Zoom for Mac made it too easy for hackers to access webcams. Here’s what to do [Updated]

Enlarge / Artist’s impression of wireless hackers in your computer.

reader comments

60 with 49 posters participating

Share this story

Update 7:23pm ET: As this post was being reported, Zoom developers reversed their previous position and issued an update that changes the contested behavior.

“Initially, we did not see the Web server or video-on posture as significant risks to our customers and, in fact, felt that these were essential to our seamless join process,” Zoom’s Jonathan Farley wrote. “But in hearing the outcry from our users in the past 24 hours, we have decided to make the updates to our service.”

The update makes the following changes:

- complete removal of the local Web server and
- an addition to the menu that allows users to remove the app

Zoom developers also added new details about a previously mentioned update, which is now scheduled for Friday. It will

- Automatically save first-time users' selection of the "Always turn off my video" preference and
- allow returning users to update their video preferences and make video OFF by default at any time through the Zoom client settings

What follows is the story as it ran earlier:

One of the easiest ways to tell if someone is a practitioner of computer security is to look at their laptop. If the webcam is covered by tape or a sticker, they likely are. A recently published report on the Zoom conferencing application for Macs underscores why this practice makes sense.

Researcher Jonathan Leitschuh reported on Monday that, in certain cases, websites can automatically cause visitors to join calls with their cameras turned on. It's not hard to imagine this being a problem for people in their bathrobes or in the middle of a sensitive business conference since a malicious link would give no warning in advance it will open Zoom and broadcast whatever is in view of the camera.

Zoom developers almost certainly intended the behavior to make it easier to use the Web conferencing app. But unless users have properly tweaked their settings in advance, Lietschuh's findings show how miscreants can turn this ease-of-use against unwitting users. A proof-of-concept exploit is available here, but reader be warned: depending on your Zoom settings, your webcam may soon be transmitting whatever it sees to perfect strangers.

"This vulnerability allows any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission," Leitschuh wrote.

Leitschuh is mostly correct there. Clicking the link will automatically open Zoom and join a call. But as mentioned earlier, video is collected only when Zoom is configured to begin conferences with a camera turned on. Some media reports

and social media commentators have said this behavior allows websites to “hijack” a Mac webcam. I’d argue that’s a stretch since (1) it’s fairly obvious that Zoom is opening and broadcasting whatever the camera sees and (2) it’s easy to immediately leave the conference or simply turn off the camera.

What’s more, preventing the video grab involves a one-time click to a box in the Zoom preferences that keeps video turned off when joining a video. But user beware: even when this setting is on, sites still can force Macs to open Zoom and join a conference.

Dan Goodin
That’s not to say the threat Leitschuh disclosed is mere handwaving. It’s not. But it underscores the near-impossible balancing act developers must strike. Make a feature too hard to use and people will move to a competing product. Make it too easy and attackers may abuse it to do bad things the developer never imagined.

In this case, Zoom developers should have warned that the ability to automatically join a conference with video turned

on was a powerful feature that could be used to compromise users' privacy. Instead, the developers left it up to users to decide with no up-front guidance. (By contrast, audio is automatically turned off when joining a Zoom conference.) In other words, Zoom developers made this automatic webcam joining way too easy. In retrospect, thanks to Leitschuh's post, that's easy to see.

In a response to Leitschuh's disclosure Zoom's Richard Farley said the company will roll out an update this month that will "apply and save the user's video preference from their first Zoom meeting to all future Zoom meetings." Farley didn't say if Zoom will provide the guidance many users will need to make an informed choice.

An always-on webserver

Leitschuh's research uncovered another behavior by Zoom for Mac that is also unsettling to security-conscious people. The app installs a webserver that accepts queries from other devices connected to the same local network. This server continues to run even when a Mac user uninstalls Zoom. Leitschuh showed how this webserver can be abused by people on the same network to force Macs to reinstall the app.

This clearly isn't good. While the webserver is only accessible to devices on the same network, that still exposes people using untrusted networks. And if hackers were ever to come across a code-execution vulnerability in the webserver, the potential for abuse is even higher. Farley said Zoom introduced the webserver as a way to work around a change introduced in Safari 12 that requires users confirm with a click each time they want to start the Zoom app prior to joining a meeting.

"We feel that this is a legitimate solution to a poor user-experience problem, enabling our users to have faster, one-click-to-join meetings," Farley wrote. "We are not alone among

video-conferencing providers in implementing this solution.”

Independent security researcher Kevin Beaumont said on Twitter that the BlueJeans video conferencing app for Mac also opens a webserver. There is no evidence that the behavior Leitschuh reported is found in Zoom for Windows.

Convenience is the enemy of security

As is the case with the auto-on webcam when joining meetings, Zoom’s implementation of a webserver is a convenience that comes at the potential cost of security. Neither behavior represents a critical vulnerability, but they do suggest Zoom developers could do more to lock down the Mac version of their app, particularly for users who may have less awareness of security issues.

And this is where precautions such as tape over a webcam come in. Users can never be sure developers have adequately safeguarded their apps against hacks or abuse, so the responsibility falls on end users to compensate. Other ways to protect against abuses of Zoom or other Web conference software is to use an app such as Little Snitch and configure it to give the conferencing software Internet access for only limited amounts of time. Another self-help protection is to configure macOS so that Zoom only has access to the webcam at specific times when it’s needed.

Yes, these additional protections can be a bother. But they also underscore the fundamental tension between convenience and security.

https://arstechnica.com/?p=1533553

UK: laboratorio di forensica cede al ricatto di un

ransomware

Lug 08, 2019 Marco Schiaffino Attacchi, Gestione dati, In evidenza, News, Privacy, RSS 0

L'azienda è uno dei maggiori contractor del governo britannico e si occupa di analisi dei dati per conto della polizia e delle procure.

C'è un proverbio che dice che "il figlio del calzolaio va in giro con le scarpe rotte". La notizia dell'attacco **ransomware** subito da **Eurofins Scientific**, società specializzata in analisi di ogni tipo (da quelli tossicologici all'ingegneria informatica forense) ci si adatta alla perfezione.

L'attacco, secondo quanto si può ricostruire dai vari comunicati dell'azienda, sarebbe avvenuto lo scorso 2 giugno. La dirigenza di Eurofins ha immediatamente denunciato l'accaduto con un comunicato stampa del giorno dopo.

Nel testo si parla di "un nuovo tipo di malware" ma, soprattutto, si fa esplicito riferimento a una procedura di ripristino dei dati a partire dal backup. Insomma: la notizia, fino a quel momento, rientrava nella normalità di un attacco ransomware che (non è la prima volta) aveva colpito un bersaglio di alto livello.

Certo, l'idea che tecnici abituati a lavorare nel settore forensico finiscano vittima di un malware ha fatto sollevare qualche sopracciglio, ma nulla di più.

Anche il successivo comunicato del 10 giugno, in cui l'azienda aggiornava sulla situazione delle sue infrastrutture IT, non conteneva alcuna notizia sconvolgente. **Le uniche notizie di rilievo riguardano il fatto che il malware in questione non sarebbe stato rilevato dagli antivirus e che il ripristino dei**

sistemi era in corso.

Venerdì sera, però, Eurofins ha ammesso che il ripristino dei sistemi non è avvenuto attraverso l'uso dei backup, ma **pagando il riscatto richiesto dai pirati informatici**.

Un "dettaglio" che cambia decisamente le carte in tavola. In primo luogo perché una società che collabora regolarmente con le forze di polizia ha adottato una strategia (se la vogliamo chiamare così) che di solito viene sconsigliata dalle stesse forze dell'ordine.

In secondo luogo perché tutti i dati contenuti nei loro sistemi, alla luce di questa notizia, potrebbero essere considerati inaffidabili.

E non stiamo parlando di contratti e fatture, ma di esami del DNA e analisi tossicologiche che dovrebbero essere utilizzate in tribunale come prove.

Le autorità si sono affrettate a dichiarare di "non vedere alcuna ragione per credere che ci sia stato un impatto sulle prove elaborate dalla società". L'affermazione, però, è decisamente ottimistica.

Considerato che tutti i dati nei sistemi di Eurofins hanno subito un processo di crittografia eseguito da un malware e una decodifica portata a termine con uno strumento fornito da cyber-criminali, sostenere che i dati possano essere

considerati “integri” è un azzardo che qualsiasi avvocato in aula potrebbe sottolineare per mettere in dubbio l’affidabilità delle prove.

Insomma, sulla base dell’incidente avvenuto il 2 giugno, centinaia (migliaia?) di processi potrebbero essere invalidati o ritardati a causa della possibile inaffidabilità dei dati forniti da Eurofins.

Condividi l’articolo

Tik Tok rischia (un’altra) multa per violata privacy dei minori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/08/uk-laboratorio-di-forensica-cede-al-ricatto-di-un-ransomware/

La protezione dei dati personali in Italia, cosa è successo all’incontro di Aidr

Conoscere il nuovo Regolamento Ue, a un anno circa di distanza dalla sua entrata in vigore, per tutelare l’identità digitale. È questo il filo conduttore attorno al quale si è sviluppato il dibattito su privacy e web, mercoledì pomeriggio a Palazzo

Madama, a cui hanno partecipato **Mattia Fantinati**, sottosegretario alla presidenza del Consiglio con delega alla Pubblica amministrazione, **Caterina Chiaravalloti**, presidente del Tribunale di Latina, **Guido Alpa**, avvocato e professore di diritto civile Università La Sapienza di Roma, e **Mauro Nicastri**, presidente di Aidr (Associazione italian digital revolution). Occasione dell'incontro, moderato dall'analista di *Huffington Post e Limes*, **Piero Schiavazzi**, è stata la presentazione dell'ultimo volume di **Giusella Finocchiaro**, professore ordinario di diritto privato e di diritto di Internet Università di Bologna, ***La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*** (Zanichelli editore).

"La protezione dei dati è fondamentale per mettere i cittadini in salvo dai rischi che il digitale può comportare sulla vita di tutti noi – ha subito inquadrato **Fantinati** -. *Rischi anche alla sicurezza nazionale. Ricordate il caso Cambridge Analytica? Da sottosegretario, sto personalmente promuovendo una rivoluzione digitale, con l'obiettivo di costruire una smart nation, bilanciando le esigenze di efficacia ed efficienza della PA con quelle di protezione dei cittadini. Tenere insieme questi aspetti è la nostra sfida. Che possiamo vincere, anche grazie ad eventi come questo. Dobbiamo mettere insieme pool di esperti, politici, cittadini. Questo convegno dimostra qual è la strada da seguire*".

"*Il Regolamento* – ha riferito dal canto suo il professor **Alpa** -, *prende in considerazione due aspetti diversi dell'utilizzo dei dati personali, fin dall'art. 1: da un lato i diritti della persona, dall'altro la libera circolazione dei dati personali. Restano aperti i problemi dei diritti della persona sui dati che rimandano a due concezioni diverse anche del consenso. Una lettura è quella proprietaria del dato, che vede il dato coessenziale alla persona. L'altra è quella che vede il dato come espressione della persona, ma allo stesso tempo bene suscettibile di circolazione".*

“La diffusione del digitale, se da un lato rende più veloce la circolazione della notizia, dall’altro altera la dimensione spazio temporale della stessa. L’esempio più emblematico è quello della diffusione della notizia del promovimento dell’azione penale a carico di un soggetto, notizia che rimane sospesa nel tempo, talora anche quando viene meno l’attualità della stessa, o addirittura non viene aggiornata in relazione all’esito del procedimento penale – ha spiegato **Chiaravalloti** *-. Sebbene sussistano degli strumenti di tutela giurisdizionale che dovrebbero rendere più effettivo il diritto alla rettifica, contestualizzazione ed eventualmente cancellazione dei dati, ci si chiede tuttavia se – tenuto conto peraltro dell’arco temporale durante il quale la notizia rimane nella disponibilità del web – la diffusione del dato giudiziario, espressione del diritto di cronaca, quale esplicazione del più ampio diritto di libera manifestazione del pensiero, non vanifichi la tutela di altri diritti della persona. In primis, quello della presunzione d’innocenza dell’imputato”.*

A lanciare il tema della *“reputazione”* online è stato **Nicastri**, che a nome dell’Aidr ha posto così la questione: *“Durante la nostra attività di diffusione della cultura digitale, capita spesso di registrare paure, tensioni e impotenza di diversi cittadini nei confronti di pubblicazioni web a tratti calunniose, diffamanti, che non si riesce in alcun modo a cancellare, eliminare dalla Rete. Si tratta di un problema molto serio, perché va a compromettere la reputazione del soggetto malcapitato, che avrebbe invece diritto a non discolparsi in merito magari a reati mai commessi o fatti mai avvenuti”.*

“Il termine ‘privacy’, – ha risposto **Finocchiaro** – *oggi, indica, molti temi diversi: dalla riservatezza vera e propria, alla protezione dei dati personali, all’identità digitale e*

alla reputazione. Per tutelare i diritti sottesi l'ordinamento giuridico offre strumenti diversi. Occorre comporre questi diversi diritti in un sistema, che oggi è tutto da costruire. Non è ancora ben delineato il sistema della protezione della personalità che va dalla Carta dei diritti fondamentali dell'Unione europea, al Regolamento europeo, alla normativa italiana, ai provvedimenti del Garante, alla giurisprudenza e alla dottrina. Il sistema e la visione complessiva spesso sfuggono a chi si concentra soltanto sul dettaglio, perdendo la visione complessiva".

"Il Regolamento europeo – ha rimarcato infine l'autrice del libro presentato a Palazzo Madama – *richiede un bilanciamento costante fra diritti e interessi contrapposti: basti pensare all'utilizzo dei dati personali nelle applicazioni di intelligenza artificiale o al diritto all'oblio. Il Regolamento non risolve e non potrebbe risolvere il problema, ma indica invece le direttrici lungo le quali si deve svolgere il ragionamento giuridico e il necessario costante bilanciamento".*

https://www.key4biz.it/aidr-ecco-di-cosa-si-e-parlato-allincontro-al-senato-su-privacy-e-web/264247/

MailUp lancia il corso online "Dati personali: istruzioni per l'uso"

A più di un anno dall'entrata in vigore del *General Data*

Protection Regulation, o più comunemente conosciuto con l'acronimo **Gdpr**, il regolamento generale adottato dall'Unione europea sulla protezione dei dati e della privacy necessità ancora di un'adeguata promozione e comprensione, se è vero, come riportato da Eurobarometro, che in Europa solo il 67% dei cittadini è a conoscenza del Regolamento, o comunque ne hanno sentito parlare, mentre in Italia il 49% dei cittadini ha sentito parlare del Gdpr e appena il 17% sa esattamente di cosa si tratta.

In tale contesto, MailUp annuncia il lancio di un corso online di 13 lezioni dal titolo "***Dati personali: istruzioni per l'uso***", con l'obiettivo di indirizzare le aziende alla corretta attività di trattamento e valorizzazione dei dati personali.
L'iniziativa, che sarà curata dall'Avvocato **Marco Maglio,** Presidente dell'Osservatorio Europeo sulla *Data Protection* e fondatore di Lucerna Iuris, è tesa a favorire la comprensione aziendale dei principi operativi del nuovo Regolamento europeo sul trattamento dei dati personali, che poi sono gli elementi chiave su cui sviluppare e a cui allineare le proprie strategie.
"*Parlare di rispetto dei dati significa parlare di rispetto delle persone: consumatori, clienti, potenziali tali, fornitori e collaboratori, il cui rispetto dei dati permette alle aziende di basare la relazione sul rispetto, la fiducia, la trasparenza* – ha commentato **Stefano Branduardi**, Marketing Director di MailUp – *con questo corso vogliamo avvicinarci al GDPR in modo concreto, pratico, operativo, per dare alle aziende le linee guide con cui gestire al meglio le attività di trattamento e sfruttare il potenziale dei dati personali* ".
Tredici lezioni, duqnue, che si addentreranno tra i principi cardine della normativa, utili a scongiurare eventuali sanzioni, valorizzare i dati e massimizzare il potenziale delle informazioni.

Diversi infine i temi toccati dal corso di MailUp, tra cui: i

concetti base, tecnici e giuridici del trattamento, con un focus sulla figura dell'interessato; gli elementi fondamentali per condurre un trattamento conforme al GDPR; i principi del trattamento; le modalità operative della privacy by design e privacy by default; il principio trasversale della trasparenza; i diritti degli interessati che la legge garantisce; l'accountability e le figure chiave del trattamento; in chiusura, la lezione dedicata alle eventuali sanzioni (civili e amministrative) applicabili a chi non rispetta le regole.

https://www.key4biz.it/mailup-lancia-il-corso-online-dati-personali-istruzioni-per-luso/264227/

Reddito di cittadinanza, il Garante Privacy da l'ok al sistema informativo

Con il parere favorevole del Garante privacy sullo schema di decreto del Ministero del lavoro che disciplina il Sistema informativo del reddito di cittadinanza (Rdc) si conclude una complessa attività per la messa in sicurezza dei dati di milioni di persone.

Lo schema sottoposto all'Autorità ha accolto tutte le indicazioni fornite dall'Ufficio nel corso di numerosi incontri tenuti con i rappresentanti del Ministero e **dell'Anpal** (Agenzia nazionale politiche attive del lavoro), volti ad assicurare il rispetto della normativa in materia di protezione dei dati personali.

Lo schema di decreto definisce le finalità e i titolari del

trattamento nell’ambito del Sistema informativo e disciplina nel dettaglio i flussi di dati tra le amministrazioni coinvolte. Lo schema stabilisce che spetta al Ministero del lavoro, avvalendosi dei dati trasmessi dall’**Inps** e dall’**Anpal**, individuare, in base ai criteri stabiliti in un allegato allo stesso schema, le platee dei beneficiari da indirizzare, rispettivamente, ai Servizi per il lavoro e ai Servizi competenti dei comuni, e alimentare di conseguenza le relative Piattaforme.

Nel Sistema informativo del reddito di cittadinanza vengono trattati su larga scala dati personali relativi alla salute, alla condizione sociale e alla situazione economica e finanziaria, elaborati anche in base alla valutazione dello stato di bisogno dei beneficiari (compresi anche soggetti vulnerabili o minori d’età).

Il trattamento di una mole così rilevante di dati potrebbe comportare rischi per i diritti di milioni di beneficiari.

Il Garante ha quindi chiesto ed ottenuto l’introduzione nello schema di una serie di misure a tutela delle persone interessate e delle migliaia di enti pubblici e privati a vario titolo coinvolti. Le misure riguardano, in particolare, la minimizzazione dei dati personali trattati, in modo tale da assicurare, in relazione ad ogni flusso informativo disciplinato, il rispetto del principio di proporzionalità con l’individuazione delle tipologie di dati, delle operazioni eseguite, dei soggetti cui possono essere comunicati e delle categorie di soggetti autorizzati all’accesso, anche per quanto riguarda l’accesso da parte della Guardia di finanza. Le garanzie introdotte nello schema riguardano anche l’adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi: in particolare l’introduzione di accesi selettivi ai dati

contenuti nel Sistema informativo, l'utilizzo di adeguati sistemi di autenticazione informatica alle Piattaforme digitali e di canali di trasmissione sicuri per gli scambi di dati tra le diverse amministrazioni coinvolte, il tracciamento delle operazioni svolte mediante le Piattaforme digitali; le modalità di utilizzo di dati anonimi o aggregati da parte del Ministero e da parte delle Regioni.

Navigator

Da metà agosto **i navigator** saranno pienamente operativi nei **Centri per l'impiego,** per la gestione delle attività connesse al Reddito di cittadinanza. L'obiettivo è definito nel cronoprogramma elaborato da **Anpal Servizi** che prevede dal 19 al 24 luglio l'avvio e la definizione delle procedure di contrattualizzazione dei vincitori delle selezioni. Cominceranno il 29 e si concluderanno 31 luglio, tre giornate di orientamento a Palermo, Cagliari e Roma. Poi dal 1 agosto due settimane di formazione sul territorio, sotto la supervisione di un tutor di Anpal Servizi.

Propedeutiche a tutto il percorso di contrattualizzazione, orientamento e formazione, saranno le convenzioni che **Anpal Servizi e le Regioni** si sono impegnati a sottoscrivere il 18 luglio per definire il perimetro operativo in cui i navigator saranno chiamati a supportare i Centri per l'impiego.

https://www.key4biz.it/reddito-di-cittadinanza-il-garante-privacy-da-lok-al-sistema-informativo/264214/

Facebook, il down ha svelato come l'IA interpreta le immagini (fregandosene della privacy)

Il grande black out di due giorni fa – che ha messo fuori uso per parecchie ore le tre grandi piattaforme social **Facebook, Instagram e WhatsApp** – ha offerto uno sguardo dietro le quinte su come l'Intelligenza artificiale e l'algoritmo di Facebook "vedono" le tue foto.

L'interruzione, che è iniziata mercoledì 3 luglio e ha colpito 1,5 miliardi di utenti di Facebook e reso Instagram quasi inutilizzabile, ha 'bloccato' le immagini dei social media dal caricamento e ha lasciato al loro posto descrizioni come: "*l'immagine può contenere: tavolo, pianta, fiore, e l'immagine può contenere 1 persona, con sorriso, primo piano*"

Queste descrizioni o tag mostrano come l'intelligenza artificiale di Facebook interpreta le immagini.

> *Oh yeah! I forgot Facebook uses machine learning to tag our photos with what it sees in the picture.*
>
> *To be fair, "one person, beard" is pretty much a spot-on description of me.* *pic.twitter.com/fCpydUxtpz*
>
> *— Zack Whittaker (@zackwhittaker)* *3 luglio 2019*

Su Twitter, le persone hanno condiviso screenshot di come le loro foto sono state taggate. *"A dir la verità, 'una persona, barba' è praticamente una descrizione azzeccata di me*", ha

scritto **Zack Whittaker**, un editor di **TechCrunch**.

L’IA per i non vedenti

L’utilizzo dell’IA sulle immagini viene utilizzata negli sforzi di accessibilità dell’azienda per descrivere le foto a persone non vedenti o ipovedenti e che accedono al sito tramite uno screen reader. In breve, Facebook utilizza l’apprendimento automatico per interpretare automaticamente le foto, quindi legge questa interpretazione ad alta voce agli utenti non vedenti.

La privacy

Quindi, anche se qui potrebbe esserci una spiegazione benigna, è ancora un duro promemoria di quanti dati Facebook sta raccogliendo in ogni momento, anche quando non ci rendiamo conto che sta accadendo. Grazie alla sua tecnologia IA sempre più sofisticata, Facebook può persino raccogliere informazioni da qualcosa cosa, anche innocua, come una foto di qualcuno in vacanza.

Alcuni utenti sono infatti stati “descritti” dalla IA esattamente con il loro nome. L’intelligenza artificiale non solo quindi ha riconosciuto il contenuto dell’immagine, ma l’ha saputa associare ad una persona specifica. L’identificazione quindi è massima. Il malfunzionamento del 3 luglio ha permesso agli utenti di vedere ancora una volta quante informazioni effettivamente condividono in rete, e quanto sopratutto, sia forte il potere del social di **Mark Zuckerberg.**

https://www.key4biz.it/facebook-il-down-ha-svelato-come-lia-interpreta-le-immagini-fregandosene-della-privacy/264169/

Tik Tok rischia (un’altra) multa per violata privacy dei minori

Lug 05, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Scenario 0

Il governo inglese ha avviato una procedura sul trattamento dei dati dei minori. L’azienda cinese rischia una multa da 20 milioni di euro.

Il difficile rapporto tra tutela della privacy dei minori e Internet vive un nuovo capitolo che conferma (ancora una volta) la presenza di un problema cui si stenta a trovare una soluzione.

Protagonista è **TikTok**, l’applicazione social che spopola tra i ragazzini e che consente di registrare e condividere filmati in cui i protagonisti si esibiscono in performance musicali e non solo.

L’azienda cinese sarebbe finita nel mirino delle agenzie governative britanniche, che stanno valutando la possibilità di sanzionare TikTok per violazione della normativa in tema di protezione dei dati (**GDPR**) relativa ai contenuti pubblicati dai minori di 13 anni.

