imparailpc

Il marchio e il logo sono regolarmente registrati e di esclusiva proprieta' di imparailpc.

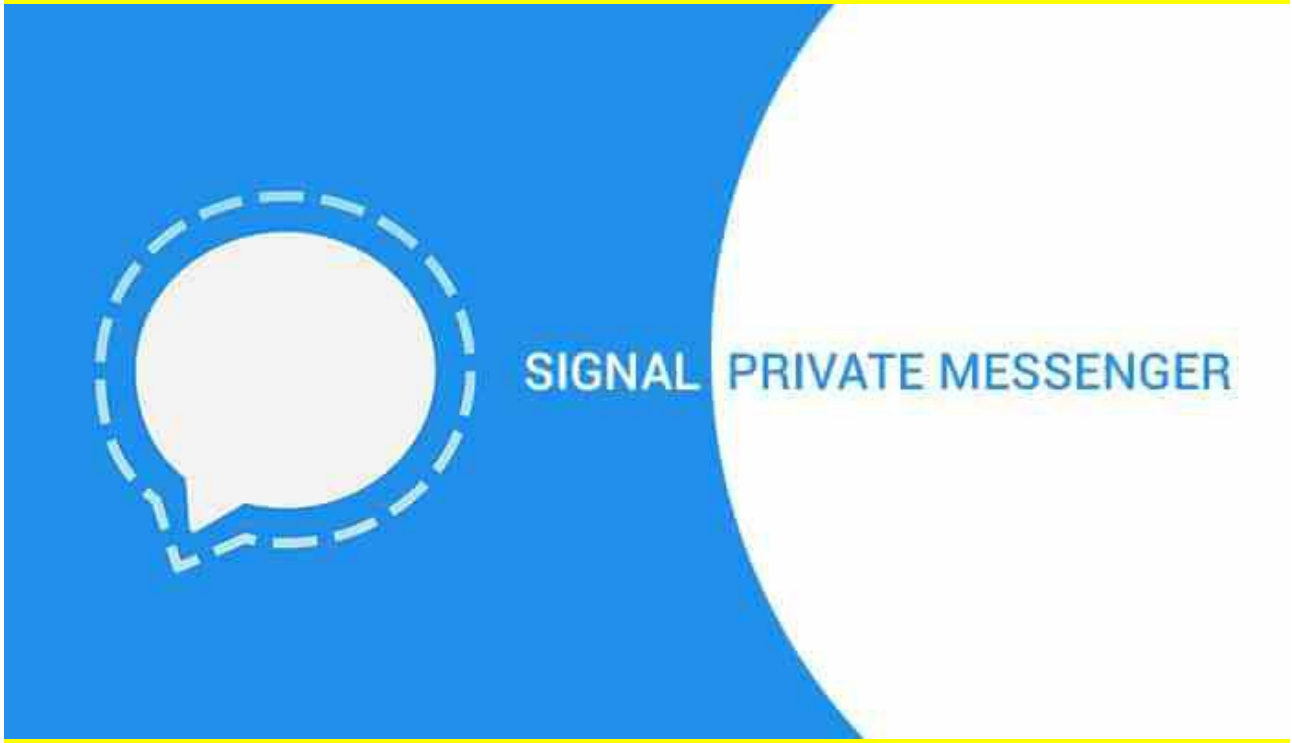
Ogni utilizzo, è di esclusiva proprieta' del titolare.

Primo numero in uscita

3 GENNAIO 2019

Fonte immagini: Google.

