4 – Proteggere gli accessi online

Chiudete le porte a chiave quando uscite di casa? Proteggete anche i vostri dispositivi e gli accessi online da utilizzi non autorizzati.

Punti principali:

- Proteggete il vostro computer e i dispositivi mobili (smartphone, tablet, ecc.) da eventuali accessi non autorizzati e bloccate lo schermo quando non li state usando attivamente.
- Utilizzate password sicure (lunghe almeno 12 caratteri, composte da cifre, lettere maiuscole e minuscole e caratteri speciali).
- Non utilizzate sempre le stesse password dappertutto, ma per i diversi servizi online utilizzate password diverse.
- Se possibile, attivate la cosiddetta autenticazione a doppio fattore.

4 – Proteggere gli accessi online

5 operazioni per la vostra sicurezza digitale

Con la chiave, stop ai furti di auto!
Con la **password**, stop ai furti di dati!

eBanking ma sicuro! www.ebas.ch

Proteggere i dispositivi dagli accessi non autorizzati

Proteggete tutti i vostri dispositivi con una protezione degli accessi. Soprattutto con notebook, tablet e smartphone, il rischio di subire la perdita o il furto di un dispositivo mobile è molto maggiore rispetto al PC di casa.

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

Inoltre, è consigliabile crittografare i dati presenti sul vostro dispositivo mobile. Il consiglio vale, in particolare, anche per gli archivi aggiuntivi come i dischi rigidi esterni o le chiavette USB. In questo modo impedite alle persone non autorizzate di accedere ai vostri dati e alle vostre app da sistemi terzi.

iPhone/iPad

Blocco degli accessi fino ad iPhone 9: In **Impostazioni / Touch ID e codice** potete proteggere il dispositivo con un codice numerico o una password, e salvare anche le vostre impronte digitali.

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

Blocco degli accessi da iPhone 10 in poi: In **Impostazioni / Face ID e codice** si può configurare il riconoscimento del volto.

Sull'iPhone o iPad i dati vengono crittografati automaticamente.

Android

A seconda del dispositivo potete configurare il blocco degli accessi all'interno di **Impostazioni / Sicurezza e privacy**.

Potete attivare la crittografia in **Impostazioni / Sicurezza e privacy / Più sicurezza e privacy / Crittografia e credenziali** – se del caso, anche per gli archivi aggiuntivi.

Password sicura

Le password sono da sempre le chiavi più comuni e utilizzate nel mondo elettronico per proteggere l'accesso a dati sensibili e privati. Bastano poche semplici regole per la gestione delle password per aumentare la propria sicurezza.

6 regole per una password sicura – utilizzare...

- almeno 12 caratteri
- cifre, lettere maiuscole e minuscole e caratteri speciali
- nessuna sequenza di tasti come «asdfgh» o «45678»
- nessuna parola di una lingua conosciuta: la password cioè non dovrebbe significare nulla e non apparire in alcun dizionario
- password diverse dappertutto
- non salvate la vostra password senza averla crittografata

Creare una password sicura non è per niente difficile! Qui di seguito viene descritto come potete creare e ricordare una password sicura con la massima semplicità:

- Pensare a una frase facilmente ricordabile e formare la password utilizzando le varie iniziali e cifre:
  «**M**ia **f**iglia **T**amara **M**eier **c**ompie **g**li **a**nni **i**l **19** **g**ennaio**!**»

- Si ottiene così una password da una sequenza di caratteri a piacere che non si avrà difficoltà a ricordare:
  «**MfTMcgai19g!**»

Password manager

Un password manager vi consente di archiviare in modo cifrato tutte le vostre password – e quindi avete bisogno di ricordare un'unica password.

Windows

Per l'uso in Windows consigliamo i password manager seguenti, alcuni dei quali disponibili gratuitamente:

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.com)
- Proton Pass (https://proton.me/pass)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

macOS

Per l'uso in Mac consigliamo i password manager seguenti, alcuni dei quali disponibili gratuitamente:

- KeePassXC (https://keepassxc.org)
- Proton Pass (https://proton.me/pass)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

Smartphone und Tablet

Per l'uso sullo smartphone o sul tablet consigliamo i password manager seguenti, alcuni dei quali disponibili gratuitamente:

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.com)
- Proton Pass (https://proton.me/pass)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_Passwortmanager_it.mp4

Ulteriori informazioni e un confronto dettagliato dei password manager comuni sono disponibili nel «Fact Sheet Password Manager» (https://docs.datenschutz.ch/u/d/publikationen/factsheets-engl/factsheet_password_managers.pdf) dell'incaricato per la protezione dei dati del Cantone di Zurigo.

Autenticazione a doppio fattore

Abbinata a una password sicura, la cosiddetta autenticazione a doppio fattore offre una sicurezza ancora maggiore. Infatti, quando viene effettuato il login viene chiesto di utilizzare, oltre al primo elemento di sicurezza (solitamente una password), anche un secondo elemento di sicurezza indipendente dal primo. Può trattarsi, per esempio, di un codice che viene inviato a un telefonino o che viene generato su uno smartphone.

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_2FA_it.mp4

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 doppio fattore. È una funzione che si può utilizzare per avere un grado maggiore di si-

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

curezza. Qui (https://www.ebas.ch/category/23) potete trovare una descrizione delle diverse procedure applicate dagli istituti finanziari.

Passkeys

Le passkey sono una soluzione di sicurezza alternativa alle password basata sulla crittografia avanzata e la biometria. Questa nuova tecnologia offre un modo semplice e sicuro per accedere agli account online. Una passkey è una chiave digitale composta da due elementi: una chiave pubblica e una segreta. La chiave segreta è memorizzata sul vostro dispositivo e protetta da PIN o dati biometrici come l'impronta digitale o il riconoscimento facciale. Anche se il vostro dispositivo viene rubato, nessuno può accedere alle vostre passkey senza disporre dei vostri dati biometrici o del PIN. Scoprite come funzionano e come si creano le passkey nel nostro articolo sulle passkey (https://www.ebas.ch/it/passkey/) .

Il mio accesso online è stato violato?

Controllate se la password di uno dei vostri account online è stata crackata:

Have I Been Pwned (https://www.ebas.ch/it/have-i-been-pwned/)

Qui potete scoprire se le vostre credenziali d'accesso a un account online sono state compromesse o pubblicate in occasione di una fuga di dati. Il sito esegue una ricerca nel database della nota piattaforma https://haveibeenpwned.com (https://haveibeenpwned.com) e vi presenta i risultati in italiano. Inserite il vostro nome utente o indirizzo e-mail, mai la password che volete far controllare!

Proteggete i vostri dati e tutti i vostri dispositivi con le «5 operazioni per la vostra sicurezza digitale»:

Fase 1 – Salvare (https://www.ebas.ch/it/1-salvare-i-dati/)

Fase 2 – Monitorare (https://www.ebas.ch/it/2-monitorare-con-antivirus-e-firewall/)

Fase 3 – Prevenire (https://www.ebas.ch/it/3-prevenire-con-aggiornamenti-software/)

Fase 4 – Proteggere

Fase 5 – Fare attenzione (https://www.ebas.ch/it/5-fare-attenzione-ed-essere-vigili/)

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica