LastPass •••|

La psicologia delle password

Uno stile di vita sempre più digitale e comportamenti sbagliati nella gestione delle password

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

La pandemia di COVID-19 ha rivoluzionato gli ambienti di lavoro di milioni di persone in tutto il mondo. Gli uffici fisici hanno dovuto chiudere. Molte persone sono passate al telelavoro. Non potendo andare da nessuna parte, hanno iniziato a trascorrere più tempo online.

I singoli individui e le aziende non sono mai stati così a rischio. Gli hacker approfittano delle vulnerabilità umane e le sfruttano come mai prima d'ora. I tipi di attacchi sono cambiati a causa del gran numero di persone che ricorrono al telelavoro e passano più tempo online.

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

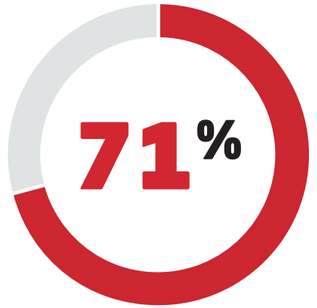
85%

La maggior parte delle violazioni dei dati, pari a uno sconcertante 85%, ha coinvolto un elemento umano (phishing, furto di credenziali ed errore umano).

36%

Lo scorso anno il 36% delle violazioni ha riguardato il phishing, con un aumento dell'11%.

Durante la pandemia:



ha lavorato da remoto sempre o in parte.

ha trascorso più tempo online per l'intrattenimento personale e per il lavoro.

Panoramica del sondaggio

Il nostro report sulla psicologia delle password esplora i comportamenti di 3.750 professionisti di sette paesi per quanto riguarda la sicurezza delle password. Abbiamo chiesto ai partecipanti cosa ne pensano della sicurezza online e quali comportamenti adottano.

Paesi destinatari del sondaggio:

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

La consapevolezza è tanta, ma non si traduce abbastanza in azione.

Cosa dicono gli utenti.

79%
riconosce che le password compromesse sono preoccupanti...

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

Cosa fanno.

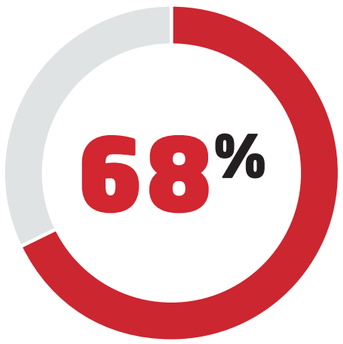
51%
...si affida alla propria memoria per tenere traccia delle password.

65%
...eppure utilizza sempre o quasi la stessa password o variante.

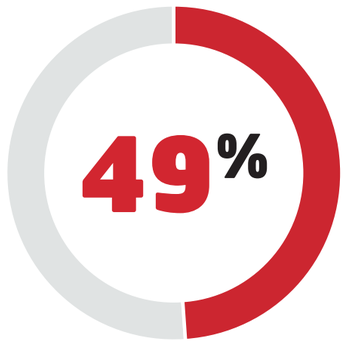
IL 45% NON HA CAMBIATO LE PASSWORD

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

Le persone adottano la sicurezza delle password selettive, ma vorrebbero creare password più complesse per:



Account finanziari



Account email

Account correlati al lavoro

Account clinici

Solo l’8% ha dichiarato che una password complessa non deve avere attinenza con informazioni personali.

8%

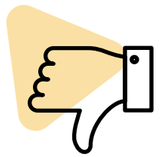
Questo significa che la maggior parte degli utenti crea password basate su informazioni personali che, a loro volta, hanno connessioni con possibili dati pubblici, come la data del compleanno o l’indirizzo di casa.

IL CONSIGLIO DEGLI ESPERTI

Utilizza espressioni senza senso inframezzate da numeri e simboli piuttosto che singole parole per ottenere password più lunghe, più complesse e più facili da ricordare, rendendole anche più difficili da scoprire per gli hacker.

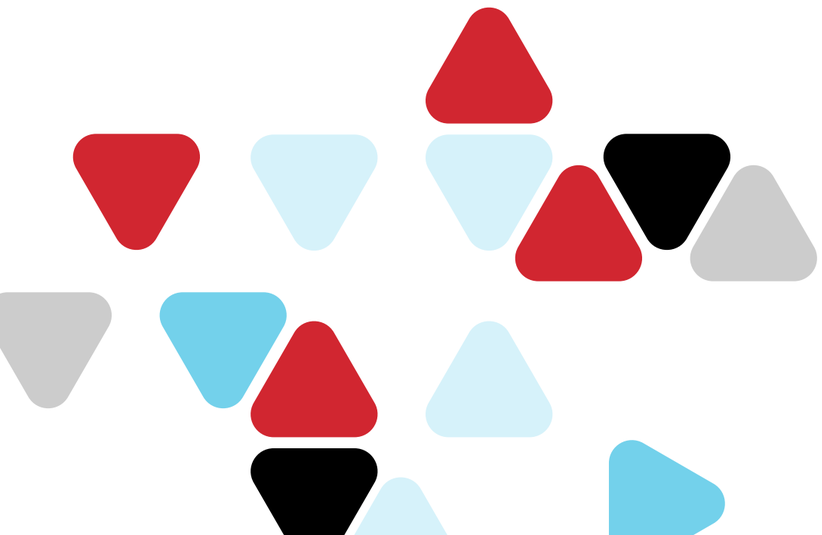
Luci e ombre

A predominare è la dissonanza cognitiva. Gli utenti scelgono quali informazioni ritengono degne di essere protette. Di conseguenza, adottano consapevolmente comportamenti rischiosi con le password, anche quando restano online per periodi di tempo senza precedenti per il lavoro e l'intrattenimento durante una pandemia.



83% non sapeva se le proprie informazioni erano sul dark web.

76% dichiara di utilizzare l'MFA per motivi personali e di lavoro, una percentuale in aumento del 10% rispetto all'anno scorso.



IL CONSIGLIO DEGLI ESPERTI

Tratta tutte le credenziali come se fossero vulnerabili. Potresti pensare che le tue credenziali della palestra locale non abbiano valore per gli hacker, ma se quelle credenziali sono identiche o simili a quelle di accesso al tuo conto bancario, una violazione nella tua palestra potrebbe comportare anche l'esposizione di informazioni finanziarie sensibili.

Uno stile di vita sempre più digitale

Mai come ora così tanti account.

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

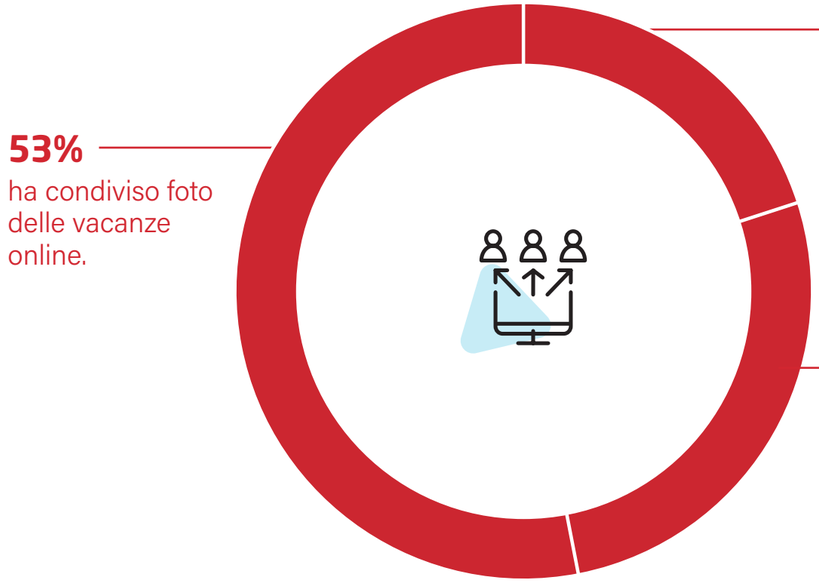
Il 90% degli intervistati dichiara di avere fino a 50 account online/di app.

50% I partecipanti hanno il 50% di account in più nel 2021 rispetto al 2020.

Via via che aumenta la nostra presenza nel mondo digitale, abbiamo bisogno di una protezione più efficace per le nostre informazioni personali.

La nostra vita è diventata molto più digitale durante la pandemia di COVID-19. L'isolamento nelle nostre giornate ci ha spinti a collegarci online più che mai. Il risultato: creazione di più account e condivisione online di più informazioni personali.

La quantità di dati personali online è in aumento:



53%
ha condiviso foto delle vacanze online.

20%
ha condiviso foto dei propri animali domestici con i rispettivi nomi e poi ha usato tali nomi nelle password, **il 5% in più rispetto al 2020.**

27%
ha condiviso foto della propria casa o del quartiere, **il 7% in più rispetto al 2020.**

IL CONSIGLIO DEGLI ESPERTI

Mantieni riservati i tuoi aggiornamenti sui social media o sii prudente con i tuoi post pubblici. I malintenzionati estraggono dati dai profili pubblici e possono utilizzare informazioni apparentemente innocue per violare account al di fuori dei tuoi social media.

Telelavoro: le prospettive dei dipendenti e dei datori di lavoro

Abitudini di telelavoro dei dipendenti:

47% non ha cambiato le abitudini sulla sicurezza online da quando lavora in remoto.

46% non ha utilizzato password più complesse con il telelavoro.

44% ha condiviso informazioni sensibili e password di account professionali durante il telelavoro.

Abitudini di telelavoro dei datori di lavoro:

39% si è assicurato che i dipendenti accedessero alla rete aziendale tramite reti sicure durante il telelavoro.

35% ha invitato i dipendenti ad aggiornare le password più regolarmente.

35% ha migliorato i metodi di autenticazione.

Gli amministratori informatici devono prestare attenzione. La presenza di un rischio di per sé non incoraggia le persone a seguire procedure più sicure. Quasi metà dei dipendenti adotta un comportamento rischioso riguardo alle password durante il telelavoro.

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

IL CONSIGLIO DEGLI ESPERTI

Investi in una soluzione di **gestione delle password** per migliorare le pratiche e la sicurezza in materia di password. Implementa l'**SSO** e l'**MFA** per proteggere tutti i punti di accesso. Organizza corsi di formazione sulla sicurezza per informare e istruire.

Spaccato regionale:

Regno Unito

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

Questa stessa percentuale di utenti è anche risultata meno propensa a condividere informazioni personali online **(41%).**

Germania

La Germania è al primo posto per la conoscenza del dark web **(79%).**

Solo il **14%** sapeva se le proprie informazioni personali erano sul dark web.

Francia

Solo il **15%** dei partecipanti francesi ha lavorato da remoto durante l'emergenza COVID.

Soltanto il **43%** ha cambiato abitudini sulla sicurezza online durante il telelavoro.

Singapore

Singapore risulta il paese più preoccupato per le password compromesse **(93%).**

I suoi utenti sono anche al primo posto in quanto a sapere cosa fare se subiscono un attacco **(74%).**

India

L'India è notevolmente più propensa di altri paesi a utilizzare un gestore di password o un browser per memorizzare le password **(64%).**

I partecipanti indiani sono al primo posto per la disponibilità a cambiare le abitudini in materia di sicurezza online durante il telelavoro **(81%).**

Australia

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

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

Stati Uniti

Gli americani erano più propensi a utilizzare servizi di monitoraggio del credito se il loro account veniva compromesso **(31%).**

Tuttavia, il **39%** pensava di non dover cambiare abitudini sulla sicurezza online durante il telelavoro perché le password erano già efficaci.

Conclusioni

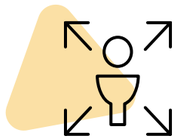
Perché le persone adottano comportamenti sbagliati riguardo alle password quando sanno chiaramente quali sono le pratiche migliori?

68% riutilizza le password perché ha paura di dimenticarsele.

52% le riutilizza perché vuole avere il controllo di tutte le sue password.

36% non considera i propri account sufficientemente preziosi per gli hacker.

Perché il riutilizzo delle password è così pericoloso, considerando soprattutto che la nostra vita è sempre più digitale?



Il furto di un unico nome utente combinato con una password rubata fornisce a un hacker l'accesso a molti account.

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

GLI UTENTI ADOTTANO UN COMPORTAMENTO SBAGLIATO

Con uno stile di vita sempre più digitale e la carenza di un supporto per la cibersicurezza, le persone tendono a cambiare i propri comportamenti online a causa di una combinazione di fattori, ovvero abitudini, emozioni e mancanza di un senso di urgenza.

La lotta ai comportamenti sbagliati nella gestione delle password

La pandemia di COVID-19 ha generato un cambiamento senza precedenti nel modo in cui lavoriamo e interagiamo. Passiamo più tempo online. Condividiamo più contenuti digitali. Se sappiamo perché le persone si comportano così, come possiamo fare per correggere questo comportamento?

Qual è un comportamento corretto nella gestione delle password?

- Crea password univoche.
- Utilizza combinazioni di caratteri senza senso.
- Attiva l'autenticazione a due fattori.
- Aggiorna le password quando ricevi la notifica di una violazione.

Vinci le tue paure.

Utilizza un **gestore di password** per gestire e proteggere le password. Affida a un gestore di password il compito di creare, memorizzare e inserire le tue password.

Vinci le tue ansie.

Aggiungi un livello di sicurezza con l'**autenticazione a più fattori (MFA)** per avere la certezza di essere l'unico ad accedere alle tue informazioni.

Vinci la tua apatia.

Monitora i dati e assicurati di sapere quando le tue informazioni sono state compromesse con il **monitoraggio del dark web.**

LastPass •••|

LastPass è la soluzione cui si affidano oltre 30 milioni di utenti e 85.000 aziende per salvare e inserire le password, i dati delle carte di credito e altre informazioni sensibili. Usando LastPass, è possibile generare password complesse e inserirle automaticamente per accedere ai siti e alle applicazioni da qualsiasi dispositivo.

Altre informazioni