La normativa europea, infatti, prevede che qualsiasi trattamento dei dati di utenti minorenni (l’età può essere definita da ogni singolo stato) **debba essere autorizzata dai genitori**.

Una previsione di difficile applicazione pratica e piuttosto facile da aggirare, per esempio mentendo sull'età o fornendo un indirizzo email del presunto genitore che lo stesso minore gestisce.

Nel caso di TikTok, l'azienda ha cercato di tutelarsi da eventuali problemi inserendo nelle condizioni di utilizzo il **divieto di iscrizione ai minori di 13 anni**. Lo stratagemma, però, non sembra aver funzionato.

TikTok, infatti, è stata recentemente sanzionata negli Stati Uniti (dove il **Children's Online Privacy Protecion Act** prevede un sistema simile al GDPR) con una multa di **5,7 milioni di dollari** per non aver vigilato sul rispetto delle condizioni. All'azienda, nel dettaglio, è stato contestato il fatto di non aver bloccato contenuti condivisi da utenti che avevano palesemente un'età inferiore ai 13 anni.

La procedura avviata nel Regno Unito, però, rischia di essere ancora più pesante. Il mancato rispetto del GDPR, infatti, può portare a una sanzione pari al 4% del fatturato mondiale dell'azienda multata. **Per TikTok si parlerebbe di 20 milioni**

di euro di multa.

Le preoccupazioni delle autorità, soprattutto, si concentrano sulla possibilità che i minori iscritti al servizio possano essere contattati direttamente da adulti che potrebbero approfittare dell'ingenuità dei ragazzi per circuirli allo scopo di indurli a condividere con loro informazioni personali o contenuti sessualmente espliciti.

Un fenomeno tristemente noto, che negli ultimi tempi sta però vivendo preoccupanti evoluzioni. Secondo l'**FBI**, per esempio, negli Stati Uniti si stanno moltiplicando i casi di estorsioni ai danni di minori che in un primo momento vengono convinti a condividere video o immagini compromettenti e poi **vengono ricattati con la minaccia di renderli pubblici**.

Insomma: oltre ai "normali" predatori sessuali, alla lista delle minacce si stanno aggiungendo criminali senza scrupoli, che approfittano della vulnerabilità dei minori per ottenere guadagni illeciti. Allo schifo non c'è mai fine.

Condividi l'articolo

Android: 182 app malevole su Google Play e altri store

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/05/tik-tok-rischia-unaltra-multa-per-violazione-della-privacy/

ASSO DPO, Matteo Colombo (Presidente) ‘Con la privacy in Italia 50mila nuovi posti di lavoro’

L’Assemblea nazionale di **ASSO DPO**, principale associazione italiana dei Data Protection Officer, riunita il 2 luglio 2019 a Milano ha eletto il nuovo Comitato Direttivo e confermato per il triennio 2019 – 2022 **Matteo Colombo** quale Presidente della stessa.

A parere di Matteo Colombo: “*la sfida associativa sarà accompagnare i professionisti della data protection ad accrescere la loro competenze e conoscenze del Regolamento GDPR, di altre disposizioni dell’Unione o degli Stati membri relative alla protezione dei dati. La difesa dei dati è uno dei punti cruciali della società digitale e un punto di confronto importante fra aziende, istituzioni e consumatori. Questa nuova professione, continua Colombo, ha portato solo in Italia più di 50.000 nuovi posti di lavoro in un anno e secondo uno studio di IAPP – International Association of Privacy Professional – sono più di 500.000 i DPO in Europa; una professione del nuovo millennio che va oltre i confini, e per la quale è necessario fare rete su scala internazionale*”.

A sei anni dalla fondazione, ASSO DPO – Associazione dei Data Protection Officer, che conta quasi 1000 iscritti ed è iscritta al registro **MISE**, continua a sostenere e sviluppare l’attività dei DPO, dei Consulenti della Privacy, dei Responsabili della Protezione dei Dati, mediante il confronto e lo scambio di informazioni tra gli associati.

