Watchdog: FEMA Wrongly Released Personal Data of Victims

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/YNU0aTeqrRo/watchdog-fema-wrongly-released-personal-data-victims

---

D.C. Attorney General Introduces New Data Security Bill

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/7HA_xytzW0c/dc-attorney-general-introduces-new-data-security-bill

---

Sicurezza, privacy e smartphone: 5 consigli per proteggersi

Parlare di privacy e di smartphone sembra quasi un ossimoro: è chiaro che per poter utilizzare tutte le funzionalità di un dispositivo avanzato dobbiamo rinunciare ad una parte di essa,

dagli spostamenti che facciamo ogni giorno all'attività fisica, dai siti che ci piace consultare spesso ai social network. Questo, però, non significa che dobbiamo arrenderci ad essere spiati 24 ore su 24, in ogni momento del giorno e della notte: la **consapevolezza** di come funziona il nostro amato/odiato dispositivo è **il primo passo da fare per evitare di renderlo ancora più invasivo e, in certi casi, anche pericoloso**. Ecco, quindi, 5 consigli utili per proteggersi dalle minacce più diffuse e per vivere più serenamente, senza necessariamente installare antivirus, antispam e altri tool pesanti sul vostro dispositivo.

Spegnete Wifi, GPS, NFC e Bluetooth se non si utilizzano

Lo so, siamo pigri e addirittura alcuni sistemi operativi oggi decidono per noi quando attivare e disattivare tali funzionalità. Tuttavia dobbiamo abituarci a farlo manualmente, perché in questo modo non solo risparmieremo batteria, ma ci difenderemo da alcuni rischi potenziali, come ad esempio:

- accessi indesiderati da Bluetooth e Wifi (ovviamente se state sfruttando hotspot sicuri e le reti delle vostre **offerte ADSL e fibra di casa**, nessun problema);
- allaccio a reti senza fili realizzate ad hoc per attaccare e/o per appropriarsi di dati personali in modo illecito;
- furto di denaro attraverso l'NFC (sempre più possibile con la maggior diffusione dei pagamenti contactless);
- localizzazione continua attraverso il GPS (che sia Google o un criminale informatico, **è davvero necessario far sapere a tutti dove siamo in qualsiasi istante della nostra esistenza?**).

Occhio ai social network

Per questo punto sarebbe necessario scrivere un trattato in merito: i social network vivono e guadagnano con la raccolta dati ed è l'utente stesso a fornirli, **più o meno volontariamente** (il recente caso di **Facebook sotto inchiesta penale per la cessione di dati ad altre aziende** dovrebbe fare riflettere). Se, però, non potete fare a meno di Facebook, Twitter, Instagram, etc…, cercate di utilizzarli in modo intelligente, **evitando di condividere informazioni e contenuti particolarmente personali e/o sensibili**.

Ricordate, inoltre, che pubblicare sui social network **non è mai privato**, pur impostando le opzioni privacy in modo restrittivo: **ogni amico o follower può potenzialmente condividere a loro volta i vostri post, le vostre foto e i vostri dati**, sia sullo stesso social network che all'esterno, con screenshot e altri sistemi. Insomma, prima di scrivere o pubblicare qualcosa, fatevi prima la seguente domanda: ne vale davvero la pena?

Occhio alle app

Gli store di Apple e Google vengono controllati regolarmente eppure non mancano casi, anche eclatanti, di app spia e/o particolarmente affamate di dati personali presenti all'interno dei cataloghi ufficiali e scovate in ritardo: **pensate, quindi, cosa potrebbe nascondersi negli store alternativi**. Se da questo lato Apple ha una politica di chiusura abbastanza stringente sulle app esterne (anche se con qualche metodo è possibile aggirare i blocchi), Android è

molto più esposto alle app più pericolose.

-

Evitate, quindi, di installare applicazioni sconosciute, provenienti da fonti a rischio, ma dubitate anche quelle app che vi richiedono troppi permessi "strani" al momento dell'installazione. Un esempio: se state installando un'applicazione per la navigazione stradale è chiaro che sarà necessario l'accesso al GPS per poterla utilizzare, ma se state scaricando un'app per gli sfondi del telefonino che vi richiede la localizzazione geografica, beh, passate ad altro.

Evitate di rispondere o richiamare numeri esteri

Se fate un lavoro che implica anche le comunicazioni con l'estero, ovviamente saprete già con quali Paesi sarete in contatto. Tuttavia, se non avete alcun interesse al di fuori dei confini nazionali e vi ritrovate chiamate con prefissi stranieri, evitate di rispondere o di ricontattarli. Spesso, infatti, **potrebbero nascondersi vere e proprie truffe**, che potrebbero scalarvi denaro e aprire la strada ad altri tipi di attacchi. Tra i servizi truffa via telefono più diffusi ultimamente, quelli provenienti da Tunisia ed est europeo (molto frequenti i seguenti prefissi: **+216, +373 e +383**);

Evitate siti e banner dubbi

Se state navigando su Internet dal vostro smartphone e vi si aprono pagine con annunci di vincite (iPhone, viaggi, pc, etc…), inviti alla compilazione di test o sondaggi mai richiesti, **quasi certamente si tratta spam** o, ancora peggio, un metodo per attaccare il vostro dispositivo e, quindi, i vostri dati. **Evitateli come la peste** e, se sono

particolarmente frequenti, utilizzate browser più sicuri e dotati di ad block.

Non cliccate sui link

Che vi arrivino sulla mail, su WhatsApp, su Facebook, su Skype, non ha importanza: prima di cliccare su qualsiasi indirizzo Internet, anche proveniente da una fonte sicura, **chiedete conferma che sia stata quella specifica fonte ad averlo inviato**. Se ciò non è possibile, analizzate attentamente il link che avete ricevuto: è un indirizzo attendibile? Ha un dominio verosimile? Ha senso che il vostro amico, collega o familiare ve lo abbia inviato?

Sembra quasi paranoico doversi preoccupare di controllare qualsiasi link che vi venga spedito, ma sappiate che spesso le minacce peggiori si nascondono su questi innocenti indirizzi. Attraverso link "malevoli" i criminali informatici **possono sfruttare i bug e gli accessi dei sistemi operativi e violarne la sicurezza**, consentendo il furto dati, l'accesso ai file o addirittura prendere il comando a distanza del dispositivo stesso (ad esempio attivando la fotocamera, cancellando o creando dati sulla memoria, etc…). Riuscite ora a percepirne le devastanti potenzialità? Bene, probabilmente il controllo dei link prima di un click ora vi sembrerà meno esagerato.

Ecco, quindi, 5 consigli per proteggervi dalle minacce sul vostro smartphone: non sono certamente gli unici ma possiamo considerarli certamente tra i più importanti e utili. Perché **il primo antivirus e il primo sistema d'allarme per i nostri dispositivi – è importante tenerlo a mente e averne consapevolezza – siamo noi**.

https://www.key4biz.it/sicurezza-privacy-e-smartphone-5-consigli-per-proteggersi/250792/

Privacy. Snowden: ‘La crittografia end-to-end non basta, Apple&Co. hanno ancora gravi vulnerabilità’

“*Il mio lavoro oggi? Analizzare in che modo le tecnologie, create per liberarci, vengono invece usate per controllarci, e cercare di spostare l’asticella di un grado a favore delle persone ordinarie, invece di chi vuole avere il controllo sulle nostre vite*”.

Sono queste le parole di **Edward Snowden,** il più famoso ex agente dell’intelligence Usa, che “**La Repubblica**” ha intervistato via chat dalla **Russia**, il Paese dove Snowden risiede da 5 anni con un permesso temporaneo grazie all’appoggio del Governo.

Nato a **Elizabeth City**, negli Stati Uniti, nel 1983, Edward Snowden, ex analista della Cia ed ex collaboratore della Nsa (la National Security Agency, l’agenzia per la sicurezza nazionale Usa), è stato accusato di spionaggio a causa delle sue rivelazioni nel 2013 sui programmi top secret di sorveglianza di massa dei governi **Usa** e **Gb**.

Da quel momento per arginare il problema, Apple e altri giganti tecnologici iniziarono a blindare i propri device e le loro altre tecnologie con lo sviluppo di una crittografia molto forte, in grado di reggere la privacy degli utenti. Ma secondo Snowden, questo non è bastato ad argine lo strapotere della Nsa.

