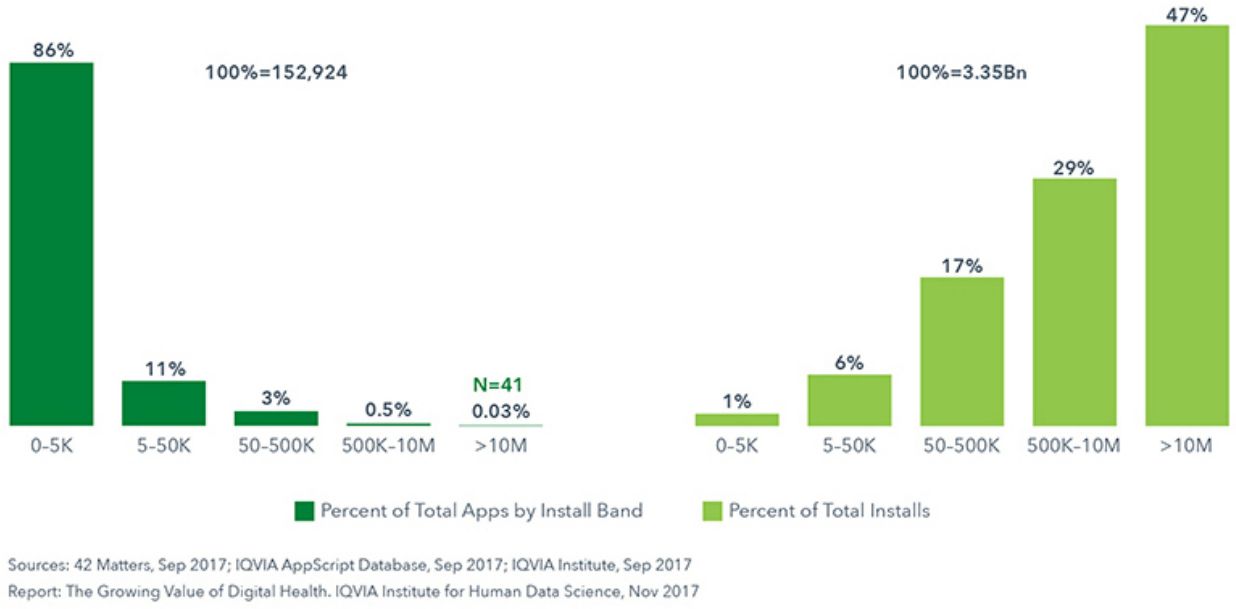
Irish Regulator Investigates Facebook Over Exposed Passwords

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5T4iX9u-vBU/irish-regulator-investigates-facebook-over-exposed-passwords

---

Le app e la salute, come la pensano gli italiani?

Rubrica settimanale **SosTech**, frutto della collaborazione tra **Key4biz** e **SosTariffe**. Per consultare gli articoli precedenti, **clicca qui**.
Il confine tra l'effettiva utilità per il singolo e la quantità di **informazioni** che siamo disposti a divulgare su di noi è il grande tema digitale di questi anni, ma è anche un evidente paradosso. Non ci facciamo particolari problemi quando si tratta di permettere ai siti e alle diverse applicazioni che popolano i nostri **computer** e **dispositivi mobili** di accedere a più o meno tutti i nostri **dati sensibili**; basta che ci permettano di caricare le foto della cena al ristorante della sera prima o di controllare dove lavora l'ex collega. Ma a quanto pare siamo molto più restii se in ballo c'è qualcosa di meno *glamour* come **la nostra salute**, che potrebbe invece beneficiare di un accesso condiviso ai valori che possono segnalare per tempo se qualcosa non va.



I dati sanitari? Il 60% non li vuole condividere

Secondo l'indagine **Tech4Life** presentata qualche settimana fa e condotta da **Community Media Research** in collaborazione con **Confindustria Dispositivi Medici**, infatti, **6 italiani su 10** non sono d'accordo a condividere i dati sulla propria salute, malgrado il parere sulla prevenzione, in generale, sia più che positivo (9 italiani su 10 si dicono favorevoli agli screening e più di 6 su 10 negli ultimi 5 anni si sono volontariamente sottoposti a esami diagnostici come le analisi del sangue). È per questo, forse, che quando una delle funzionalità più interessanti dell'**Apple Watch 4** – la possibilità di avere un **EKG** in 30 secondi – ha fatto il suo esordio in Italia, la maggior parte degli utenti ha, tutto sommato, fatto spallucce.

