LastPass •••|

La psicologia delle password

Le pratiche (inadeguate) dei dipendenti che mettono a repentaglio le imprese.

Bisogna aumentare sicurezza e conformità senza complicare le cose

In un periodo in cui la sfera personale e quella professionale di noi tutti si vanno sovrapponendo con una rapidità senza precedenti, osservare pratiche adeguate in materia di password risulta fondamentale al successo e alla sicurezza di un'azienda. In un mondo in cui il lavoro non ha più confini, i team informatici sono chiamati ad adattarsi per garantire protezione alle credenziali del personale.

Il presente rapporto indaga le pratiche in materia di password di 3.750 professionisti di tutto il mondo e può aiutare le imprese a:

- **prestare più attenzione alla sicurezza** e migliorare l'approccio alle password
- **acquisire le migliori pratiche** per abolire il riutilizzo delle password e conservare le credenziali in modo sicuro
- **stabilire degli obiettivi** che consentano una sensibilizzazione efficace alla sicurezza in un contesto lavorativo remoto

Liberando i team informatici e il resto del personale dalle complicazioni, LastPass Business si rivela un alleato importante per l'organico di un'azienda: **consente di risparmiare tempo, offrendo ai dipendenti una gestione semplificata delle password, e garantisce agli amministratori vigilanza e intervento** con caratteristiche quali una reportistica avanzata e oltre 100 criteri di sicurezza personalizzabili.

Maggiori informazioni sono disponibili all'indirizzo lastpass.com/business.

La sicurezza delle password nel 2021: come superare le vulnerabilità umane

La pandemia di COVID-19 ha sconvolto gli ambienti di lavoro di milioni di persone in tutto il mondo: gli uffici tradizionali hanno dovuto chiudere, molte persone sono passate al lavoro agile e, non potendo andare da nessuna parte, hanno iniziato a trascorrere più tempo online.

I singoli individui e le aziende non hanno mai corso così tanti rischi
Gli hacker approfittano delle vulnerabilità umane e le sfruttano come mai prima d'ora. I tipi di attacchi sono cambiati a causa del numero elevato di persone che operano in smart working e passano più tempo in rete.

Secondo il Data Breach Investigations Report (DBIR) del 2021, i criminali informatici stanno prendendo sempre più spesso di mira i singoli individui e i loro dispositivi.

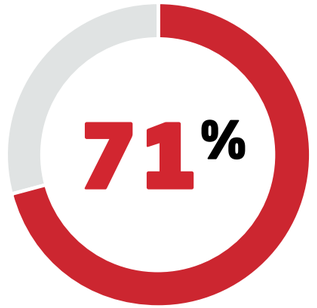
85%

La maggior parte delle violazioni di dati, pari a uno sconcertante 85%, è dovuta a un fattore umano (phishing, furto di credenziali o errore umano).

36%

Il 36% delle violazioni dello scorso anno è riconducibile al phishing – il che equivale a un aumento dell'11%.

Durante la pandemia:



Tasso di chi ha lavorato sempre o a volte in modalità remota.

Tasso di chi ha trascorso più tempo in rete per lavoro e intrattenimento personale.

Il sondaggio in breve

Questo rapporto di LastPass sulla psicologia delle password indaga le pratiche di sicurezza adottate in materia da 3.750 professionisti che operano in sette Paesi, ai quali è stato chiesto cosa ne pensassero della sicurezza online e quali pratiche adottassero al riguardo.

Paesi coinvolti nel sondaggio:

- Stati Uniti
- Regno Unito
- Germania
- Francia
- Australia
- Singapore
- India

C’è tanta consapevolezza, ma non sempre viene messa in pratica

Cosa pensano le persone...

79%

Il 79% ammette che le password compromesse sono un motivo di preoccupazione...

92%

Il 92% sa bene che usare la stessa password o una variante è rischioso...

... e cosa invece fanno

51%

... nondimeno, il 51% si affida alla propria memoria per gestire le password.

