Sicurezza online e password complesse

Come proteggere i vostri account online dagli accessi non autorizzati

La vostra Polizia e la Prevenzione Svizzera della Criminalità (PSC) – un servizio intercantonale della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP), in collaborazione con la Scuola Universitaria Professionale di Lucerna e “eBanking – ma sicuro!”

Così come chiudete a chiave la porta di casa quando uscite, dovreste fare tutto il possibile per impedire a malintenzionati di accedere ai vostri dispositivi e account online.

Punti da tener presente

- Proteggete il vostro computer e i vostri dispositivi mobili (smartphone, tablet, ecc.) dagli accessi non autorizzati e **bloccate lo schermo** quando non li state usando attivamente.
- Utilizzate **password complesse** (lunghe almeno 12 caratteri, composte da numeri, lettere maiuscole e minuscole e caratteri speciali).
- Non utilizzate sempre la stessa password dappertutto. Create invece una **password diversa** per ogni account online.
- Se possibile, attivate la cosiddetta **autenticazione a due fattori.**

Il mio account online è stato violato?

Per sapere se la password di uno dei vostri account online è stata violata, entrate nel sito **www.ebas.ch/haveibeenpwned**. Qui potrete scoprire se le vostre credenziali d'accesso a un account online sono state utilizzate da terzi o pubblicate in occasione di una fuga di dati. Questo sito è infatti collegato al database della nota piattaforma **haveibeenpwned.com** e vi presenta i risultati in italiano. Attenzione: inserite unicamente il vostro nome utente o indirizzo e-mail. La password che volete far controllare non deve mai essere immessa!

www.ebas.ch/it/have-i-been-pwned

haveibeenpwned.com

Come proteggere i vostri dispositivi mobili dagli accessi non autorizzati

Proteggete tutti i vostri dispositivi mobili securizzandone gli accessi. Tenete presente che il rischio di perdita o furto di un dispositivo mobile è molto maggiore per i notebook, i tablet e gli smartphone che per il PC di casa.

Assicuratevi quindi, in particolare per i vostri dispositivi mobili, di attivare il blocco automatico dello schermo tramite codice, password, impronta digitale o riconoscimento facciale.

È inoltre consigliabile crittografare i dati presenti sul vostro dispositivo mobile, in particolare, anche sugli archivi aggiuntivi come i dischi rigidi esterni o le chiavette USB. In questo modo impedirete qualsiasi tentativo di accesso ai vostri dati e alle vostre app da sistemi di terzi.

iPhone/iPad

- Blocco degli accessi fino ad iPhone 9: in **Impostazioni / Touch ID e codice** potete proteggere il vostro dispositivo con un codice numerico o una password, e salvare anche le vostre impronte digitali.
- Blocco degli accessi da iPhone 10 in poi: in **Impostazioni / Face ID e codice** potete configurare il riconoscimento facciale.
- Sull'iPhone o sull'iPad i dati vengono crittografati automaticamente.

Android

- A seconda del dispositivo potete configurare il blocco degli accessi selezionando **Impostazioni / Sicurezza e privacy.**
- Potete attivare la crittografia in **Impostazioni / Sicurezza e privacy / Più sicurezza e privacy / Crittografia e credenziali.** Lo stesso vale per gli archivi aggiuntivi.

Come creare password complesse

Le password sono da sempre le chiavi più comuni e utilizzate nel mondo elettronico per progettere l'accesso ai dati sensibili e privati, a condizione di rispettare alcune semplici regole.

Sei regole per creare una password complessa

1. Almeno 12 caratteri
2. Numeri, lettere maiuscole e minuscole e caratteri speciali
3. Nessuna sequenza di tasti come «asdfgh» o «45678»
4. Nessuna parola contenuta in un dizionario, indipendentemente dalla lingua
5. Una password diversa per ogni account
6. Non salvate mai la vostra password se non l'avete prima crittografata

Creare una password complessa è molto semplice. Ecco come fare:

- Pensate a una frase facile da ricordare e formate la vostra password utilizzando la prima lettera di ogni parola e includendo la punteggiatura e i numeri: «**M**ia **f**iglia **T.** **M**eier **c**ompie **g**li **a**nni **i**l **19** **g**ennaio**!**»
- Otterrete così una password costituita da una sequenza di caratteri apparentemente arbitraria ma facile a ricordare: «**MfT.Mcgai19g!**»

Il password manager

Un password manager vi consente di archiviare in modo cifrato tutte le vostre password. Dovrete quindi ricordarvi di un'unica password. Ulteriori informazioni utili si trovano nel sito

www.ebas.ch/step4

Video sul password manager:

www.youtube.com/watch?v=f_nASWNWDo4

L’autenticazione a due fattori

Abbinata a una password complessa, la cosiddetta autenticazione a due fattori permette di aumentare la sicurezza dei vostri account online. In questo caso, quando effettuate il login, vi viene chiesto di utilizzare, oltre al primo elemento di sicurezza (solitamente una password), anche un secondo elemento di sicurezza indipendente. Può trattarsi per esempio di un codice numerico inviato sul vostro telefonino o generato direttamente dal vostro dispositivo.

Oltre agli istituti finanziari, oggi ci sono già diversi altri fornitori di servizi online (tra cui Google e Facebook) che offrono anche l’autenticazione a due fattori. Attivate questa funzione per aumentare la vostra sicurezza. Troverete una descrizione delle diverse procedure applicate dagli istituti finanziari nel sito seguente:

www.ebas.ch/it/attenzione-al-login

Video sull’autenticazione a due fattori:

www.youtube.com/watch?v=4O6kkjweCDg

Le passkey

Le passkey sono una soluzione di sicurezza alternativa alle password basata sulla crittografia avanzata e la biometria. Questa nuova tecnologia vi offre un modo semplice e sicuro per accedere ai vostri account online. Una passkey è una chiave digitale composta da due elementi: una chiave pubblica e una privata. La chiave privata è memorizzata sul vostro dispositivo. Ogni utilizzo è convalidato da un PIN o dai vostri dati biometrici come l’impronta digitale o il riconoscimento facciale. Anche se il vostro dispositivo viene rubato, nessuno potrà accedere alle vostre passkey se non dispone dei vostri dati biometrici o del vostro PIN. Scoprite come funzionano e come si creano le passkey nel sito seguente:

www.ebas.ch/passkeys

Gennaio 2025

SKPPSC

Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
3001 Berna

www.skppsc.ch

Questo pieghevole è stato realizzato in collaborazione con la **Scuola Universitaria Professionale di Lucerna** e **"eBanking – ma sicuro!"**.

www.ebas.ch | www.ebankingmasicuro.ch

HSLU Hochschule Luzern

eBanking ma sicuro!