Bitdefender
Global Leader
In Cybersecurity

Dalle violazioni dei dati alla violazione degli account: come gli hacker sfruttano le fughe di dati per dirottare gli account

Con l'inizio della scuola e l'avvicinarsi del mese di ottobre, il mese tradizionalmente dedicato alla sensibilizzazione della sicurezza informatica, è opportuno riflettere sul fatto che le password sicure sono ancora il punto cardine delle buone pratiche di sicurezza. Tuttavia, si stima che oltre 12 miliardi di account (più della popolazione umana) siano stati violati e commercializzati sul dark web.

Adulti e ragazzi utilizzano le password per qualsiasi cosa, dalla sicurezza di computer e telefoni, alla protezione delle finanze personali, alla pubblicazione di post sui social media e all'intrattenimento in streaming. Comprendere come i criminali informatici ottengono e decifrano le password (anche quelle apparentemente più solide) è fondamentale per ciascuno di noi per proteggersi meglio.

Le password svolgono un ruolo fondamentale per la sicurezza da molto prima dell'invenzione dei computer. Il concetto di password risale all'antichità, quando si usavano parole o frasi segrete per accedere a luoghi esclusivi o a conoscenze confidenziali.

Nei primi computer, le password venivano utilizzate per controllare l'accesso ai sistemi mainframe e ai terminali; si trattava generalmente di password spesso semplici e facili da ricordare perché i sistemi informatici non erano così diffusi e connessi come oggi e i rischi non erano così frequenti.

Con l'arrivo di Internet, le password sono diventate fondamentali per proteggere le informazioni personali. Spesso costituiscono l'unica barriera tra la sfera privata e quella pubblica della nostra complessa esistenza digitale. Attirati dalla ricchezza di informazioni che si trovano dall'altra parte della barriera, i criminali informatici fanno di tutto per acquisire le credenziali d'accesso dei servizi online.

Nel corso degli anni, abbiamo ripetutamente cambiato il modo in cui utilizziamo e memorizziamo le password . La memorizzazione delle password in testo normale è stata la prima, nonché meno sicura, implementazione: infatti, chiunque con accesso a un database potrebbe vedere le password di ogni account. Indipendentemente dal livello di sicurezza della password, un utente malintenzionato con accesso al database potrebbe sfruttare immediatamente le credenziali.

Revisione delle best practice di sicurezza

Le violazioni dei dati sono in costante aumento. Al momento in cui scriviamo, si sa che più di **12 miliardi di account** sono stati violati e scambiati su forum specializzati. Ed è ancora peggio se si considera che le vittime spesso riutilizzano la stessa combinazione di nome utente e password per più account. In questo caso, un criminale informatico esperto effettuerebbe

un attacco di credential stuffing, cercando di accedere ad altri importanti servizi a cui la vittima potrebbe essersi iscritta.

Per affrontare questi problemi di sicurezza, le aziende e gli esperti hanno iniziato a promuovere pratiche più rigorose per la scelta delle password. Per esempio, si consiglia di utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali per creare password complesse e uniche. Si raccomanda inoltre di evitare parole comuni o informazioni facilmente indovinabili, come compleanni o nomi di animali domestici.

Nonostante questi progressi, permane il problema del frequente riutilizzo delle stesse password per più account o del basso livello di sicurezza delle password scelte, che mette a rischio la sicurezza online degli utenti. Pertanto, è importante seguire una serie di buone pratiche in materia di password, come l'utilizzo di password uniche e solide, la loro rotazione regolare e l'attivazione di misure di sicurezza aggiuntive come l'autenticazione a due o più fattori, se disponibili. Questi metodi richiedono agli utenti di fornire una forma di verifica ulteriore, come un codice temporaneo inviato ai loro dispositivi mobili, oltre alla password. Questo aggiunge un ulteriore livello di protezione contro gli accessi non autorizzati.

Attenendosi a queste linee guida, gli utenti dovrebbero creare e memorizzare decine di password forti e uniche per ogni account che possiedono. Dovrebbero inoltre ruotare le password compromesse in caso di violazione dei dati.

Informazioni su Bitdefender

Bitdefender è una società leader nella sicurezza informatica che offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce del mondo. Proteggendo milioni di consumatori, aziende e ambienti governativi, Bitdefender è considerata uno degli esperti più affidabili del settore per eliminare le minacce, proteggere la privacy e i dati, e ottenere la resilienza informatica. Grazie a notevoli investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida miliardi di query sulle minacce al giorno. L'azienda ha aperto la strada a innovazioni rivoluzionarie in varie tecnologie, come anti-malware, sicurezza IoT, analisi comportamentale e intelligenza artificiale. La sua tecnologia è usata su licenza da più di 180 dei marchi tecnologici più noti al mondo. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo. Per maggiori informazioni, visitare https://www.bitdefender.it.

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it