I rischi di Dr. Google

Tutto questo senza dimenticare che la Rete, quando si tratta di salute, è sollecitata dagli utenti, e non poco: il **57% degli italiani** si rivolge a **Google** per avere più informazioni su patologie o specifici disturbi, in molti casi – e questo è

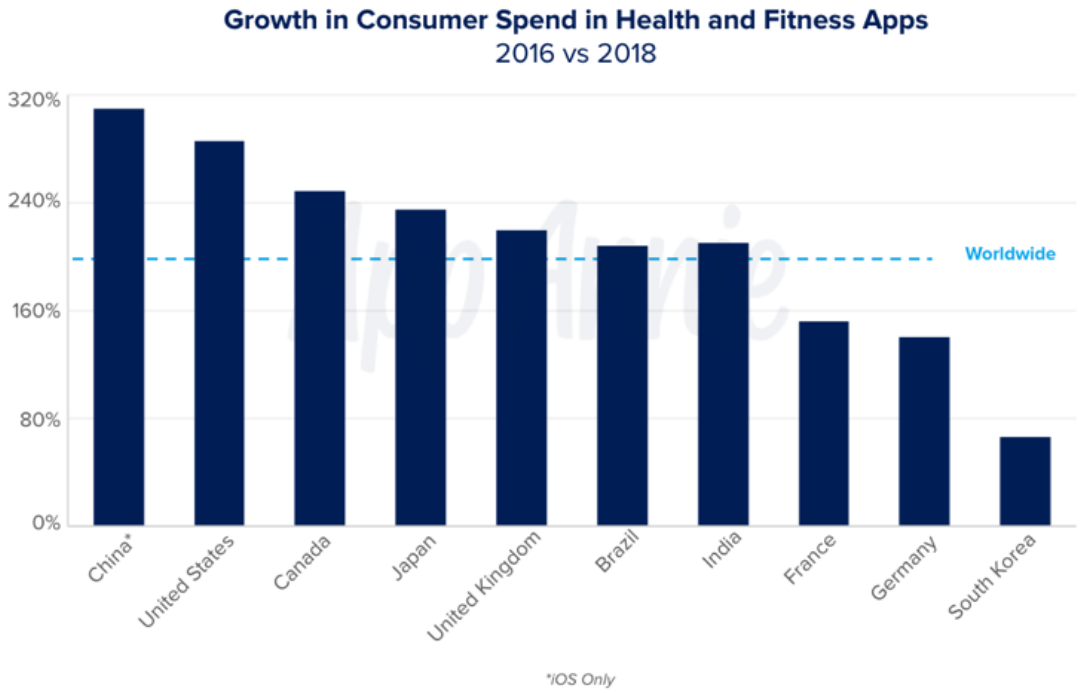
davvero allarmante – accontentandosi della risposta trovata in un forum non specialistico e rinunciando così a recarsi dal medico, risparmiando forse tempo e denaro, ma rischiando moltissimo: sottovalutazione (o sopravvalutazione) del disturbo, autodiagnosi e automedicazioni errate e, più in genere, **rimedi peggiori dei mali**, con ritardi che possono essere fatali quando poi diventa inevitabile l'intervento del dottore.

Il mercato c'è. Secondo gli ultimi dati di **App Annie**, i download di applicazioni mediche nel 2018 sono arrivati a **400 milioni**, il 15% in più rispetto al 2016. Un simile aumento si è verificato sia nei mercati più maturi, come gli **Stati Uniti**, il **Regno Unito** e la **Francia** (rispettivamente +35%, +40% e +40%), sia in quelli emergenti (**Brasile**, **India** e **Indonesia**, rispettivamente con +35%, +65% e +110%). La spesa è addirittura triplicata, anche se bisogna tenere conto che della categoria fanno parte anche le applicazioni di **fitness**, legate sì alla salute ma in modo più indiretto.



Anche in caso di emergenze, avere sempre con sé il proprio smartphone o comunque uno strumento in grado di comunicare in mobilità, con l'aggiunta di canoni sempre più bassi per **internet mobile** (su **SosTariffe.it** è sempre possibile confrontare tra di loro gli abbonamenti più convenienti), è in effetti **un valore aggiunto**, soprattutto se i dispositivi sono così a stretto contatto con noi (i *wearables*, appunto) da essere in grado di rilevare i nostri parametri biometrici e

avvertirci con una notifica al momento giusto. O addirittura effettuare una chiamata di emergenza, se abbiamo perso i sensi in seguito a una caduta o a un malore.



Il futuro dell’e-health

L’**e-health** rimane uno dei settori più promettenti per quanto riguarda le innovazioni in campo tech, soprattutto da quando i *wearable* sono diventati parte della routine quotidiana e anche chi aveva smesso di utilizzare orologi da anni, accontentandosi dell’indicazione dell’ora sul cellulare, trova nuovamente naturale arrotolarsi un cinturino al polso ogni mattina. Un’occasione perfetta per **monitorare il nostro battito cardiaco** nelle diverse fasi della giornata, a riposo e sotto sforzo, ma anche la qualità del sonno o il tempo trascorso seduti al computer, senza sgranchirsi i muscoli. Di più: gli operatori sanitari possono controllare in remoto la condizione dei malati in qualsiasi momento.

Tutto ciò si chiama “**medicina partecipativa**”, e si prevede – secondo la recente ricerca di **Juniper Research** dal titolo “Digital Health: Disruptor Analysis, Country Readiness e

Technology Forecast 2018-2023” – che la spesa annuale per health tracker e dispositivi indossabili raggiunga i **20 miliardi di dollari** entro il 2023, e saranno **5 milioni** i pazienti monitorati a distanza dagli operatori sanitari proprio grazie a questi apparecchi.

In Italia la strada da fare è ancora lunga: il dispositivo più utilizzato per la medicina partecipativa è ovviamente lo **smartphone** (14,3%), ma è solo il 7,6% della popolazione a utilizzare un’applicazione per monitorare la propria salute. Com’era prevedibile, i più scettici sono soprattutto gli italiani delle fasce d’età più anziane, mentre il 49,6% dei giovani tra i 18 e i 34 anni si dichiara disposto a mettere in Rete i propri dati sanitari.

La privacy e i dati sanitari

La sfiducia non riguarda, fortunatamente, tutto ciò che coinvolge i propri dati e la salute in versione digitale: sono 11 milioni e mezzo infatti gli italiani che hanno dato il consenso all’apertura di un proprio **fascicolo sanitario elettronico**, utilizzato ormai in 19 regioni su 20. È coinvolto pure il **GDPR**, ovvero il nuovo regolamento UE in materia di protezione dei dati, tanto che il Garante ha dovuto chiarire che i medici potranno trattare i dati dei pazienti per **finalità di cura** senza richiedere il loro consenso, ma saranno comunque tenuti a fornire informazioni complete sull’uso dei dati. Insomma, il nodo di **privacy e salute** è al cuore di una situazione molto complessa.

Per questo **Massimiliano Boggetti**, da poco presidente di **Confindustria Dispositivi Medici**, a margine della presentazione della ricerca Tech4Life ha dichiarato che «*i cittadini devono essere informati in modo corretto sulle tecnologie mediche a beneficio della propria salute e sulle possibilità di miglioramento della qualità della propria vita che la nuova medicina offre loro. Per questo con l’indagine*

Tech4life abbiamo voluto fare un punto sulla consapevolezza degli italiani del valore delle tecnologie e delle nuove frontiere della medicina. Vogliamo favorire la divulgazione coinvolgendo il mondo scientifico e le istituzioni, che svolgono un ruolo cruciale in questo processo». Come ha concluso Boggetti, è necessario «*fare in modo che l'informazione corretta ed equilibrata sulle nuove possibilità di prevenzione e cura diventi sempre più centrale soprattutto sul web, dove le persone cercano sempre più spesso la risposta ai proprio bisogni di salute*».