Signal Private Messenger

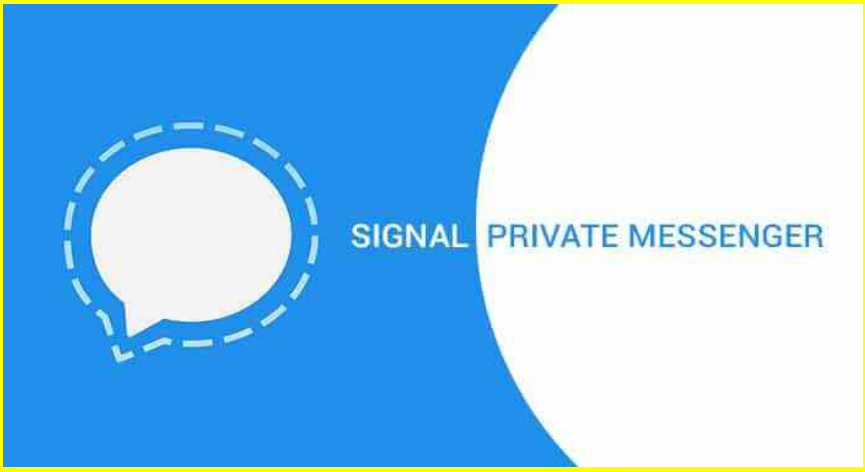


Signal Private Messenger, forse a molti non dira' molto, ma si tratta, dell' applicazione piu' sicura sul mercato, almeno allo stato attuale.
Signal, è nata nel 2010, in un mondo in cui le app, erano ancora sconosciute alla massa, ed è stata poco considerata, almeno per i primi 3 anni di vita.
Nel 2013, quando è scoppiato lo scandalo Datagate, con le rivelazioni di Edward Snowden, sullo spionaggio di massa da parte della NSA e del governo americano, ai danni di ignari cittadini innocenti, Snowden, dopo essere rifugiato in Russia, ha inserito Signal, negli strumento di autodifesa digitale.

Da quel momento, l' app, ha iniziato ad avere una crescita importante, che oggi ha superato i 10 milioni di utenti.

Logo Signal Private Messenger

In un documento interno, tra quelli trafugati da Snowden, si legge chiaramente, che il governo americano, è preoccupato per l' utilizzo di Signal, perchè impossibile da intercettare, tanto che pare che l' app, sia stata discussa alla casa bianca.
Ma Signal, non è stata fondata da uno qualunque, ma niente di meno che da Moxie Marlinspike, uno tra gli uomini piu' professionali al mondo, che ha inventato la crittografia end-to-end, e che ha lavorato anche per Twitter, come capo della sicurezza.
Come se non bastasse, dopo che il co-founder di Whatsapp, Brian Acton, ha lasciato il suo incarico a Facebook, proprio per divergenze interne in termini di privacy, ha deciso di investire ben 50 milioni di dollari, in Signal, per mandare avanti l' app, che è una no-profit tutt' oggi.



Signal, è disponibile anche in versione Desktop, scaricabile gratuitamente, ed utilizzabile tramite lo scan del QR Code, con il proprio device.

Ma passiamo al lato tecnico dell' app, che è sicuramente la parte piu' importante di tutte:

Signal, utilizza la crittografia end-to-end, per ogni messaggio, e per le chiamate

effettuate tramite l' app, tra utenti iscritti al servizio, con il proprio numero telefonico, ma è progettata, per rilasciare il minor numero di dati, che attualmente, sono 3, di cui 1, facoltativo.
I 3 dati che possono essere intercettati o che possono essere richiesti da un giudice, in caso di un eventuale processo, sono: l' ultimo accesso effettuato all' app, il numero telefonico dell' utente, e la lista dei contatti, ma solo l' utente ha attivato la sincronizzazione col server.
Solo questi 3 dati, sono rintracciabili tramite l' app, ed è appunto, talmente sicura, che nemmeno la Signal Foundation, la no-profit che controlla Signal, ha in mano le chiavi per decriptare i messaggi degli utenti.

L' unico modo con il quale le autorita' possono rintracciare una conversazione avvenuta tramite Signal, è quello di avere accesso fisico, al device in questione, per le chiavi crittografiche, vengono generate sui dispositivi, e non sul server, che non ha nessuna possibilita' quindi, di rilasciare alcun dato.

Schema semplice di come transita un messaggio criptato.