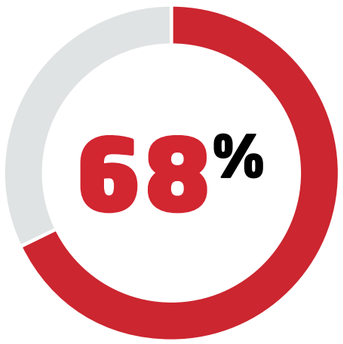
65%

... eppure, il 65% lo fa lo stesso, sempre o quasi sempre.

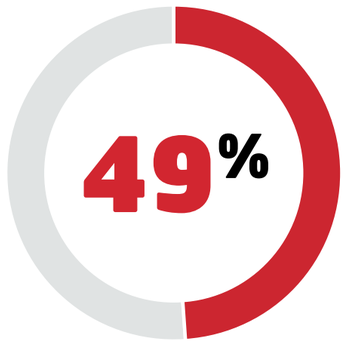
IL 45% NON HA CAMBIATO LE PASSWORD

Il 45% degli intervistati non ha cambiato le password lo scorso anno neanche dopo che si è verificata una violazione.

Le persone adottano un approccio alla sicurezza delle password di tipo selettivo e tendono a creare password più complesse per:

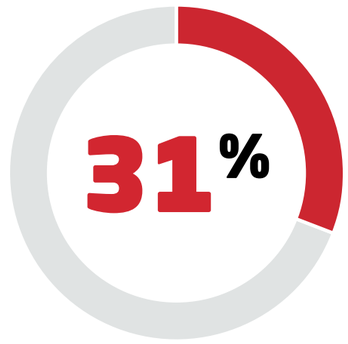


Account finanziari



Account e-mail

Account di lavoro



Account clinici

8%

Solo l'8% ha dichiarato che una password complessa non dovrebbe avere attinenza con le informazioni personali.

Ciò significa che gran parte degli utenti crea password basate su informazioni personali correlate con dati probabilmente disponibili al pubblico, come la data del compleanno o l'indirizzo di casa.

IL CONSIGLIO DEGLI ESPERTI

Anziché singole parole, sarebbe opportuno richiedere che i dipendenti utilizzino frasi prive di senso cosparse di numeri e simboli per renderne le password più lunghe, complesse e facili da ricordare per i legittimi proprietari, sebbene, al tempo stesso, più difficili da violare per gli hacker.

Luci e ombre

Predomina la dissonanza cognitiva. Le persone decidono quali informazioni meritano di essere protette. Di conseguenza, adottano consapevolmente pratiche pericolose in materia di password, anche quando trascorrono su Internet una quantità di tempo senza precedenti per motivi di lavoro o intrattenimento durante una pandemia.

L'**83%** non ha modo di sapere se le proprie informazioni siano finite nel Web oscuro.

Il **76%** sostiene che utilizza l'MFA per motivi sia personali che di lavoro, il che equivale a un aumento del 10% rispetto all'anno scorso.

IL CONSIGLIO DEGLI ESPERTI

Tutte le credenziali andrebbero trattate come se fossero vulnerabili. I dipendenti di un'impresa potrebbero pensare che, ad esempio, la password della palestra in città non desti l'interesse di un pirata informatico. Se quella password è uguale a un'altra che usano per lavoro, tuttavia, una violazione informatica ai danni della palestra rappresenterebbe una minaccia anche per le informazioni aziendali sensibili di natura finanziaria.

Le nostre vite digitali sono cresciute a dismisura

Un numero di account senza precedenti

Il **91% degli intervistati** ha creato almeno un nuovo account quest'anno.

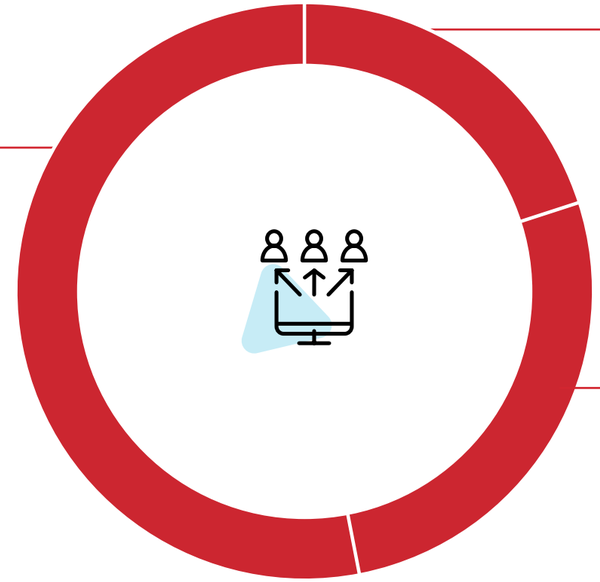
Il **90% degli intervistati** dichiara che il proprio numero di account digitali, considerando anche le applicazioni, arriva fino a 50.

50% Nel 2021, gli intervistati hanno il 50% di account in più rispetto al 2020.

Con il crescere della nostra presenza digitale, urge una protezione più sicura per i dipendenti e le imprese

Durante la pandemia di COVID-19, le nostre vite digitali sono cresciute enormemente. La distanza che ci separava ci ha spinto a trascorrere sempre più tempo in rete per stare più vicini. Di riflesso, dunque, è aumentato il numero di nuovi account creati, come anche la quantità di dati personali condivisi su Internet.

La quantità di dati personali online è in aumento:



53%
Tasso di chi ha condiviso online foto delle proprie vacanze.

20%
Tasso di chi ha condiviso foto dei propri animali domestici con i rispettivi nomi, che poi ha usato nelle password, ovvero **il 5% in più rispetto al 2020**.

27%
Tasso di chi ha condiviso foto della casa o del quartiere in cui abita, ovvero **il 7% in più rispetto al 2020**.

IL CONSIGLIO DEGLI ESPERTI

I criminali informatici estraggono i dati degli utenti dai profili pubblici e possono utilizzarne le informazioni, anche se apparentemente innocue, per violare account esterni alla loro cerchia social. Bisognerebbe raccomandare ai dipendenti di mantenere riservate le informazioni personali condivise online e sui social.

Smart working: l'impatto sui dipendenti e sui datori di lavoro

Pratiche dei dipendenti in smart working:

47% Il 47% non ha cambiato le proprie pratiche di sicurezza in rete.

46% Il 46% non ha utilizzato password più complesse.

44% Il 44% ha condiviso password e altri dati sensibili di account professionali.

Pratiche dei datori di lavoro in smart working:

39% Il 39% si è assicurato che i dipendenti in regime di lavoro agile accedessero alla rete aziendale tramite reti protette.

35% Il 35% ha richiesto che il personale aggiornasse le password più regolarmente.

35% Il 35% ha potenziato i metodi di autenticazione.

Gli amministratori informatici devono prestare attenzione perché la concreta presenza di un rischio di per sé non incoraggia le persone ad adottare una condotta più sicura. Quasi metà dei dipendenti che lavorano a distanza, infatti, adotta pratiche pericolose in materia di password.

Gli amministratori informatici devono ripensare le loro strategie di sicurezza esattamente come i dipendenti ridefiniscono e riconsiderano il modo in cui lavorano.

IL CONSIGLIO DEGLI ESPERTI

Il consiglio è di: investire in una soluzione per la **gestione delle password** che favorisca pratiche più adeguate e una maggiore sicurezza; implementare l'**SSO** e l'**MFA** per proteggere tutti i punti di accesso; organizzare corsi di formazione sulla sicurezza per informare e sensibilizzare.

Spaccato regionale

Regno Unito

Il **61%** sa che una password univoca e complessa non ha attinenza con le informazioni personali.

Gli intervistati del Regno Unito sono inoltre risultati i meno propensi a condividere le proprie informazioni personali in rete (**41%**).

Germania

Con il **79%**, la Germania ha il tasso più alto di intervistati che affermano di essere informati sul dark web,

sebbene solo il **14%** abbia modo di sapere se le proprie informazioni siano finite in questo mondo sommerso.

Francia

Solo il **15%** degli intervistati francesi ha lavorato da remoto durante l'emergenza Covid.

