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, Internet ci espone però 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 **Monitorare** con antivirus e firewall

Fase 3 **Prevenire** con aggiornamenti software

Fase 4 **Proteggere** gli accessi online

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 valgono per voi i vostri dati? Salvateli regolarmente su almeno un altro supporto e controllate che siano stati effettivamente memorizzati.

Punti principali

- 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.
- 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 documenti, e-mail, foto, video, musica e molto altro ancora, sotto forma di dati digitali.

Non si può escludere che un errore di gestione (come una cancellazione accidentale), un difetto tecnico (p. es. nel disco rigido), lo smarrimento o il furto del dispositivo oppure virus, worm e cavalli di Troia possano causare la perdita parziale se non totale di questi contenuti.

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

Maggiori informazioni, con istruzioni dettagliate e strumenti, si possono trovare su:
www.ebas.ch/step1

Con il cockpit, avete tutto sotto controllo!
Con antivirus e firewall, monitorate il traffico dati!

2

Monitorare con antivirus e firewall

Quali «porte d'accesso» sono aperte sul vostro dispositivo e quali virus possono attaccarvi? Praticamente nessuno, se avete attivato un firewall e installato un programma antivirus.

Punti principali

- Utilizzate un programma antivirus e attivate l'aggiornamento automatico.
- Eseguite regolarmente un controllo completo del sistema per identificare eventuali malware.
- Attivate il firewall integrato di Windows o macOS prima di collegare il vostro dispositivo a Internet o a un'altra rete.

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 in pochissimo tempo. Tutti i dati salvati potrebbero quindi essere visualizzati, manipolati o completamente cancellati da soggetti non autorizzati.

→ **Monitorate la vostra comunicazione Internet con un programma antivirus e un firewall attivato!**

Maggiori informazioni, con istruzioni dettagliate e strumenti, si possono trovare su:
www.ebas.ch/step2

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

3

Prevenire con aggiornamenti software

Chi potrebbe occuparsi della sicurezza del vostro software più del suo produttore? Installate regolarmente gli ultimi aggiornamenti per il vostro sistema, i vostri programmi e tutte le app.

Punti principali

- Installate soltanto i programmi e le app che vi servono e scaricateli sempre dal sito del produttore o da uno Store ufficiale.
- Attivate la funzione di aggiornamento automatico per il sistema operativo e tutti i programmi e le app installati.
- 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 il lavoro 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.

Installare soltanto il software e le app di cui si ha bisogno
Installate soltanto i programmi e le app di cui avete davvero bisogno e accertatevi che provengano da una fonte affidabile, cioè direttamente dal produttore o dallo Store ufficiale (p. es. l'App Store di Apple o Google Play Store).

Mantenere aggiornati i dispositivi
Assicuratevi di utilizzare sempre la versione più recente di un software. Alla base di tutto c'è sempre un sistema operativo aggiornato. Anche tutti gli altri programmi installati (p. es. browser come Firefox, Chrome o Adobe Acrobat Reader), però, devono essere aggiornati all'ultimissima versione.

→ Prevenite installando gli ultimi aggiornamenti software!

Maggiori informazioni, con istruzioni dettagliate e strumenti, si possono trovare su:
www.ebas.ch/step3

Con la chiave, nessun furto d'auto!
Con la password, nessun furto di dati!

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 10 caratteri, composte da cifre, lettere maiuscole e minuscole e caratteri speciali).
- Non utilizzate sempre le stesse password dappertutto, ma sceglietene diverse per i vari servizi online.
- Se possibile, attivate la cosiddetta autenticazione a doppio fattore.

Accurata gestione delle password

Password brevi e semplici non sono sicure, poiché un hacker, per es., potrebbe indovinarle. In particolare, si sconsiglia di utilizzare cognomi, nomi di figli o animali domestici, parole in 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 sceglietene diverse per i vari servizi online e non comunicatele a nessuno. Se necessario, annotatele e conservatele in un luogo sicuro.

Creare una password sicura non è per niente difficile: pensate a una frase facile da memorizzare e formate la password utilizzando varie iniziali, cifre e caratteri speciali: «**M**ia **f**iglia **T**amara **c**ompie **g**li **a**nni **i**l **19** **g**ennaio**!**» Otterrete così una password con una sequenza di caratteri a piacere che non avrete difficoltà a ricordare: «**MfTcgai19g!**».

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

5

Fare attenzione ed essere v

Voi credete a ogni cosa che vi viene detta? A
persona e navigate sempre in Internet con u

Autenticazione a doppio fattore
Abbinata a una password sicura, la cosiddetta autenticazione a doppio fattore offre una sicurezza ancora più grande. 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.

Punti principali

- Quando navigate in Internet siate sempre diffidenti e prestate attenzione a dove pubblicate e a chi fornite 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 non telefonano per chiedere la loro password o la modifica della stessa.
- Quando utilizzate dispositivi mobili (smartphone, tablet) adottate le stesse precauzioni che seguite a casa sul computer.
- Chiedete supporto se avete dubbi o nutrite il sospetto di essere stati vittima di un attacco.

→ Proteggete i vostri dispositivi e gli accessi online da utilizzi non autorizzati!

Maggiori informazioni,
con istruzioni dettagliate e strumenti,
si possono trovare su:
www.ebas.ch/step4

trade si viaggia con responsabilità!
net si naviga con buonsenso!

vigili

Assumetevi le vostre responsabilità in prima
na buona dose di diffidenza.

Attuando le fasi da 1 a 4 avete creato un'ottima protezione tecnica per i vostri dispositivi e accessi online. Spesso, tuttavia, il rischio maggiore è rappresentato dal comportamento dell'utente stesso, ed è questo a finire nel mirino degli attacchi: per questo motivo, fate sempre ricorso al vostro buon senso.

Protezione contro il phishing e il social engineering
Con il phishing via e-mail o al telefono, i truffatori cercano di conquistarsi la vostra fiducia spacciandosi p. es. per il vostro istituto finanziario e attirandovi su un sito Internet dall'aspetto simile a quello del vostro 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.

Rischi maggiori con i dispositivi mobili
Molte app si prendono, senza chiari motivi, ampi diritti. Per esempio, non è necessario che ogni singola app acceda ai dati della posizione, alla rubrica o allo stato del telefono. Per questo motivo, è consigliabile valutare con occhio critico se i diritti d'accesso sono realmente necessari per l'esecuzione delle funzioni e se non è il caso di disattivare tutti i diritti non indispensabili.

→ Prestate attenzione e navigate in Internet con cautela!

Maggiori informazioni,
con istruzioni dettagliate e strumenti,
si possono trovare su:
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, creata dal dipartimento di Informatica della Scuola Universitaria Professionale di Lucerna, che vi aiuta a garantire la sicurezza delle vostre informazioni personali. Sul sito Internet www.ebas.ch si trovano ulteriori informazioni pratiche sui provvedimenti necessari e le regole di comportamento da adottare per un uso sicuro delle applicazioni di e-banking.

- Sito principale: **https://www.ebas.ch**
- Pagina Facebook:
  https://www.facebook.com/ebankingabersicher
- Canale YouTube:
  https://www.youtube.com/user/ebankingabersicher
- Area media:
  https://www.ebas.ch/mediasection

Scuola Universitaria Professionale di Lucerna – Dipartimento di Informatica

Il dipartimento di Informatica della Scuola Universitaria Professionale di Lucerna offre in un unico campus corsi di Bachelor e Master, la possibilità di effettuare lavori di 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

Gennaio 2020