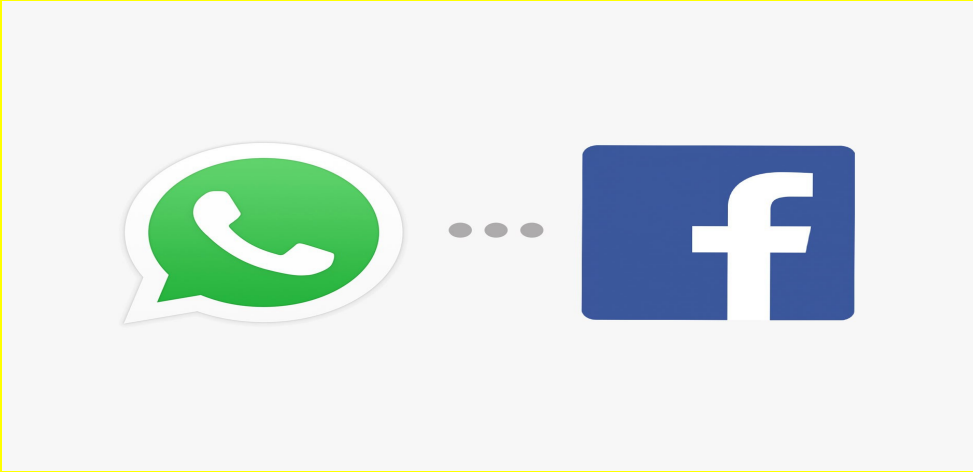
Gli utenti, possono anche attivare l' autodistruzione di un messaggio, in modo che dopo un preciso lasso di tempo, si autodisgrugga in maniera automatica, e Signal inoltre, non esegue mai il backup delle conversazioni, a meno che non sia l' utente a farlo manualmente, e solo su scheda SD, per la quale viene rilasciata una precisa chiave crittografica, per poterle poi riaprire.
La EFF, ovvero l' Electronic Frontier Foundation, ha inserito Signal, nella lista delle app, per l' autodifesa digitale.
Inoltre, Signal Private Messenger, è totalmente open source, il che significa che chiunque, puo' controllare il codice, per verificarne l' integrita'.
Che aspetti? Prova Signal Private Messenger adesso, scaricala gratuitamente dallo store del tuo Android, o da Apple Store se hai iOS!

Whatsapp: La regina delle app è sicura?

Logo Whatsapp

Whatsapp: il solo nome, non ha piu' segreti, tanto che ormai, l' applicazione regina indiscussa della messaggistica, ha oltre 1,5 miliardi di utenti in tutto il mondo. Whatsapp, è stata fondata nel 2009, da due ex dipendenti di Yahoo!, Jan Koum e Brian Acton.

Il primo ad aver avuto l' idea, è stato Koum, che ha iniziato fondando Whatsapp dal nulla, ma i primi periodi, non sono stati facili, perchè l' app, continuava ad avere crash improvvisi.
Dopo poco dalla creazione pero', fu l' Apple Store di Apple, che involontariamente, diede a Koum, la possibilita' di avanzare con l' app, perchè introdusse, le notifiche push, assenti in precedenza.
Whatsapp, fu lanciata sul mercato, e come hanno sempre detto i suoi fondatori, senza nessuna operazione di marketing, l' app, fini' tra i top trend di Apple Store.
La scelta di non fare pubblicita', non fu casuale, perchè Koum e Acton, sono fermamente convinti, che la pubblicita', non semplifichi la vita delle persone, tanto che inizialmente, l' app è stata lanciata in forma gratuita nello store di Apple.
Dopo che Whatsapp riscosse successo, vennero introdotti gli abbonamenti, tra cui i famosi 89 centesimi/annui, per utilizzare il servizio, fino ad arrivare al 2014, quando fu Mark Zuckerberg, fondatore e amministratore delegato di Facebook, che decise di acquistare l' app, per ben 19 miliardi di dollari.



Whatsapp è sotto il controllo d Facebook dal 2014 e le due societa' sono unite

Ma passimo al lato tecnico dell' app: Whatsapp, ha introdotto da

tempo, la crittografia end-to-end, per rendere i messaggi, totalmente criptati e sicuri, illeggibili da estranei, ma sara' veramente cosi'?

La risposta, è no, perchè infatti, sebbene Whatsapp adotti la crittografia, ha un funzionamento sul lato tecnico, che la rende vulnerabile.