“*Se non riescono a forzare la crittografia, hackerano gli apparecchi elettronici che cifrano le nostre comunicazioni: i nostri telefoni, i nostri computer. È la via imboccata dopo il 2013 perché tanto loro hanno trovato nuove crepe per accedervi”,* ha dichiarato Snowden a La Repubblica. “*Le vulnerabilità nelle tecnologie sviluppate da* ***Apple****,* ***Google*** *e tutte le più grandi aziende, anche* ***Microsoft*** – continua l’ex dipendente dell CIA nell’intervista-*, hanno una serie infinita di gravi vulnerabilità nei loro software e purtroppo non sono costrette a pagare nessuna conseguenza. Fino a quando andremo avanti così, non cambierà nulla*”.

L’Italia spiata dagli Usa

Quando nel 2013 annunciò al mondo i suoi file, rivelò anche lo spionaggio Nsa contro l’Italia per influenzare le scelte politiche del nostro Paese.

“*La ragione più importante e che non cambierà mai è semplicemente l’influenza,* continua Snowden. *“Gli Stati Uniti vogliono essere in grado di influenzare le future direzioni in cui l’Italia si muove, politicamente, economicamente e in generale. Se sei un cittadino italiano, non hai alcuna protezione legale dallo spionaggio Usa. E allora basta pensare cosa questo possa significare per un giudice italiano che indaghi su un caso che riguarda gli Stati Uniti, per un politico italiano, per un reporter che lavora a un articolo scomodo per i poteri oltreoceano*“.

https://www.key4biz.it/privacy-snowden-la-crittografia-end-to-end-non-basta-appleco-hanno-ancora-gravi-vulnerabilita/250284/

EU to Slap Google With Fresh Fine: Sources

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/1AiT23brr0A/eu-slap-google-fresh-fine-sources

---

E-Commerce Company Gearbest Leaked User Information

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ySMQYGn7wfM/e-commerce-company-gearbest-leaked-user-information

---

China Does Not Ask Firms to Spy on Others: Premier

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/XWQcrXAt4b8/china-does-not-ask-firms-spy-others-premier

---

Epic says its Game Store is not spying on you

Enlarge / Despite what you may have read, Epic says this is not spyware.

reader comments

83 with 57 posters participating

Share this story

This week, certain corners of the gaming Internet have been abuzz with a bit of self-described “amateur analysis” suggesting some “pretty sketchy,” spyware-like activity on the part of the Epic Game Store and its launcher software. Epic has now stepped in to defend itself from those accusations, while also admitting to an “outdated implementation” that can make unauthorized access to local Steam information.

The Reddit post “Epic Game Store, Spyware, Tracking, and You!” points to a wide-ranging set of implications based on some broad file and network access traffic observations when the Epic Game Store is running. But much of the post is focused on Epic’s association with Chinese gaming giant Tencent, which owns a share of the company.

“Tencent is a significant, but minority shareholder in Epic,” co-founder and CEO Tim Sweeney wrote in response to the conspiracy theory in one Reddit thread. “I’m the controlling shareholder of Epic… The decisions Epic makes are ultimately my decisions, made here in North Carolina based on my beliefs as a game developer about what the game industry needs!”

Sweeney offered a similar defense of Epic’s relationship with

Tencent back in December, when similar concerns first popped up. “Epic does not share user data with Tencent or any other company,” he wrote at the time. “We don’t share it, sell it, or broker access to it for advertising like so many other companies do. I’m the founder and controlling shareholder of Epic and would never allow this to happen.”

“Epic is controlled by Tim Sweeney,” Epic’s VP of Engineering Daniel Vogel added in response to another recent thread. “We have lots of external shareholders, none of whom have access to customer data.”

Vogel went on to offer explanations for some other suspicious-looking Epic Games Store app activity. A “tracking.js” file, for instance, is used to track revenue-sharing statistics for Epic’s Support-a-Creator program, he wrote. Vogel also pointed to the open source code behind features like the anonymized hardware survey, the Unreal Editor, and the Chromium-based launcher UI, which he said cause most of what the original post identifies as “sketchy” app activity.

Vogel does admit, though, that “the launcher makes an encrypted local copy of your localconfig.vdf Steam file” automatically and without explicit user permission. However, he writes, that hashed file is only sent to Epic if you choose to import your Steam friends to the Epic Game Store in order to find potential matches with others that have opted in.

