OUCH! | Settembre 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

I Password Manager

Introduzione

Una delle iniziative più importanti che potete intraprendere per proteggervi è di usare una password forte e diversa per ogni account. Sfortunatamente, è impossibile per ognuno di noi ricordare tutte le varie password di tutti i nostri account. Ecco perché molte persone riutilizzano sempre la stessa password, pratica molto pericolosa poiché se una password venisse compromessa, anche gli altri vostri account che la usano sarebbero in pericolo. Una semplice soluzione consiste nell'utilizzare un Password Manager, chiamato anche Password Vault. Si tratta di un'applicazione che conserva tutte le vostre password in modo sicuro, permettendovi così di avere una password diversa per ogni account. I Password Manager semplificano la vita perché anziché dover ricordare tutte le password, dovrete ricordare solo quella che vi consente di accedere al programma.

L'autore di questo numero

Chris Christianson è un consulente in Information Security basato in California, con oltre 20 anni di esperienza e numerose certificazioni tecniche. È intervenuto come speaker in molte conferenze e ha pubblicato diversi articoli. Potete raggiungerlo su Twitter (**@cchristianson**) e su **https://ismellpackets.**

Come funzionano i Password Manager

Questi programmi consentono di memorizzare tute le vostre password in un database, chiamato anche vault. Il Password Manager cifra il contenuto del database e lo protegge con una master password che solo voi conoscete. Quando avete bisogno di recuperare le vostre password, come ad esempio la login al sistema di e-banking o all'email, non dovete far altro che digitare la master password nel programma. In molti casi, il Password Manager consente di recuperare automaticamente la password ed effettuare la login. Tutto questo rende più semplice la gestione di centinaia di password forti e diverse, poiché non dovete più ricordarle!

Alcuni Password Manager memorizzano il database sul computer o sui dispositivi mobili, mentre altri lo conservano nel Cloud. Inoltre, molti Password Manager prevedono la possibilità di sincronizzare automaticamente il contenuto del database su vari dispositivi in modo che se modificate una password sul vostro laptop, il cambiamento venga propagato su tutti gli altri device in vostro possesso. indipendentemente da dove il database è memorizzato, dovete installare l'applicazione Password Manager sui sistemi o sui dispositivi per utilizzarla.

I Password Manager

Quando configurate un Password Manager per la prima volta, dovete inserire manualmente o importare le vostre login e password. Successivamente, il programma individuerà quando vi state registrando per un account online o quando modificate la password per un account esistente, aggiornando conseguentemente il database cifrato. Ciò è possibile perché molti Password Manager lavorano di concerto con il browser e questa integrazione consente loro di gestire l'inserimento delle vostre credenziali nei siti web.

È fondamentale che la master password che usate per proteggere il Password Manager sia forte e difficile da indovinare. Vi raccomandiamo di utilizzare una passphrase, uno dei tipi di password più forti. Se il Password Manager supporta la verifica in due passaggi, usatela. Ricordate che se dimenticate la master password non potrete più accedere a nessuna delle vostre password.

I Password manager sono un modo semplice per conservare e usare in sicurezza tutte le vostre password.

Scegliere un Password Manager

Ci sono molti Password Manager tra cui scegliere: nella ricercar di quello che fa per voi, considerate sempre I seguenti punti:

- il Password Manager deve essere facile da usare. Se il programma è troppo complesso, trovatene un'altro che si adatti meglio al vostro stile e alla vostra padronanza della tecnologia;
- il programma dovrebbe funzionare su tutti i dispositivi con i quali vi serve utilizzare delle password. Dovrebbe anche essere semplice sincronizzare le password tra i vari dispositivi;
- usate solo password manager conosciuti e affidabili. Fate attenzione ai prodotti che non hanno storia e nessun feedback dalla community. I criminali informatici potrebbero creare programmi falsi per impossessarsi delle vostre informazioni. Siate anche cauti nei confronti dei prodotti caratterizzati da una soluzione di cifratura proprietaria;
- evitate quei Password Manager che dichiarano di essere in grado di recuperare la vostra master password, poiché significa che la conoscono, elemento che vi espone a troppi rischi;

I Password Manager

- assicuratevi che qualsiasi soluzione scegliate, il produttore continui ad aggiornarla costantemente e voi abbiate installato l'ultima versione disponibile;
- il PM dovrà essere in grado di generare password forti mostrandovi gli elementi di forza della password generata;
- il PM dovrebbe darvi la possibilità di memorizzare anche altri dati sensibili, come le risposte alle domande di sicurezza, il numero di carta di credito e altro ancora.

I Password Manager sono un ottimo modo per memorizzare le vostre password e i dati sensibili. Poiché il loro compito è di conservare informazioni molto importanti, proteggeteli con una password forte e unica che sia difficile da trovare per un hacker, ma facile da ricordare per voi.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

I migliori gestori password a confronto: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_it.pdf

Le Passphrase: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf

La verifica in due passaggi: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201611_it.pdf

Il decalogo per proteggere gli account online:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_it.pdf

Direzione editoriale: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley