Come proteggere i nostri dati

Autore: Daniela Baudino
Fonte: Città Nuova

Nel giorno della sicurezza in Rete, qualche consiglio per evitare di essere un bersaglio troppo facile per i malintenzionati. E i libri per approfondire l'argomento

Si chiamano Collection #1 e Collection #2-5: rappresentano il **più grande archivio di e-mail e password rubate nella storia**. Due enormi *database* (e forse rappresentano solo la punta di un *iceberg* decisamente più profondo) di oltre 932 GigaByte totali (l'equivalente di circa 900 film), con al loro interno più **di 2,2 miliardi di indirizzi e-mail e password**. Questa collezione di dati che girano indisturbati sulla Rete (Collection #2-5 è stata scaricata ben 1100 volte) è il risultato dell'unione di elenchi minori, di dati rubati da furti precedenti, come le violazioni che hanno coinvolto Yahoo, Linkedin e Dropbox. Non bisogna però farsi prendere dal panico: nella maggior parte dei casi, infatti, le credenziali rubate sono datate e potrebbero essere state aggiornate dagli utenti. Oltretutto, queste collezioni sembrano essere una raccolta **casuale di dati**, fatta esclusivamente per massimizzare il numero di credenziali accessibili agli *hacker*. È come se fossero stati rinvenuti in un magazzino una grande quantità di indirizzi civici e dall'altra una grossa quantità di mazzi di chiavi di casa. Quindi può essere che i nostri *account* non abbiano subito una vera violazione, visto che i dati "ritrovati" provengono da diverse "retate di dati", ma se con alcuni sistemi gli *hacker* tentassero di combinare tra loro i dati potrebbero certamente essere in grado di entrare nei nostri *account*. Queste notizie possono dunque anche servire a ricordarci l'**importanza delle azioni che facciamo (o non facciamo) per garantire la nostra sicurezza online**. **Come controllare se il nostro indirizzo email o la nostra password sono stati "raccolti"** Per capire se il nostro indirizzo email è presente nelle raccolte basta collegarsi al sito Have I Been Pwned: inseriamo il nostro indirizzo email nella barra al centro e poi clicchiamo sul pulsante "pwned". Il risultato può essere di due tipi: in **verde**, se la nostra e-mail non è stata violata; in **rosso** invece nel caso in qualche modo il nostro indirizzo email sia finito in qualcuna delle liste presenti in Collection #1. Nei risultati è possibile anche trovare il numero dei siti illegali dove sarebbero presenti le informazioni relative al nostro indirizzo di posta elettronica. Per Collection #2-5 ci si deve invece collegare a questo altro sito, inserire il proprio indirizzo email: il responso arriverà attraverso una email allo stesso indirizzo inserito. In modo analogo, è possibile **scoprire se la nostra password sia presente in Collection #1** collegandosi al sito Pwned Password. Anche in questo caso è sufficiente inserire nella barra di ricerca la password di cui vogliamo verificare l'integrità e attendere il risultato verde o rosso, con i vari dati corrispondenti. **Cosa fare se i nostri dati sono stati segnalati come "bucati"** Innanzitutto niente panico, perché **è possibile rimettere in sicurezza tutti gli indirizzi email e proteggere tutte le nostre informazioni cambiando la nostra password**. Per ognuno degli indirizzi coinvolti sarà quindi necessario:

- accedere alla nostra casella email attraverso un browser Internet ed entrando nelle opzioni cambiare la password, creandone una abbastanza robusta, unica per ogni indirizzo email
- se il sistema lo permette, abilitiamo **l'autenticazione a due fattori**, un sistema che ci permette di autenticarci generando una sequenza di numeri casuali inviati al nostro smartphone, che poi devono essere reinseriti durante l'accesso al sito
- una volta modificata la password online è possibile che ci venga chiesto di rieseguire l'accesso in tutti i dispositivi in cui avevamo collegato il nostro indirizzo email utilizzando la nuova password

Come creare una password sicura e buone pratiche di sicurezza

- scegliere una frase o un insieme di parole con cui creare associazioni analogiche, magari inserendo qualche errore grammaticale. **Lunghezza minima**, almeno 9-12 caratteri
- trasformare la stringa sostituendo alcune lettere con numeri e caratteri speciali: per esempio “Conddividere X Unnire” può trasformarsi in C0ndd1v1d3r3xUnn1r3!
- imbottire una frase con simboli ripetuti sia all’inizio che alla fine o in mezzo alle parole. Il nostro esempio potrebbe diventare “@@@C0nddividere?Unn1re!!!”
- **Utilizzare password diverse per servizi diversi**, o comunque non utilizzare per servizi importanti password che utilizziamo per registrazioni a servizi minori, perché altrimenti “bucata” una password, “bucate” tutte le password. Se diventa difficile creare tante password sicure diverse si può pensare di utilizzare un **password manager**, un software che permette di **gestire tutte le password attraverso un’unica password centrale** (possibilmente sicura), che una volta inserita permette di accedere a tutte le altre senza doverle sempre ricordare
- Attenzione alle domande che servono per recuperare la password: siccome lasciamo molti nostri dati online sui social, **non diamo risposte corrette**!
- evitare di fare login attraverso i sistemi di Social Login di Facebook, Twitter ect
- **evitare di fare operazioni “delicate” attraverso connessioni Wifi pubbliche**, come acquisti online o l’accesso a sistemi di home banking
- **scollegarsi sempre dai propri account**, a maggior ragione se usiamo pc di altri, ma anche quando siamo sul nostro computer
- **cambiare spesso** la propria password

Per approfondire l'argomento, si possono acquistare questi due libri pubblicati da *Città Nuova*:

- Nasci, cresci e posta
- Cyberbullismo