

## Studio IBM sul Futuro delle Identità Digitali: i Millennial trasformano il panorama delle soluzioni di autenticazione

Oggi gli utenti che si collegano alle app danno maggiore priorità alla sicurezza. I giovani sono indulgenti rispetto all'uso delle password e più inclini all'autenticazione a più fattori e biometrica

**Cambridge - 29 gen 2018:** – IBM Security annuncia uno studio<sup>[1]</sup> che analizza, su scala mondiale, le tendenze dei consumatori rispetto a identità e autenticazioni digitali. Dallo studio emerge che oggi le persone, quando accedono a dispositivi e app, privilegiano la sicurezza rispetto alla praticità. Emergono inoltre differenze generazionali: i giovani adulti riservano meno attenzione alla gestione delle password tradizionali e sono invece più propensi a utilizzare soluzioni di autenticazione biometriche e a più fattori e gestori di password per aumentare la propria sicurezza personale.

Poiché i Millennial diventeranno presto la generazione più rappresentata nell'ambito della forza lavoro<sup>[2]</sup>, queste tendenze potranno influire sul modo in cui i datori di lavoro e le aziende tecnologiche forniranno l'accesso a dispositivi e applicazioni nel prossimo futuro. Nel complesso, gli intervistati riconoscono i vantaggi che le tecnologie biometriche, quali i lettori di impronte digitali, le scansioni facciali e il riconoscimento vocale, hanno rispetto alla continua crescita delle minacce alla propria identità digitale.

Nel realizzare lo studio *Future of Identity* gli esperti di IBM Security hanno intervistato quasi 4.000 adulti provenienti da USA, dalla regione Asia-Pacifico (APAC) e dall'Europa per ottenere informazioni sui punti di vista dei consumatori riguardo all'autenticazione. Ecco alcune importanti conclusioni:

- **La sicurezza supera la praticità:** nell'utilizzo delle applicazioni, in particolare quando si tratta di app legate al denaro<sup>[3]</sup>, la sicurezza ha la massima priorità.
- **La biometria è destinata a diventare dominante:** il 67% degli intervistati si sente oggi a proprio agio nell'utilizzare l'autenticazione biometrica, mentre l'87% dichiara che utilizzerà volentieri queste tecnologie in futuro.
- **I Millennial sono già oltre le password:** sebbene il 75% dei Millennial<sup>[4]</sup> non abbia problemi con le soluzioni biometriche, meno della metà utilizza password complesse e il 41% riutilizza le stesse password. Le generazioni precedenti mostravano maggiore attenzione nella creazione delle password, ma erano meno inclini ad adottare soluzioni di autenticazione a più fattori o biometriche.
- **APAC in testa sul fronte della biometria:** gli intervistati nei paesi dell'Asia-Pacifico si sono rivelati i più esperti e quelli maggiormente a proprio agio con l'autenticazione biometrica, mentre gli USA hanno mostrato di essere parecchio indietro in queste aree.

La continua evoluzione delle tecnologie e delle minacce informatiche mette a rischio i tradizionali metodi di accesso basati su password e informazioni personali per autenticare le nostre identità online. Nel 2017, le violazioni di dati hanno rivelato informazioni personali, password e persino numeri di previdenza sociale per milioni di consumatori. A ciò si aggiunge che l'utente medio di Internet gestisce oltre 150 account online che richiedono una password, numero che si prevede salirà a 300 account nei prossimi anni.<sup>[5]</sup>

*“In seguito alle numerose violazioni di dati personali altamente sensibili, non c'è più alcun dubbio che le stesse informazioni che abbiamo utilizzato in passato per dimostrare la nostra identità online sono ora un segreto condiviso nelle mani degli hacker”,* ha dichiarato Limor Kessem, Executive Security Advisor, IBM Security. *“Poiché i consumatori riconoscono l'inadeguatezza delle password e attribuiscono una maggiore priorità alla sicurezza, i tempi sono maturi per adottare metodi più avanzati in grado di dimostrare l'identità*

*digitale su più livelli e di essere adattati in base al comportamento e al rischio.”*

## **Priorità alla sicurezza e biometria più sicura delle password**

I risultati del sondaggio in merito a sicurezza, praticità e privacy mostrano che per la maggior parte delle applicazioni, in particolare per quelle legate al denaro, alla sicurezza viene attribuita maggiore importanza rispetto alla privacy e alla praticità. In particolare:

- La sicurezza è stata ampiamente classificata come la priorità principale per le app relative al settore bancario, agli investimenti e alla gestione del denaro in generale; per queste categorie in media il 70% ha scelto la sicurezza come priorità assoluta, il 16% ha scelto la privacy e il 14% ha scelto la praticità.
- La sicurezza è stata considerata di massima priorità anche per i marketplace, le app per il lavoro e la posta elettronica.
- Per le app dei social media, le priorità sono diverse, con la praticità che ha guadagnato un leggero vantaggio (scelta dal 36%), seguita da sicurezza (34%) e privacy (30%).

Il sondaggio ha esaminato, inoltre, le opinioni dei consumatori sulla sicurezza dei vari metodi di accesso e ha rilevato che alcuni tipi di soluzioni di autenticazione biometrica sono considerate più sicure delle password; tuttavia, sicurezza e privacy rimangono le preoccupazioni principali nell'adozione della biometria.

- Il 44% ha classificato le soluzioni biometriche di rilevazione delle impronte digitali come uno dei metodi di autenticazione più sicuri; password e PIN sono stati considerati meno sicuri (rispettivamente 27% e 12%)
- Le maggiori preoccupazioni delle persone riguardo all'autenticazione biometrica sono la privacy (il modo in cui i dati vengono acquisiti e utilizzati, 55%) e la sicurezza (che altri possano utilizzare dati biometrici falsi per accedere ai propri account, 50%).[\[6\]](#)

## **Differenza di età: i Millennial utilizzano tecniche più nuove, mentre le generazioni precedenti sono in testa nella gestione delle password**

Il sondaggio ha rivelato diverse differenze generazionali quando si tratta di proteggere l'identità personale online. Gli adulti più anziani hanno mostrato abitudini migliori in termini di creazione delle password, mentre le giovani generazioni sono più inclini ad adottare gestori di password, soluzioni di autenticazione a più fattori o biometriche come metodi per proteggere i propri account online. Ciò potrebbe indicare che le giovani generazioni hanno meno fiducia nelle password e cercano invece metodi alternativi per proteggere i propri account.

- Solo il 42% dei Millennial utilizza password complesse che combinano caratteri speciali, numeri e lettere (rispetto al 49% di quelli di età pari o superiore a 55 anni) e il 41% riutilizza la stessa password più volte (rispetto al 31% di quelli di età superiore a 55 anni)
- In media, le persone di età superiore a 55 anni usano 12 password, mentre i post-millennials (età 18-20) usa in media solo 5 password, il che potrebbe indicare un tasso di riutilizzo maggiore
- Per i Millennial esiste una probabilità doppia di utilizzare un gestore di password (34%) rispetto a persone di età superiore a 55 anni (17%)
- È emerso che i Millennial sono più propensi ad attivare l'autenticazione a due fattori in seguito a una violazione (32% contro il 28% della popolazione generale).

I giovani adulti hanno anche mostrato la massima preferenza per la praticità: quasi la metà (47%) degli adulti sotto i 24 anni preferiscono un'esperienza di accesso più veloce a una forma di autenticazione più sicura. Questa potrebbe essere una delle ragioni per cui è più probabile che i giovani adottino l'autenticazione biometrica; infatti, il 75% dei Millennial ha dichiarato di essere favorevole a usare soluzioni di autenticazione biometrica rispetto al 58% di quelli oltre i 55 anni.

## **Nel mondo: influenza della posizione geografica su utilizzo delle password e prospettive di autenticazione**

Il sondaggio ha rilevato che la posizione geografica ha una forte influenza sulla percezione e sulla familiarità con le tecniche di autenticazione emergenti: la regione Asia-Pacifico è la più esperta e quella più disinvolta nell'utilizzo di metodi quali autenticazione a più fattori o biometrica. Gli USA sono i più arretrati in termini di conoscenza e familiarità riguardo alla maggior parte delle categorie. In particolare:

- Gli intervistati nell'APAC sono risultati i più propensi a dichiarare di essere informati sulle soluzioni di autenticazione biometrica (il 61% rispetto al 40% nell'UE e il 34% negli USA).
- È emerso anche che nell'APAC non hanno problemi a utilizzare oggi soluzioni biometriche (78% rispetto al 65% nell'UE e il 57% negli USA)
- L'Europa possiede le migliori prassi nella creazione delle password, con il 52% degli intervistati che utilizza password complesse (contro il 46% nell'APAC e il 41% negli Stati Uniti).
- Il 23% degli intervistati negli USA ha dichiarato di non essere interessato a utilizzare soluzioni di autenticazione biometrica ora o nel prossimo futuro, quasi il doppio della media globale

## **Il futuro delle identità digitali**

L'analisi contenuta nel rapporto di IBM Security indica in dettaglio che gli atteggiamenti rispetto all'autenticazione delle identità digitali sono molto varie e, sebbene sia in crescita l'accettazione di nuove forme di autenticazione come quelle biometriche, persistono le preoccupazioni, in particolare tra le generazioni meno giovani e le persone negli USA.

IBM consiglia alle organizzazioni di prendere atto di queste preferenze e di avvalersi di piattaforme di autenticazione di identità digitali in grado di offrire agli utenti la possibilità di scegliere tra diverse opzioni, ad esempio consentendo di passare da una notifica *push mobile* che si avvale di lettori di impronte digitali sul telefono o di un passcode da fornire una tantum. Le organizzazioni possono trovare un equilibrio tra le esigenze di sicurezza e praticità utilizzando anche approcci basati sul rischio, che attivino ulteriori punti di controllo dell'autenticazione in determinati scenari, ad esempio quando segnali comportamentali o attribuzioni di connessione (al livello di dispositivo, posizione geografica, indirizzo IP) segnalano un'attività anomala.

Inoltre, i dati rivelano che le generazioni più giovani danno meno importanza alla gestione delle password tradizionali e questo rappresenta una sfida per datori di lavoro e imprese che gestiscono l'accesso ai dati tramite password da parte di utenti Millennial. Mano a mano che aumenterà il numero dei Millennial e post-Millennial nella forza lavoro, le organizzazioni e le imprese dovranno adattarsi alla propensione delle nuove generazioni per le nuove tecnologie, consentendo un maggiore uso dei dispositivi mobili come fattore di autenticazione primario e integrando approcci che sostituiscano i metodi biometrici o l'utilizzo di token al posto delle password.

IBM Security offre suggerimenti ai consumatori su come proteggere la propria identità digitale in un [post blog](#)

[qui](#).

Per ulteriori dettagli sullo studio e consigli per le aziende affinché si preparino per il futuro dell'autenticazione, è possibile scaricare il rapporto completo all'indirizzo: [ibm.biz/FutureOfIdentity](http://ibm.biz/FutureOfIdentity)

### **Informazioni su IBM Security**

IBM Security offre un portfolio di offerta di prodotti e servizi per la protezione aziendale tra più avanzati e integrati del mercato. Il portfolio, supportato dalla ricerca IBM X-Force® di fama mondiale, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dispone di una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza tra le più grandi al mondo, monitora 35 miliardi di eventi di protezione al giorno in più di 130 Paesi e ha ottenuto oltre 3.000 brevetti di sicurezza. Per maggiori informazioni, visitare il sito: [www.ibm.com/security](http://www.ibm.com/security), seguire [@ibmsecurity](https://twitter.com/ibmsecurity) su Twitter o visitare il [blog di IBM Security Intelligence](#).

### **Informazioni sullo studio**

Lo studio è stato progettato con Ketchum Global Research and Analytics. La raccolta dei dati è stata svolta da Research Now. Il sondaggio è stato condotto tra il 21 ottobre e il 5 novembre 2017, con un margine di errore di +/- 2,0 per il campione USA e di +/- 3,07 per i campioni UE e APAC, all'intervallo di confidenza del 95%.

Il sondaggio online di 15 minuti ha totalizzato le risposte di 3.977 adulti negli Stati Uniti (USA), nell'Unione Europea (UE) e nella regione dell'Asia-Pacifico (APAC), con:

- USA: 1.976 intervistati
- UE: 1.004 intervistati (Regno Unito, Francia, Italia, Germania, Spagna)
- APAC: 997 intervistati (Australia, India, Singapore)

---

[1] I mercati oggetto del sondaggio comprendono Europa, Asia-Pacifico e Stati Uniti. [1] I mercati oggetto del sondaggio comprendono Europa, Asia-Pacifico e Stati Uniti.

[2] [ManPower Group, 2016](#)

[3] IBM Security: Studio sul futuro delle identità digitali: il 70% degli intervistati ha classificato la sicurezza come la priorità assoluta rispetto a praticità o privacy quando si accede ad app finanziarie (investimenti, app bancarie, gestione del denaro).

[4] "Millennials" si riferisce agli intervistati di 20-36 anni di età al momento del sondaggio (2017)

[5] [Dashlane, 2017](#)

[6] Il 55% degli intervistati era preoccupato di "come vengono utilizzati i dati raccolti"; il 50% era preoccupato riguardo alle "persone che usano la biometria falsa/ingannevole per accedere alle mie informazioni"

Contatti

**Claudia Ruffini**