Nell’ultimo mandato ricordiamo l’ammissione dell’associazione in **CEDPO** (Confederazione Europea delle data protection

organizations) e l’organizzazione a Milano del 5° Congresso Internazionale Annuale che riunisce a maggio il gotha dei professionisti della privacy.

https://www.key4biz.it/asso-dpo-matteo-colombo-rieletto-presidente-con-la-privacy-in-italia-50mila-nuovi-posti-di-lavoro/263901/

Smart home: in Europa ce ne sono 21 milioni, restano i dubbi su privacy e sicurezza

Il mercato europeo della domotica sta crescendo rapidamente, trainato soprattutto dai nuovi *smart objects*, dalla sensoristica e la videosorveglianza per la sicurezza *indoor/outdoor*. In una parola, è l’internet delle cose a guidare la trasformazione digitale delle nostre abitazioni.

Secondo un nuovo studio IDC, le spedizioni sul mercato europeo sono arrivate a 21,3 milioni nel primo trimestre 2019, con un aumento del 23,9% sull’anno passato.
Il podio del mercato degli oggetti intelligenti, interconnessi tra loro e con la rete, vede Google al primo posto, con il 16,8% delle quote, Samsung sul secondo gradino, attestata al 13,4%, e Amazon sul terzo, con il 13,7%.
Seguono LG (10%) e Sony (5,8%) che chiudono la Top 5 del settore.

Al momento, le *smart home* europee si definiscono per alcune

tipologie di tecnologie, tra cui le *smart tv* e i *digital media adapters* per il *video entertainment* (+11,2%), gli *smart speakers*, che sono cresciuti notevolmente (+58%), ma anche i sistemi di illuminazione, di sicurezza e i contatori intelligenti hanno visto crescere le proprie quote (+10%), raggiungendo il 21% del mercato complessivo.

La *smart home* è dunque una realtà sempre più diffusa e desiderata. Secondo stime Markets and Markets, **il mercato mondiale dei prodotti smart home dovrebbe crescere di valore dai 76,6 miliardi del 2018 ai 151,4 miliardi attesi per il 2024**.

Secondo un'indagine condotta da Houzz Italia, però, anche se molti hanno dichiarato di documentarsi di fatto sui sistemi IoT (*Internet of Things*) di nuova generazione che entrano in casa, **il 47% ancora non ha acquistato una soluzione di questo tipo**.
Un altro 9% crede proprio che la casa connessa sia ancora un "*esperimento*" e non si fida dell'internet delle cose.
Un 33% si ritiene "*proattivo*", tiene sotto controllo le novità e ha già iniziato ad acquistare 1-2 prodotti smart per la casa. Solo l'11% ha deciso di avere una vera *smart home* e ha già installato tra 5 e 6 prodotti tecnologici.
Anche qui, le applicazioni più desiderate sono quelle legate alla videosorveglianza e alla predisposizione di sistemi di antifurto. **Il 41% vorrebbe installare allarmi e domotica di controllo per aumentare la sicurezza della propria abitazione**, il 31% desidera invece un sistema per controllare da remoto gli apparecchi della casa e gestire facilmente i diversi elettrodomestici. C'è anche un 28% che ama il comfort, e non sarebbe affatto dispiaciuto di poter comodamente comandare dal

divano impianti luce, oscuranti o sistemi termici.

A frenare la diffusione delle smart home, però ci sono ancora degli ostacoli abbastanza rilevanti: **il 32% teme per la propria privacy** e ha paura che i propri dati sensibili vengano diffusi in maniera involontaria; **il 27% crede che queste nuove tecnologie siano ancora troppo costose**; il 18% teme di non saperne sfruttare appieno le potenzialità e, infine, il 10% crede che questi sistemi diventino obsoleti in tempi troppo rapidi. C'è anche un 11%, infine, che non sente il bisogno di aggiungere elementi domotici alla propria abitazione e per ora se la cava benissimo con le proprie vecchie abitudini.

https://www.key4biz.it/smart-home-in-europa-ce-ne-sono-21-milioni-restano-i-dubbi-su-privacy-e-sicurezza/263880/

Italy Fines Facebook Over Cambridge Analytica Case

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5Hx2wtR892o/italy-fines-facebook-over-cambridge-analytica-case