Fonti:

https://www.key4biz.it/le-app-e-la-salute-come-la-pensano-gli-italiani/255794/

Canada Privacy Watchdog Taking Facebook to Court

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/fyKqCodB8dQ/canada-privacy-watchdog-taking-facebook-court

---

Facebook Anticipates an FTC Privacy Fine of up to $5

Billion

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/oVnZUydeBAY/facebook-anticipates-ftc-privacy-fine-5-billion

---

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

Seduto al tavolino di un bar accanto gli uffici di **Italiaonline** ad Assago, un hacker ha rubato credenziali di accesso alle caselle di posta elettronica di 1 milione e 400.000 clienti dei servizi di **Libero Mail** e di **Virgilio Mail.**

Sono questi gli esiti della vicenda raccontata dal *Corriere della Sera dell'attacco hacker avvenuto nel milanese,* messo a punto da un hacker 24enne.

Il criminale informatico, secondo la ricostruzione del Corriere, sarebbe entrato nelle rete Wifi dell'azienda attraverso l'uso di un computer portatile e di una grande antenna, usando la password di un dipendente e avrebbe iniziato l'attacco, riuscendo a violare **1 milione e 400mila dati.**

Sulla vicenda, secondo il quotidiano, sta indagando la **Procura di Milano** e sta svolgendo una apposita ispezione il **Garante per la privacy,** avvisato del Data Breach da Italiaonline come impone il GDPR, il nuovo regolamento europeo.



L'azienda ha fatto sapere che il sistema antintrusione ha funzionato dichiarando che "*allo stato attuale, non ci sono utenti che abbiano segnalato accessi indesiderati alla propria posta*".

Il rischio, invece, si palesa per chi usa la stessa password della posta elettronica per accede ad altre piattaforme, quali conti bancari: in questo caso è necessario cambiare immediatamente tutte le parole chiave, per evitare che i pirati informatici si introducano nella piattaforma bancaria.

Consigli sulle password

Avere password differenti per ogni account, email o conti correnti è una buona regola per non essere vittime di criminali informatici e dover fare i conti con furti di dati. E allora ecco qualche semplice consiglio su come ricordare password complesse, in modo da poter ricordare tutte le password più importanti.

1. Creare una "static string" (quella parte di password che resta sempre uguale)

1. Pensare ad una frase, al testo di una canzone, alle citazioni di un film, ad una filastrocca o a qualcosa di simile, che sia facile da ricordare;

2. Prendere la prima lettera delle prime tre o prime cinque parole;
3. Aggiungere, tra una lettera e l'altra, un carattere speciale (ad esempio: #, @, / e simili).
4. Da questo momento in poi, è possibile basare tutte le proprie password uniche su questa singola stringa di caratteri.

2. Sfruttare la potenza dell'associazione di idee

1. In caso di necessità di una password per uno degli account online in uso (ad esempio per Facebook, Twitter, eBay, per l'online banking, per lo shopping online o i siti di videogiochi…), si deve prendere nota della prima parola che si associa ad un determinato sito o ad una certa piattaforma.
2. Ad esempio, se si sta creando una password per l'account di Facebook, si potrebbe associare al social media il colore blu, presente nel logo. Basterebbe, quindi, aggiungere la parola "blu", magari in lettere maiuscole, alla fine della "static string" creata in precedenza

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

---

Facebook fights to "shield Zuckerberg" from punishment

in US privacy probe



Enlarge / Facebook CEO Mark Zuckerberg leaving the Merrion Hotel in Dublin after meeting with Irish politicians to discuss regulation of social media on Tuesday, April 2, 2019.
Getty Images | NurPhoto

reader comments

171 with 70 posters participating

Share this story

Federal Trade Commission officials are discussing whether to hold Facebook CEO Mark Zuckerberg personally accountable for Facebook’s privacy failures, according to reports by The Washington Post and NBC News. Facebook has been trying to protect Zuckerberg from that possibility in negotiations with the FTC, the Post wrote.

