5 operazioni per la vostra sicurezza digitale

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)

5 operazioni
per la vostra sicurezza digitale

Internet è diventato parte integrante della nostra quotidianità. In Internet leggiamo le ultime notizie, controlliamo gli orari dei mezzi di trasporto, paghiamo fatture o comunichiamo semplicemente con amici e conoscenti.

Oltre a offrirci tutte queste possibilità, però, Internet ci espone anche a nuovi pericoli. Infiniti software dannosi cercano costantemente di crearsi un varco per accedere ai nostri computer, smartphone o tablet, sui quali sono memorizzati dati personali come foto, lettere o documenti importanti. Se un attacco va a segno, i criminali possono arrecare gravi danni ai vostri dispositivi e a voi stessi: possono infatti modificare o cancellare questi dati oppure sfruttare illecitamente le informazioni contenute al loro interno, per es., per effettuare acquisti su Internet a nome vostro e a spese vostre.

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

Fase 1 **Salvare** i dati

Fase 2 **Proteggere** con un programma antivirus

Fase 3 **Monitorare** con il firewall

Fase 4 **Prevenire** con aggiornamenti software

Fase 5 **Fare attenzione** ed essere vigili

La cintura di sicurezza vi salva dagli infortuni!
Il backup vi salva dalle perdite di dati!

1

Salvare i dati

Quanto sono preziosi i vostri dati? Salvateli regolarmente su almeno un altro supporto e verificate che siano stati effettivamente memorizzati.

Punti importanti

- Salvate regolarmente i vostri dati su un disco rigido esterno, DVD, CD oppure online su un archivio cloud.
- Controllate che i dati siano presenti nel backup e che possano essere ripristinati.
- Per garantire che i vostri dati di backup siano protetti al meglio dal malware, collegate il disco esterno solo quando lo utilizzate ed effettuate la connessione all'archivio online soltanto per l'esecuzione del backup e non in modo permanente.

Oggigiorno su computer, tablet e smartphone si salvano grandi quantità di dati sotto forma di documenti, e-mail, foto, video, musica e molto altro ancora. Non si può escludere che un errore di gestione (come una cancellazione accidentale), un difetto tecnico (per es. nel disco rigido) oppure virus, worm e cavalli di Troia possano causare la distruzione parziale se non completa dei dati.

→ Proteggete i vostri dati con un backup prima di perderli!

www.ebas.ch/step1

Il parabrezza vi protegge!
L'antivirus tiene lontani i parassiti digitali!

2

Proteggere con un programma antivirus

Quali virus penetrano nel vostro computer, tablet o smartphone? Praticamente nessuno, se avete installato un programma antivirus.

Punti importanti

- Utilizzate un programma antivirus aggiornato.
- Impostate il programma antivirus in modo tale che si aggiorni automaticamente e regolarmente e sia quindi in grado di combattere anche le minacce più recenti.
- Verificate regolarmente che sul vostro computer o dispositivo mobile non vi sia malware. A tal fine fate eseguire al programma antivirus una scansione completa del sistema.

Se non si adottano provvedimenti appositi, un computer, tablet o smartphone viene esposto del tutto ai pericoli di Internet e in certi casi potrebbe essere infettato da software dannoso (virus, worm, cavalli di Troia – il cosiddetto malware) in pochissimo tempo. Tutti i dati salvati potrebbero quindi essere visualizzati, manipolati o completamente cancellati da soggetti non autorizzati.

→ Proteggete i vostri dispositivi con un programma antivirus!

www.ebas.ch/step2

Niente furti d'auto grazie al portone del garage!
Niente furti di dati grazie al firewall!

3

Monitorare con il firewall

Avete chiuso le «porte» del vostro computer o dei vostri dispositivi mobili? Un firewall attivo le chiude in modo affidabile e controlla il traffico Internet sul vostro dispositivo.

Punti importanti

- Assicuratevi di attivare il firewall offerto dal vostro sistema operativo prima di collegare il dispositivo a Internet o a un'altra rete.
- Alcuni programmi online, come i giochi via Internet, richiedono l'apertura di determinate «porte d'accesso» (Ports). Fate attenzione ad aprire esclusivamente gli accessi indispensabili e a non disattivare il firewall nel suo complesso.

Quando gli utenti navigano in Internet con il computer, il tablet o lo smartphone, per instaurare la comunicazione si aprono sui dispositivi invisibili «porte d'accesso» (Ports) che li espongono agli attacchi provenienti dalla rete. Una volta installato, il firewall chiude queste porte nella misura necessaria e monitora il traffico dati tra i dispositivi e Internet. Il firewall mostra un avviso quando scopre degli scambi di dati «sospetti».

→ Monitorate la vostra comunicazione Internet attivando un firewall!

www.ebas.ch/step3

Con una manutenzione periodica l'auto è intatta!
Con gli update tutti i programmi sono aggiornati!

4

Prevenire con aggiornamenti software

Chi potrebbe occuparsi della sicurezza dei vostri programmi più dei rispettivi produttori? Prendetevi cura dei vostri programmi e delle vostre applicazioni e installate regolarmente gli ultimi aggiornamenti. Così sarete al sicuro.

Punti importanti

- Attivate la funzione di aggiornamento automatico per tutti i programmi e le app che installate (in particolare sistema operativo, programma antivirus, firewall, browser con relativi componenti aggiuntivi e programmi per la visualizzazione dei documenti).
- Scaricate programmi, app e i relativi aggiornamenti soltanto dal sito del produttore e non da terzi.
- Per accedere a Internet utilizzate sempre e solo l'ultimissima versione del browser.

I programmi obsoleti presentano spesso alcune falle di sicurezza e semplificano agli hacker l'intento di prendere il controllo di un dispositivo. I fornitori di software risolvono tali falle di sicurezza e rendono disponibili le correzioni sotto forma di aggiornamenti dei programmi.

→ **Prevenite installando gli ultimi aggiornamenti software!**

www.ebas.ch/step4

Con responsabilità si viaggia per strade!
Con la testa si naviga in Internet!

5

Fare attenzione ed essere vigili

Qual è un comportamento responsabile? Non credete a tutto ciò che trovate scritto in Internet e navigate sempre con una buona dose di diffidenza. Proteggete il vostro computer e i vostri dispositivi mobili con una password sicura.

Molto spesso la minaccia più grande è rappresentata dall'utente stesso: fate sempre ricorso al vostro buon senso. Con il phishing, per es., via e-mail o al telefono truffatori si spacciano per il vostro istituto finanziario e con un link tentano di spingervi verso un sito Internet che ha tutte le sembianze di quello del presunto istituto finanziario. Se riescono a farvi cadere in trappola e farvi inserire i dati d'accesso al conto elettronico, i truffatori possono saccheggiare indisturbati le vostre finanze. **Ricordate sempre che un istituto finanziario serio non vi contatterà mai via e-mail per conoscere i vostri dati di accesso al servizio e-banking.** Pertanto, in questi casi una buona dose di diffidenza non guasta.

Punti importanti

- Quando navigate in Internet siate sempre diffidenti e prestate attenzione a dove e a chi pubblicate le vostre informazioni personali.
- Gli istituti finanziari, le aziende di telecomunicazioni e altre imprese per la fornitura di servizi non inviano mai ai propri clienti e-mail o telefonate per richiedere la loro password o la modifica della stessa.
- Quando utilizzate dispositivi mobili (smartphone, tablet) adottate le stesse precauzioni che seguite a casa sul computer.

Accurata gestione delle password
Password brevi e non complesse non sono sicure, poiché un aggressore, per es., potrebbe indovinarle. In particolare, non si possono utilizzare cognomi, nomi di figli o animali domestici, parole di una lingua conosciuta, sequenze di tasti (come «asdfg» o «45678») o date di nascita. **La soluzione migliore è formata da combinazioni casuali di almeno 10 lettere maiuscole e minuscole, cifre e caratteri speciali.** Non utilizzate sempre le stesse password dappertutto, ma per i diversi servizi online utilizzate password diverse e non comunicatele a nessuno, annotandole se necessario e conservandole in un luogo sicuro.

- Scegliete password lunghe almeno 10 caratteri, costituite da combinazioni casuali di lettere maiuscole e minuscole, cifre e caratteri speciali.
- Non comunicate mai a nessuno le vostre password e conservatele sempre in un luogo sicuro, se possibile in modo cifrato.
- Non memorizzate nel browser password di accesso a siti web protetti. I browser solitamente non gestiscono queste password in modo abbastanza sicuro.

Creare una password sicura non è per niente difficile:

- Pensate a una frase facilmente ricordabile e formate la password utilizzando le varie iniziali, le cifre e i caratteri speciali: «**M**ia **f**iglia **T**amara **c**ompie **g**li **a**nni **i**l **19 g**ennaio**!**». Otterrete così una password da una sequenza di caratteri a piacere che non avrete difficoltà a ricordare: «**MfTcgai19g!**»

→ Prestate attenzione e navigate in Internet con cautela!

www.ebas.ch/step5

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

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking ma sicuro!

Informazioni su «eBanking – ma sicuro!»

«eBanking – ma sicuro!» è una piattaforma indipendente della Scuola Universitaria Professionale di Lucerna – Informatica che aiuta ad attuare misure di sicurezza dell'informazione personali. Sul sito Internet www.ebankingmasicuro.ch si trovano ulteriori informazioni pratiche sui provvedimenti necessari e le regole di comportamento per un uso sicuro delle applicazioni di e-banking.

- Sito principale:
  https://www.ebankingmasicuro.ch
  https://www.ebas.ch
- Canale YouTube:
  https://www.youtube.com/user/ebankingabersicher
- Area media:
  https://www.ebas.ch/mediasection

Scuola Universitaria Professionale di Lucerna – Informatica

La Scuola Universitaria Professionale di Lucerna – Informatica offre in un unico campus corsi di Bachelor e Master, ricerca e sviluppo orientati all'applicazione, nonché corsi di perfezionamento in informatica e informatica aziendale.

- Sito principale del dipartimento di Informatica:
  https://www.hslu.ch/informatik
- Information Security & Privacy:
  https://www.hslu.ch/forschung-information-security

SKPPSC

Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
3001 Berna

www.skppsc.ch