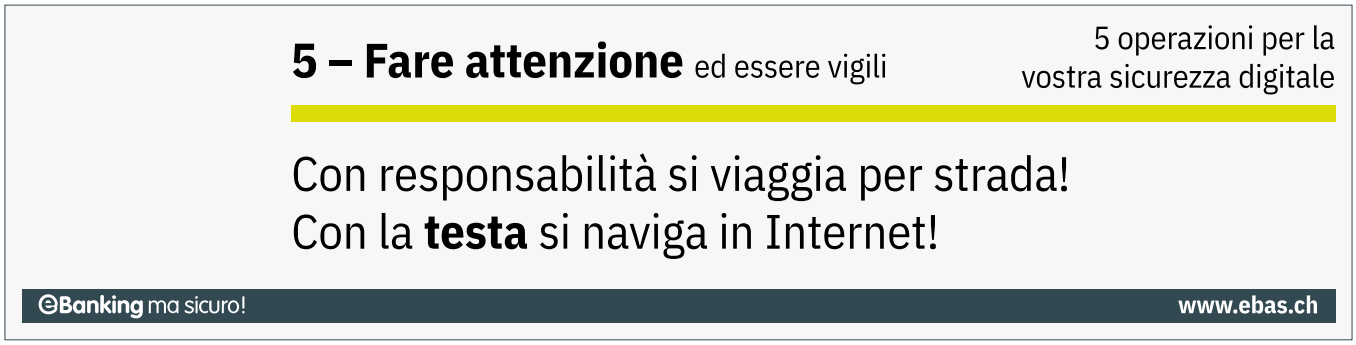
5 – Fare attenzione ed essere vigili

Voi credete a ogni cosa che vi viene detta? Fatevi carico delle vostre responsabilità in prima persona e navigate sempre in Internet con una buona dose di diffidenza.

Punti principali:

- 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 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.



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 (https://www.ebas.ch/it/phishing/), via e-mail o al telefono 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.

Oppure, con delle telefonate fraudolente dall'assistenza (https://www.ebas.ch/it/telefonate-fraudolente-dallassistenza/), venite contattati da un presunto collaboratore di Microsoft o di una società di assistenza informatica che tenterà di accedere al vostro dispositivo.

Ricordate sempre che un istituto finanziario serio non vi contatterà mai via e-mail o al telefono per conoscere i vostri dati di accesso al servizio di e-banking.

Le conoscenze di base per sferrare questo genere di attacchi, i truffatori le trovano spesso su media e reti sociali (https://www.ebas.ch/it/media-e-reti-sociali/). Usate prudenza anche lì, valutando bene quali informazioni pubblicate su

di voi.

Rischi maggiori con i dispositivi mobili

Diritti d'accesso delle app 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 possibile, disattivare tutti i diritti non indispensabili.

Come regola generale, siate restii a diffondere la vostra posizione: evitate i servizi di localizzazione e non memorizzate le informazioni sulla posizione nelle foto che caricate su Internet, perché potrebbero essere sfruttate da ladri e hacker.

Bloccare immediatamente in caso di smarrimento
Varie app permettono di bloccare in remoto i dispositivi persi o rubati. L'operazione cancella dal dispositivo i vostri dati personali, che quindi non saranno più consultabili. Attenzione però: questi comandi possono essere utilizzati anche da terzi malintenzionati. Quindi anche a questo proposito accertatevi di rivolgervi a un fornitore affidabile. Dopo aver bloccato il dispositivo, è consigliabile contattare anche l'operatore per far bloccare la scheda SIM.

Chiedere aiuto

Se avete dei dubbi, nutrite il sospetto di essere stati vittima di un attacco o se vi è già successo davvero, non esitate a chiedere aiuto – per esempio:

- In caso di incertezze o dubbi sul servizio di e-banking, contattate il vostro istituto finanziario (https://www.ebas.ch/it/partner/).
- Se vi sono problemi tecnici o sospettate un'infezione da malware, chiedete consiglio e aiuto a un esperto IT o un operatore di un servizio di assistenza informatica.
- Se siete stati vittima di un attacco, segnalatelo al vostro istituto finanziario (https://www.ebas.ch/it/partner/) e alla polizia (https://polizei.ch).

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 (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/)
Fase 5 – Fare attenzione