Federal regulators investigating Facebook are “exploring his past statements on privacy and weighing whether to seek new, heightened oversight of his leadership,” the Post reported, citing anonymous sources who are familiar with the FTC discussions.

“The discussions about how to hold Zuckerberg accountable for Facebook’s data lapses have come in the context of wide-ranging talks between the Federal Trade Commission and Facebook that could settle the government’s more than year-old probe,” the Post wrote.

According to NBC, FTC officials are “discussing whether and how to hold Facebook Chief Executive Mark Zuckerberg personally accountable for the company’s history of mismanaging users’ private data.” However, NBC said its sources “wouldn’t elaborate on what measures are specifically under consideration.”

According to the Post, one idea raised during the probe “could require [Zuckerberg] or other executives to certify the company’s privacy practices periodically to the board of directors.”

But it’s not clear how likely the FTC is to target Zuckerberg in a final settlement, and “Facebook has fought fiercely to shield Zuckerberg as part of the negotiations, one of the sources familiar with the probe said,” the Post wrote.

Facebook dismisses “recycled” storyline

When contacted by Ars, Facebook said, “These storylines have been recycled for some time.” The company cited an April 2 Politico story as an example. But the Politico story was more speculative: it said the FTC could use its authority to seek “new, more aggressive privacy auditors; or even management

changes, up to the level of Chairman and CEO Mark Zuckerberg." And unlike the new Post and NBC stories, Politico's article merely discussed the FTC targeting Zuckerberg as a theoretical possibility and didn't assert that FTC investigators themselves are considering a punishment for Zuckerberg.

As for the FTC investigation, Facebook told Ars that it hopes "to reach an appropriate and fair resolution" with the commission.

The FTC reached a settlement with Facebook in 2011 over charges that it deceived users by failing to keep privacy promises. During the lead-up to that settlement, the FTC "considered, then backed down, from putting Zuckerberg directly under order," the Post wrote. "Had it done so, Zuckerberg could have faced fines for future privacy violations."

The FTC's current investigation began in March 2018, after revelations that up to 87 million users' information was improperly shared with Cambridge Analytica. The FTC investigation focuses on whether Facebook violated the terms of its 2011 settlement with the FTC. That settlement prohibited Facebook from misrepresenting the privacy or security of user information, and it required Facebook to get consumers' express consent before making changes that override their privacy settings.

Republicans hold a 3-2 majority on the FTC. Democratic Commissioner Rohit Chopra wrote in a May 2018 memo that "the FTC should hold individual executives accountable for order violations in which they participated, even if these individuals were not named in the original orders."

https://arstechnica.com/?p=1493551

Elezioni europee, il Garante Privacy detta le regole per la propaganda

In vista delle prossime consultazioni elettorali europee, anche alla luce del nuovo quadro normativo introdotto dal **Regolamento Ue** in materia di protezione dei dati personali, il **Garante Privacy** ha approvato uno specifico provvedimento che fissa le regole per il corretto uso dei dati degli elettori da parte di partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati.

Nel provvedimento, in corso di pubblicazione sulla G.U., l'Autorità si sofferma, in particolare, sull'uso di messaggi politici e propagandistici inviati agli utenti dei social network (come **Facebook** e **Linkedin**) o su altre piattaforme di messaggistica (come **Skype, Whatsapp, Messenger**), ribadendo che tale uso deve rispettare le norme in materia di protezione dei dati Come dimostrato da casi recenti di profilazione massiva degli elettori, è fondamentale proteggere il processo elettorale ed evitare rischi di interferenze e turbative esterne.

Queste, in sintesi, le indicazioni del Garante.

Dati utilizzabili senza consenso

Per contattare gli elettori ed inviare materiale di propaganda, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono usare senza consenso i dati contenuti nelle liste elettorali detenute dai Comuni. Possono essere usati anche altri elenchi e registri pubblici

in materia di elettorato passivo e attivo (es. elenco dei cittadini residenti all'estero aventi diritto al voto o degli elettori italiani che votano all'estero per le elezioni del Parlamento europeo) e altre fonti documentali, detenute da soggetti pubblici, accessibili da chiunque. Si possono utilizzare senza previo consenso anche i dati degli aderenti a partiti o movimenti politici o di soggetti che hanno con essi contatti regolari.



Dati utilizzabili solo con il previo consenso

E' necessario il consenso informato invece per poter utilizzare recapiti telefonici contenuti negli elenchi telefonici e quindi per effettuare chiamate o inviare sms e mail. Obbligo di consenso anche per poter trattare i dati reperibili sul web, come, ad esempio: quelli presenti nei profili dei social network e di messaggistica; quelli ricavati da forum e blog; quelli raccolti automaticamente con appositi software (web scraping); le liste di abbonati di un provider; i dati pubblicati su siti web per specifiche finalità di informazione aziendale, commerciale o associative.

Necessario il consenso anche per i dati raccolti nell'esercizio di attività professionali, di impresa o nell'ambito della professione sanitaria.

Serve il consenso anche per l’utilizzo dei dati di persone contattate in occasione di singole specifiche iniziative (es. petizioni, proposte di legge, referendum, raccolte di firme) e di quelli di sovventori occasionali.

Chi intende utilizzare, acquisendole da terzi, liste cosiddette “consensate” (dati raccolti previa informativa e consenso), è tenuto a verificare che siano stati effettivamente rispettati gli adempimenti di legge. Lo stesso vale per i servizi di propaganda elettorale curata da terzi a favore di movimenti, partiti, candidati.

Dati non utilizzabili

Non sono in alcun modo utilizzabili i dati raccolti o usati per lo svolgimento di attività istituzionali come l’anagrafe della popolazione residente; gli archivi dello stato civile; le liste elettorali di sezione già utilizzate nei seggi; gli elenchi di iscritti ad albi e collegi professionali; gli indirizzi di posta elettronica tratti dall’Indice nazionale dei domicili digitali. Non sono utilizzabili i dati resi pubblici sulla base di atti nomativi per finalità di pubblicità o di trasparenza come, ad esempio quelli presenti nei documenti pubblicati nell’ albo pretorio on line; quelli relativi agli esiti di concorsi; quelli riportati negli organigrammi degli uffici pubblici contenenti recapiti telefonici ed indirizzi mail. Non si possono infine utilizzare dati raccolti da titolari di cariche elettive e di altri incarichi pubblici nell’esercizio del loro mandato elettivo o dell’attività istituzionale.

Informativa a cittadini

Gli elettori devono essere sempre informati sull’uso che verrà fatto dei loro dati personali. Se i dati sono ottenuti direttamente presso gli interessati, l’informativa va data all’atto della raccolta. Per i dati acquisiti da altre fonti è

necessario che gli interessati siano informati in un tempo ragionevole al massimo entro un mese. Qualora tale adempimento sia però impossibile o comporti uno sforzo sproporzionato, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono esimersi dall'informativa, a condizione che adottino misure adeguate per tutelare i diritti e le libertà dei cittadini, utilizzando, per esempio, modalità pubbliche di informazione.

Sanzioni

Il Garante ricorda che la violazione della disciplina sui dati comporta sanzioni che possono essere anche molto onerose, come previsto dal Gdpr.
Inoltre, in ragione delle recenti modifiche introdotte dal legislatore europeo al Regolamento Ue 1141/2014 sullo statuto e il finanziamento di partiti e fondazioni politiche europee, l'Autorità europea per i partiti politici e le fondazioni politiche europee – se viene a conoscenza di una decisione di un'Autorità nazionale di protezione dati da cui sia possibile evincere che la violazione delle norme sia connessa ad attività volte ad influenzare o a tentare di influenzare l'esito delle elezioni europee – è tenuta ad avviare una procedura di verifica, all'esito della quale potranno essere applicate sanzioni pecuniarie che potrebbero ammontare, nei casi più gravi, al 5% del bilancio annuale del partito o della fondazione.