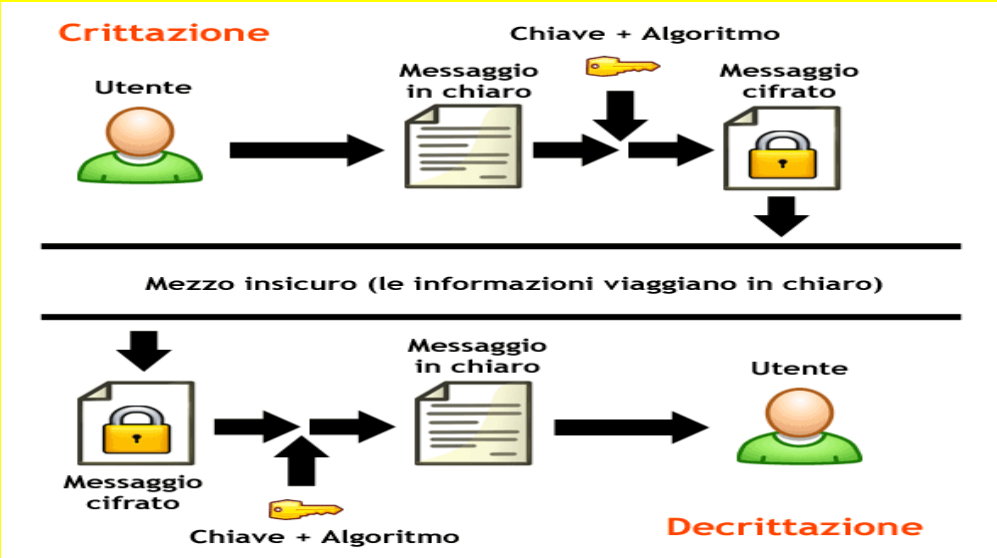
Whatsapp, quando un messaggio viene inviato ad un utente, rilascia una chiave crittografica, sul server di Facebook, che quindi, ha in mano la chiave per decriptare il messaggio in questione.
Ma come se non bastasse, Whatsapp rilascia anche metadati, come la posizione GPS di un utente, l' indirizzo ip, ed ovviamente, questo rende tracciabile un utente, nel corso del tempo.
Inoltre, se qualcuno dovesse subire un processo, il giudice potrebbe chiedere a Facebook, di consegnare il messaggio decriptato, visto che la chiave crittografica, rimane sul server dello stesso Facebook.

Sebbene sia l' app piu' utilizzata al mondo, Whatsapp, non è sicura, e rende la privacy delle persone molto vulnerabile, come lo stesso co-fondatore, Brian Acton, che dopo essersi dimesso proprio da Whatsapp, in una intervista a Forbes, ha dichiarato di aver non solo venduto l' app a Facebook, ma di essersi reso conto, che la privacy degli utenti, e' a rischio, tanto che lo stesso Acton, ha investito ben 50 milioni di dollari, per Signal, l' app piu' sicura sul mercato al momento.

Messaggio che un utente legge quando apre una nuova conversazione su Whatsapp

Nello schema qui sotto, nella parte in alto, possiamo vedere il funzinamento della crittografia in generale, che vale anche per Whatsapp, con una spiegazione molto semplice:

Il messaggio che parte da un utente, come si vede in figura sotto, nel transito fino al destinario, si ferma sul server, e seppure in maniera criptata, cioè rende il messaggio molto insicuro perchè chi gestisce il server, ne avra' accesso.



Schema di invio messaggio in maniera criptata e non.

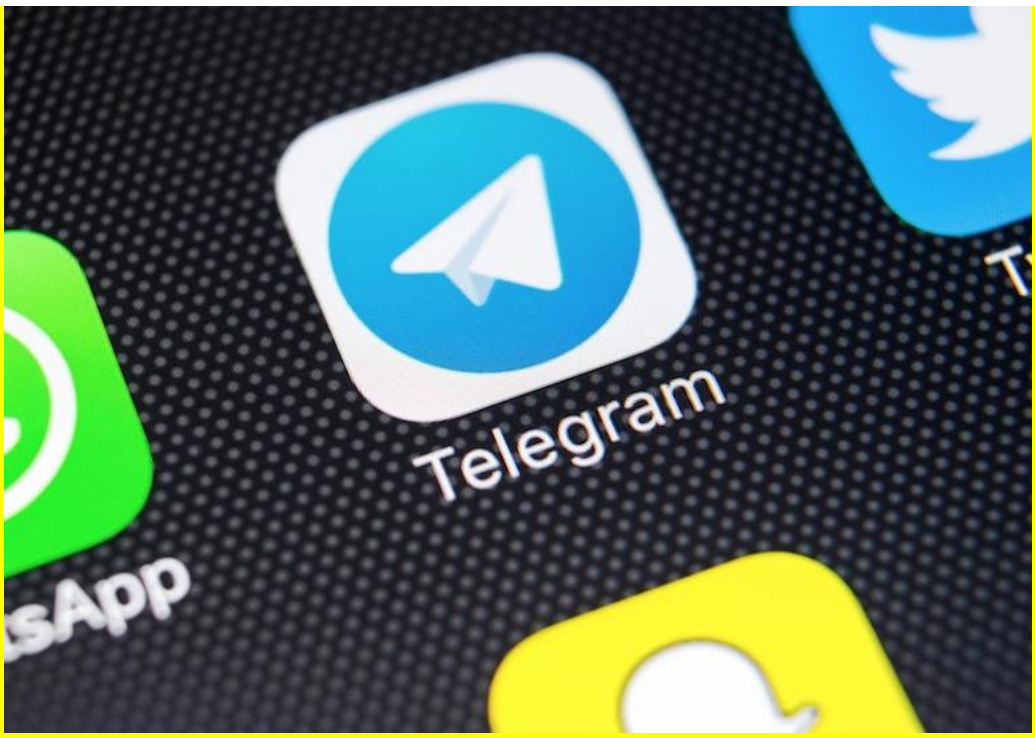
Nella parte sotto della figura , si nota invece come viene inviato un messaggio, che non è minimamente protetto da crittografia, e che quindi, è ancora piu' intercettabile, in quanto non è protetto in alcun modo.

