutions/silent-phone/

[20] https://line.me/it/

[21] https://www.viber.com/it/

Articolo a cura di **Giorgio Sbaraglia**