https://www.key4biz.it/elezioni-europee-il-garante-privacy-detta-le-regole-per-la-propaganda/255344/

Facebook Collected Email Contacts of 1.5 Million Users Without Consent

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/pCSLNGq4S2w/facebook-collected-email-contacts-15-million-users-without-consent

---

In new gaffe, Facebook improperly collects email contacts for 1.5 million



reader comments

161 with 117 posters participating

Share this story

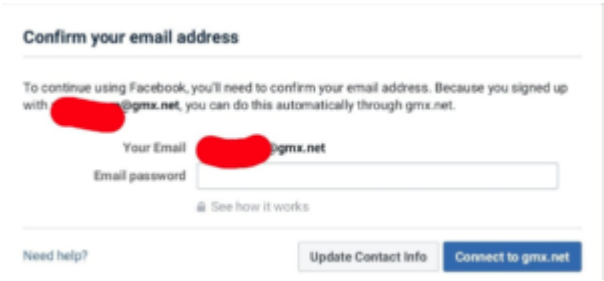
Facebook’s privacy gaffes keep coming. On Wednesday, the social media company said it collected the stored email address lists of as many as 1.5 million users without permission. On Thursday, the company said the number of Instagram users affected by a previously reported password storage error was in the “millions,” not the “tens of thousands” as previously estimated.

Facebook said the email contact collection was the result of a highly flawed verification technique that instructed some users to supply the password for the email address associated with their account if they wanted to continue using Facebook. Security experts almost unanimously criticized the practice, and Facebook dropped it as soon as it was reported.

In a statement issued to reporters, Facebook wrote:

> *Earlier this month we stopped offering email password verification as an option for people verifying their account when signing up for Facebook for the first time. When we looked into the steps people were going through to verify their accounts we found that in some cases people's email contacts were also unintentionally uploaded to Facebook when they created their account. We estimate that up to 1.5 million people's email contacts may have been uploaded. These contacts were not shared with anyone and we're deleting them. We've fixed the underlying issue and are notifying people whose contacts were imported. People can also review and manage the contacts they share with Facebook in their settings.*

Business Insider first reported the harvesting of the email contacts. When users gave their passwords to Facebook, the publication said, they received a message declaring that Facebook was importing their contacts. The collection happened without asking for permission first.



While Facebook's statement referred to the email verification step as an "option," the language displayed in a tweeted screenshot of the message (right) told users: "To continue using Facebook, you'll need to confirm your email address." Many users, it seems, could be forgiven if they thought supplying their password was a condition of using the social media site. A Facebook representative told Ars that these users could also have confirmed their accounts with a code sent to their phone or a link sent to their email had they

clicked the “need help” button in the pop-up window.

Hashing it out

Facebook has said it didn’t store the passwords, but in yet another Facebook privacy blunder disclosed last month, the company confirmed that it improperly stored hundreds of millions of user passwords in plain text rather than as cryptographic hashes. Hashes are long strings of random-looking text that are generated by passing a password, message, or file through an algorithm. Because hashes can’t be cryptographically reversed, security experts say they are the only secure way to store them.

In late March, Facebook said the plaintext password error affected hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users. The Facebook disclosure was updated on Thursday to say the number of affected Instagram accounts was much higher.

“Since this post was published, we discovered additional logs of Instagram passwords being stored in a readable format,” Thursday’s update said. “We now estimate that this issue impacted millions of Instagram users. We will be notifying these users as we did the others. Our investigation has determined that these stored passwords were not internally abused or improperly accessed.”

Facebook has been buffeted by a series of privacy gaffes since January 2018. That’s when a New York Times expose revealed that political firm Cambridge Analytica improperly harvested tens of millions of Facebook users’ data. Two months later, reporting showed that the social media site collected metadata from years’ worth of calls and texts users made or sent with Android phones.

Last month, CEO Mark Zuckerberg said he planned to rebrand the

site he founded as a privacy service.

https://arstechnica.com/?p=1493219

State Launches Online Data Survey as Part of Facebook Probe

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/0t9U9Y6QPRg/state-launches-online-data-survey-part-facebook-probe