Telegram: L' app russa protegge i dati degli utenti?

Logo Telegram

Telegram, l' app russa, è ormai nota al grande pubblico, ma quello che viene da chiedersi, visto che proprio Telegram, è entrata sul mercato come app che protegge la privacy degli utenti, ma ha alcuni aspetti, che fanno discutere in merito.

Telegram, nasce come applicazione di messaggistica, in un mercato dove non è facile arrivare, visto che la concorrente numero 1, è Whatsapp, usata ogni giorno da milioni e milioni di persone, pertanto, Telegram, entrando sul mercato, ha adottato una tecnica molto interessante, ovvero la protezione della privacy.



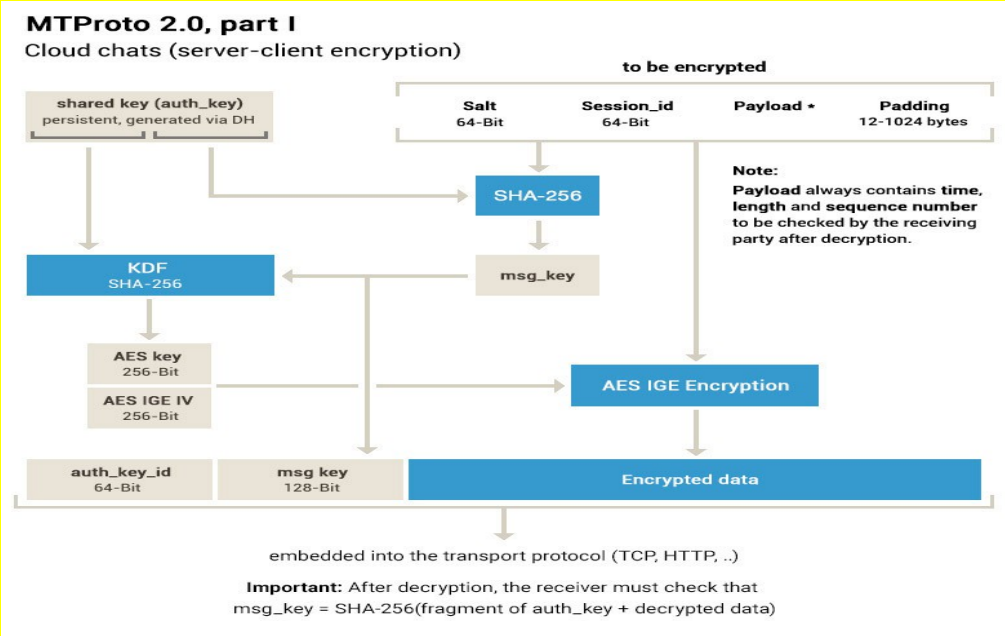
Le funzionalita' di Telegram ad oggi, sono sicuramente molto interessanti, e rendono l' app, molto ampia, anche molto piu' vantaggiosa della concorrente Whatsapp, per alcuni aspetti molto interessanti.
In primis, i gruppi, che su Telegram possono toccare ben 75 mila utenti, ad oggi,

cosa che su Whatsapp, non puo' avvenire, ma che pero', è comunque inferiore a Viber, che permette di creare gruppi, fino ad 1 miliardo di utenti.
Altra funzione interessante, sono i canali, ovvero la possibilita', di potersi creare l' apposito spazio nell' app, dove postare le notizie, oppure seguire le notizie di altri, senza possibilita' di interazione con l' admin, che quindi pubblica le notizie senza ricevere alcun commento da parte degli iscritti.

In ultimo, Telegram permette anche l' invio di file di grandi dimensioni, fino ad 1,5 GB, cosa che non è permessa sulle altre app, attualmente presenti sul mercato.

Telegram inoltre, permette anche di poter attivare le chat che si autodistruggono, esattamente come avviene su Signal, ed è sicuramente una funzionalita' molto interessante per gli utenti, ma analizzando il lato tecnico dell' app, in merito alla privacy, si riscontra, una anomalia.

Per cominciare, occorre precisare che Telegram, adotta la crittografia end-to-end, solo per le conversazioni segrete (attivabili dall' utente), e non di default, perchè viene implementato, il protocollo MT PROTO.



Funzionamento protocollo MT PROTO visionabile sopra.

Per chi non fosse a conoscenza, o non avesse praticita' con questo genere di argomento, basti pensare che il protocollo MT PROTO, non è ritenuto uno standard affidabile totalmente, esattamente come invece avviene, sulla crittografia end-to-end.

Telegram, si puo' ritenere sicuro, solo in parte, in quanto non è completamente open

source, ovvero:

Il lato client dell' app, è open source, ovvero visionabile da chiunque ne voglia verificare l' integrita' e la funzionalita' effettiva, mentre il lato server dell' app, che gioca un ruolo fondamentale in termini di sicurezza informatica, non è rilasciato, pertanto non è visibile agli occhi degli utenti, se effettivamente la conversazione, viene criptata in maniera corretta o meno.

Telegram, è comunque una applicazione, che si attesta ad essere la futura sostituta di Whatsapp, anche se per battere la concorrenza, dovra' fare ancora molta strada.

Telegram, ha sicuramente molte potenzialita' da poter sfruttare, ma l' operazione di marketing che ha avuto dal suo inizio ad ora, e che ha giocato un ruolo fondamentale per far arrivare quest' app abbastanza in alto, sarebbe sicuramente un ottimo sistema di farla conoscere al pubblico, se non fosse, che Telegram ha sempre ritenuto di essere la numero uno del settore privacy, tutelando gli utenti, ma analizzando la situazione, a livello tecnico-informatico, purtroppo Telegram, non ha tutte quelle caratteristiche, che deve avere una applicazione, per essere ritenuta sicura.

In ogni caso comunque, occorre dare atto, che solo nel mese di Marzo 2018, Telegram è riuscita ad avere bene 700mila nuovi utenti ogni 24 ore, e sicuramente è un risultato che non è da tutti facilmente raggiungibile, sintomo che evidentemente le persone, trovano in Telegram, una fonte importante di interazione.

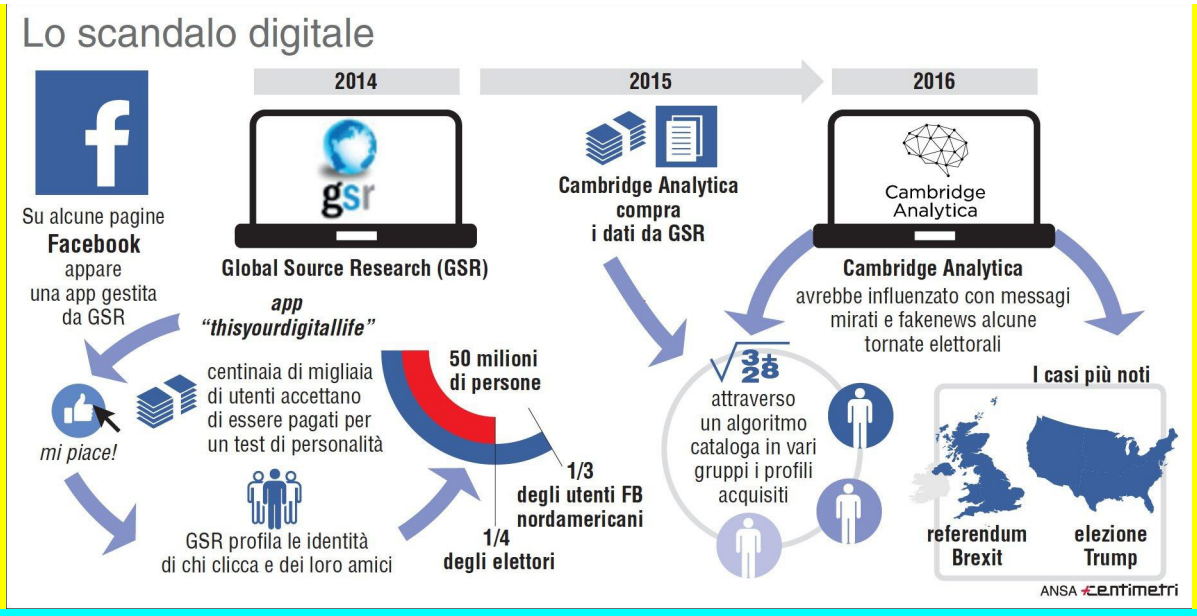
Telegram è utilizzato da 200 milioni di persone

