

Guida a Telegram: Telescope, Telegraph e la sicurezza dell'App

Telegram e la rivoluzione Instant View: di questo parlavamo nell'ultimo appuntamento della nostra Guida all'App fondata da **Pavel Durov**. Le novità però, dicevamo, non finiscono qui. altre *features* fondamentali per Telegram sono i Videomessaggi e la piattaforma Telescope, nonché Telegraph, la piattaforma di blogging proprietaria di Telegram, importante quanto lo è Pulse per **LinkedIn**, le Note per **Facebook**, o ancora la stessa piattaforma Medium.

Di che cosa si tratta? Andiamo con ordine.

Videomessaggi e Telescope

«L'aggiornamento di **Telegram** alla versione 4.0 include due delle maggiori novità: Telescope e *video messages*», si scrive sul blog il 18 maggio 2017 quando, appunto, vengono lanciati altri due updates fondamentali, il Pagamento via Bots e la già vista Instant View Platform. «Sappiamo quanto ami la velocità e la semplicità dei messaggi vocali su Telegram. Da oggi puoi mandare anche video messaggi. In qualsiasi chat di Telegram, tieni premuta l'immagine della videocamera e registra il tuo video messaggio. Quando sarà pronto, rilascia semplicemente il pulsante di registrazione: il messaggio partirà e arriverà in un batter d'occhio».

Una delle caratteristiche principali di tali video messaggi, infatti, è ancora una volta la velocità: «Telegram li comprime e li manda non appena li registri». E se invece ne ricevo uno? «Puoi continuare a guardarlo mentre navighi tra le altre chat. Il video resterà aperto in un angolo».

Come anticipato, però, c'è di più: «Ti presentiamo Telescope», continuano, «una piattaforma di video dedicata a quanti usano i video per comunicare con amici e contatti in rete – questa è fatta apposta per voi, blogger! Con Telescope i video messaggi pubblici possono diffondersi viralmente oltre l'ecosistema Telegram». In altre parole, Telescope è una piattaforma pubblica, ovunque accessibile sul Web a prescindere che si abbia o no l'applicazione. «Sì, hai sentito bene», precisano. «Non occorre un account Telegram per vederli».

«i video potranno avere durata massima di un minuto: lo stesso formato che utilizziamo per i video messaggi su Telegram. Inoltre, ogni canale pubblico adesso avrà una *telesco.pe* URL come questa: *telesco.pe/channel_name*. Qui tutti i video messaggi sono disponibili per il *world wide web*». E, aggiungono con la consueta ironia, «per il *wide, wide world*».

Ogni volta che posterai un video messaggio su un canale pubblico, questo sarà caricato automaticamente su Telescope ed avrà lì la sua URL pubblica». Così tutti i tuoi amici potranno goderselo e dividerlo sugli altri social. Vuoi mettere in termini di diffusione e popolarità acquisita? I tuoi contatti aumenteranno di certo.

Telegraph

Non è finita. Grande giorno quel 22 novembre 2016: insieme a Instant View, viene annunciata anche un'altra rilevante novità. «Oggi lanciamo Telegraph», scrivono entusiasti, «uno strumento di publishing che ti consentirà di creare post formattati come vuoi con foto e ogni tipo di contenuto embeddato. I post che scriverai su Telegraph appariranno particolarmente belli grazie alla funzione Instant View». In altre parole:

- Telegram si crea così il suo «Medium» personalizzato, il suo «LinkedIn Pulse», la sua piattaforma di blogging, peraltro fruibile da chiunque, non solo da chi abbia scaricato l'applicazione ma accessibile sul Web come qualsiasi altra piattaforma di pubblicazione, testata o blog, diffondendo viralmente così la conoscenza dello strumento;
- In occasione dell'uscita, Telegram rende particolarmente bello questo suo nuovo tool con un make-up davvero speciale, lanciandolo insieme alla funzione instant View e consentendo così alla sua piattaforma di blogging di beneficiare per prima o quasi della funzione apertura rapida tipica di Instant View;
- «Prova tu stesso», esortano. «Va' su telegra.ph, pubblica una storia e condividila su Telegram. Con Telegraph, il tuo canale Telegram potrà raccontare e condividere storie è esattamente come tutti gli altri mezzi di comunicazione *mainstream*».

Proprio su Telegraph è particolarmente attivo, com'è naturale, Pavel Durov. Quando ha comunicazioni importanti da lanciare, lo fa sempre attraverso la piattaforma di blogging, rilanciando il link con una introduzione tramite il suo Canale. Com'è accaduto il 14 agosto 2017, quando Durov scrisse un post per dare la propria risposta definitiva a chi ancora accusava l'App di non essere del tutto «sicura» come invece andava predicando. Una risposta alla domanda «Perché non rendere tutto segreto?», con un pezzo intitolato non a caso «Perché Telegram non ha la crittografia *end-to-end* di default?», che vale anche oggi come replica a dubbi e critiche che tuttora ogni tanto si ridestano, come accaduto qualche giorno fa con il pezzo, uscito su Il Sole 24 Ore, «WhatsApp ha dei problemi, ma Telegram non è la soluzione».