Di questi, soltanto il **43%** ha modificato le proprie pratiche di sicurezza in rete.

Singapore

Singapore risulta il Paese che nutre più preoccupazioni per le password compromesse (**93%**).

Il campione intervistato in questo Paese si è inoltre dimostrato il più preparato in caso di violazione (**74%**).

India

L'India è di gran lunga il Paese più propenso a utilizzare un gestore di password o un browser per memorizzare le credenziali (**64%**).

Il campione intervistato in India si è dimostrato esemplare quando si è trattato di modificare le proprie pratiche di sicurezza online in regime di lavoro agile (**81%**).

Australia

Il **71%** degli intervistati australiani utilizza sempre o quasi sempre una variante della stessa password.

Nel complesso, tuttavia, gli australiani hanno trascorso meno tempo online durante la pandemia (**61%**).

Stati Uniti

Gli intervistati statunitensi si sono rivelati più propensi a utilizzare servizi di monitoraggio del credito se i loro account venivano compromessi (**31%**).

Tuttavia, il **39%** ha ritenuto non necessario modificare le proprie pratiche di sicurezza online mentre lavorava a distanza perché le reputava già efficaci.

Conclusioni

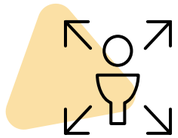
Perché le persone adottano pratiche inadeguate in materia di password (quando sanno che non dovrebbero)?

68% Tasso di chi riutilizza le password per paura di dimenticarle.

52% Tasso di chi le riutilizza perché vuole mantenerne il controllo.

36% Tasso di chi non considera i propri account abbastanza preziosi per gli hacker.

Perché il riutilizzo delle password è così pericoloso, soprattutto alla luce delle nostre vite digitali in continua crescita?



Un'unica coppia di credenziali trafugate può fornire a un criminale informatico l'accesso a molti account.

Quando un criminale informatico accede a un dispositivo utilizzato per scopi sia personali sia professionali, può accedere rapidamente a una rete aziendale per rubare dati o denaro.

LE PERSONE ADOTTANO PRATICHE INADEGUATE IN MATERIA DI PASSWORD

Con una vita digitale in continua crescita e la mancanza di un orientamento alla sicurezza informatica, è la combinazione tra le abitudini, le emozioni e l'assenza di un senso di urgenza che caratterizzano le persone a distoglierle dal modificare le proprie pratiche in rete.

Come combattere le pratiche (inadeguate) in materia di password

La pandemia di COVID-19 ha apportato un cambiamento epocale nel modo in cui lavoriamo e interagiamo. Passiamo più tempo in rete e condividiamo più contenuti digitali. Se sappiamo perché le persone adottano pratiche inadeguate, cosa possiamo fare per correggerle?

Alcune pratiche ottimali in materia di password

- Creare password univoche
- Utilizzare combinazioni di caratteri prive di senso
- Abilitare l'autenticazione a più fattori
- Modificare le password alla notifica di una violazione

Combattere la paura

Ricorrere a un **gestore di password** può aiutare a gestire e proteggere le password, creandole, memorizzandole e inserendole al posto nostro.

Combattere la preoccupazione

Aggiungere un ulteriore livello di sicurezza con l'**autenticazione a più fattori (MFA)** può aiutare a garantire che i propri dipendenti siano gli unici in grado di accedere alle informazioni e alle applicazioni aziendali.

Combattere l'inerzia

Sfruttare il **monitoraggio del dark web** può aiutare a tenere i dati sotto controllo e scoprire se vengono compromessi.

LastPass

LastPass Business offre una soluzione per la gestione delle password che può essere usata e gestita in modo semplice per ridurre le difficoltà dei dipendenti e acquisire, allo stesso tempo, un quadro più chiaro e maggiore controllo.

LastPass Business consente ai dipendenti di creare, proteggere e condividere le credenziali senza pensieri, mentre la sua infrastruttura di sicurezza basata sul principio della conoscenza zero garantisce la protezione necessaria.

Altre informazioni