Facebook: gli scandali non fermano il social network

Facebook, il re indiscusso dei social network, è ormai la piattaforma social, sovrana nel web, con oltre 2 miliardi di utenti iscritti, ogni parte del globo, o quasi.

Il social pero', è stato coinvolto in numerosi scandali sulla privacy, che hanno piu' volte messo in ginocchio il social, almeno in un primo momento, per poi risollevarsi sempre.

Gli scandali, sono davvero molti, e riguardano lo spionaggio di massa ai danni degli utenti, come l' ormai famoso spionaggio di Cambridge Analityca, che ha coinvolto ben 87 milioni di utenti in tutto il mondo, con dati spiati, e venduti per vari scopi, sia in cambio di soldi ad inserzionisti, sia ad altre societa', per influenzare il pensiero delle persone, anche in merito alla campagna elettorale in America, che ha visto ormai la vittoria di Trump.



Lo schema, identifica il funzionamento di influenza di Cambridge Analytica tramite Facebook per influenzare le elezioni americane.

Facebook, è stato piu' volte chiamato a dare una risposta agli utenti, ed ogni volta, il suo fondatore Zuckerberg, sia è scusato, sebbene poi abbia ripetuto l' errore piu' e piu' volte.

Il funzionamento strutturale di Facebook, non è noto a tutti, ma andremo adesso a vedere insieme, in maniera semplice, come funziona.

Un utente si iscrive al social, immettendo i propri dati personali, quale mail, nome, cognome, numero telefonico e via dicendo, ed inizia ad utilizzare la piattaforma normalmente, ignaro di cio' che effettivamente accada sotto, sui server, dove nessun occhio, se non quello di Facebook stesso, arriva.

I dati degli utenti, vengono inviati ad un database, che li contiene, e poi vengono analizzati, preparati per essere ceduti ad inserzionisti, cioè coloro che hanno attivita', e cercano clienti.

Le societa' controllare da Facebook, in figura sopra.

Questo avviene con Facebook, ma anche con le societa' che quest' ultimo controlla, come si vede nella foto sopra, quindi Messenger, Whatsapp, ed anche Instagram.

Nessun dato viene lasciato al caso, ed ognuno degli utenti, è una potenziale cavia da laboratorio, che fa comodo al social.

Anche i big, come Elon Musk, l' imprenditore miliardario, Steve Wozniak, co-founder di Apple, e Brian Acton, co-founder di Whatsapp, hanno invitato gli utenti, ad abbandonare il social network.

Nonostante pero' tutte le problematiche, gli utenti sono calati, ma non in grande misura, ed il social infatti, dopo un trimestre dallo scandolo sulla privacy, ha chiuso con un +49%, quindi è sintomo evidente, che la piattaforma non ha risentito piu' di tanto della problematica.

Anche Messenger, la piattaforma chat di Facebook, ha non poche problematiche, sopratutto legate alla privacy.

E' risaputo infatti, che i messaggi scambiati sulla piattaforma, non adottano di default la crittografia, e sono letti dal team dello stesso Facebook, senza alcuna privacy degli utenti.

Il logo di Facebook Messenger

L' unica scelta, sarebbe quella di togliersi dal social network, perchè restringere al massimo la privacy, non serve, anche perchè esistono molti modi per poterla aggirare, senza contare il fatto, che molte delle foto messe sul social, possono anche essere rimesse in vendita nel dark web, la parte sommersa della rete.

Allora, sei ancora sicuro di voler utilizzare Facebook?

Contatta imparailpc e facci sapere quali argomenti vorresti fossero trattati nei prossimi numeri!!!!!!

scrivi una mail a

impossibile@protonmail.com

Il prossimo numero è in uscita

Giovedi 10 Gennaio 2019

Alle ore 11