L'articolo riportava, infatti, le osservazioni mosse da Evan Sultanik, professore aggiunto della Drexel University di Filadelfia, che in una serie di tweet ricordava a tutti che se

WhatsApp non è una garanzia di privacy, le cose in Telegram sarebbero anche peggiori. «Telegram non è la soluzione – si legge all’inizio della sfilza di post su Twitter – Non lasciate che i vostri amici usino Telegram».

Alle obiezioni di Sultanik risponde molto bene **Andrea Draghetti**, esperto di sicurezza di D3Lab: «Entrambe le applicazioni – dice Draghetti – non sono perfette. Ma Evan, oltre alle tante cose sensate ha inserito anche un’imprecisione: Telegram usa ora SHA256 e non SHA1».

Da parte nostra non ci addentriamo nel cuore della polemica e non entriamo in argomentazioni tecniche. Giova però ricordare, con l’occasione, quanto già tempo fa avevamo chiarito nella nostra rubrica. Sintetizzando, in Telegram, ormai lo sappiamo, esistono due tipi di messaggi, contraddistinti rispettivamente dai due diversi livelli di crittografia già analizzati: *Cloud Chats* tradizionali, con protocollo MTProto *client-server/server-client*, e *Secret Chats*, crittografia end-to-end, anche detta client-client, apposta «per chi cerca la massima sicurezza possibile». Non transitando mai, neppure un istante, da un server, sono come cenere che si disperde nel mare prim’ancora di formarsi.

Ciò non significa, in alcun modo, che le chat standard non siano sicure. Semplicemente, eliminare del tutto i *data center* – peraltro frazionati sotto innumerevoli giurisdizioni nel mondo – implicherebbe:

- Minore disponibilità e, dunque, velocità di reperimento contenuti per l’utente;
- Un possibile campanello d’allarme per i governi, che penserebbero si abbia chissà che da nascondere.

Ne consegue che:

- Le *Cloud Chats normali* sono già sicure al 100%;
- Le *Secret Chats* lo sono al 1000 per 1000;
- Perché sacrificare velocità, immediatezza, possibilità

di accedere all'App da ogni device scambiandosi qualsiasi contenuto, di qualsiasi dimensione, Supergruppi con decine di migliaia di persone e Canali con membri illimitati in nome di una «presunta maggiore sicurezza» che già c'è?

Telegram invece così:

- Massimizza la velocità nello scambio messaggi, la loro fruibilità, da parte di team piccoli e grandi, ottimizzando per una compagnia ***Employee Experience e Customer Experience***;
- Garantisce però, al contempo, massima privacy. Certo, ancora accentuata nelle chat segrete che però, se uniche, imporrebbero diversi limiti alla piattaforma.

Questo insomma è il modo, unico ma vincente, per ottimizzare al meglio il rapporto qualità-prezzo a costo quasi zero.

Sulla scia dell'analisi di Telegram e anche delle parole di Durov, concludendo, possiamo dire che il fatto che i messaggi nelle Chat Segrete usino la crittografia *end-to-end*, mentre le Cloud Chat quella *client-server/server-client*, e siano archiviate in maniera crittografata nel Cloud di Telegram, permette ai tuoi messaggi cloud di essere sia sicuri che facilmente accessibili da tutti i tuoi dispositivi, e «puoi anche cercarli facilmente usando la ricerca su server – che risulta spesso molto utile». «L'idea alla base di Telegram sta nell'offrire qualcosa di più sicuro per le masse, che non si intendono di sicurezza e non ne vogliono sapere nulla. Essere solamente sicuri non basta per raggiungere i nostri obiettivi – bisogna essere anche veloci, potenti e *user-friendly*. Questo permette a Telegram di essere utilizzato massivamente in ampie cerchie, non solo da attivisti e dissidenti, così il semplice fatto di usare Telegram non marchierà gli utenti come obiettivo per un'elevata sorveglianza in alcuni Paesi».

L'App non è d'altronde nuova alle critiche, cui però il suo

fondatore e tutto il team hanno sempre saputo replicare, uscendone a testa alta. Se quanto analizzato sin qui non fosse bastato, ne vedremo ancora delle belle nella prossima puntata della nostra Guida a Telegram.

<https://www.key4biz.it/guida-a-telegram-telescope-telegraph-e-la-sicurezza-dellapp/259883/>