Still, Sweeney acknowledged that Epic making local access to Steam files without direct permission might justifiably rub some users the wrong way. “You guys are right that we ought to only access the localconfig.vdf file after the user chooses to import Steam friends,” he wrote on Reddit. “The current implementation is a remnant left over from our rush to implement social features in the early days of *Fortnite*. It’s actually my fault for pushing the launcher team to support it super quickly and then identifying that we had to change it. Since this issue came to the forefront we’re going to fix it.”

“This sort of independent analysis of what data software accesses… is a healthy trend and I’d love to see it done more widely,” Sweeney wrote in another comment. “In analyzing the results, it’s important to distinguish the normal from the abnormal… and to separate technical analysis from inflammatory rhetoric, such as the insane claim that we’re a bunch of Chinese spies.”

https://arstechnica.com/?p=1474647

Leading Israeli Candidate for PM Targeted by Iranian Hackers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/rHStZyJp2No/leading-israeli-candidate-pm-targeted-iranian-hackers

---

Cessione dati utenti ad aziende, Facebook sotto inchiesta penale negli Usa

Nuove nubi all’orizzonte per **Facebook**.

Secondo quanto riporta il **New York Times**, l’azienda di **Mark Zuckerberg** è sotto inchiesta penale negli Stati Uniti per gli

accordi sulla cessione dei dati degli utenti ad alcune tra le più importanti società tecnologiche.

Entrando nel dettaglio, i procuratori federali – riporta il **NYT –**, hanno aperto un'inchiesta penale sulle operazioni di condivisione dei dati tra Facebook e ad importanti produttori di dispositivi mobili.

Secondo i termini di tali accordi, Facebook ha consentito ai produttori di dispositivi tra cui **Apple**, **Amazon** e **Microsoft** di accedere ai dati degli utenti personali, inclusi elenchi di amici, informazioni di contatto e talvolta anche messaggi privati - e non sempre con consenso dell'utente.

Sempre secondo il quotidiano, il Grand Jury di New York ha già citato in giudizio e richiesto il mandato a due aziende (per ora rimaste anonime) la consegna di documentazione sulle partnership con il social network.

"*Stiamo collaborando con le indagini e prendiamo queste inchieste molto sul serio*", ha dichiarato a **Business Insider** un portavoce di Facebook. "*Abbiamo fornito testimonianze pubbliche, risposto a domande e ci siamo impegnati a continuare a farlo*".

Le partnership con le altre società

Questi due produttori di smartphone sono tre le oltre 150 società – Amazon, Apple, Microsoft e Sony comprese – che si sono accordate con Facebook sull'accesso ai dati degli utenti, in alcuni casi senza il loro consenso.

A dicembre, in seguito al rapporto del Times, Facebook ha dichiarato in un blog che queste partnership erano necessarie per abilitare determinate funzionalità social in app esterne, come accedere a un account Facebook da un telefono Windows o

condividere il brano di Spotify che stavi ascoltando tramite Facebook Messagger.

“*Per essere chiari: nessuna di queste partnership o funzionalità ha permesso alle aziende di accedere alle informazioni senza il permesso delle persone, né ha violato il nostro accordo del 2012 con la FTC*“, aveva fatto sapere Facebook in un post del suo blog.

La maggior parte di queste partnership si è conclusa negli ultimi anni proprio a causa dei recenti scandali.

L’indagine penale farà aumentare la multa della FTC?

La notizia dell’inchiesta penale è l’ultima di una serie di controversie riguardante il □□gigante tech da 2 miliardi di utenti.

Nell’ultimo anno, Facebook ha faticato a riabilitare la sua immagine pubblica a causa degli scandali sulla privacy (vedi **Cambridge Analytica)**e la crescente evidenza di come il suo social network è stato utilizzato per diffondere disinformazione e fake news durante le elezioni presidenziali degli Stati Uniti del 2016.

Come se non bastasse, ieri il social network ha subito uno dei **peggiori down della sua storia**, lasciando utenti e inserzionisti pubblicitari di tutto il mondo impossibilitati ad accedere al sito per gran parte della giornata.

Facebook sta già affrontando la prospettiva di una multa di miliardi di dollari da parte della **Federal Trade Commission,** e sicuramente, questa indagine penale potrebbe alzare la posta in modo significativo.

https://www.key4biz.it/privacy-facebook-sotto-inchiesta-penale-negli-usa/248390/