23.03.2020

Effettuare operazioni bancarie da casa – ma sicuro!

A causa del coronavirus il Consiglio federale raccomanda di restare in casa se possibile. Grazie all'e-banking, per le operazioni bancarie in generale non è un problema. Per alcune esigenze, tuttavia, serve il contatto personale con il consulente alla clientela. Anche in questo caso ci sono delle alternative sicure.

Per contenere la diffusione del coronavirus, la popolazione svizzera è invitata a non lasciare la propria abitazione, se possibile. Molte operazioni finanziarie, come i trasferimenti, si possono eseguire con la massima comodità e sicurezza tramite e-banking. Per alcune esigenze, tuttavia, è necessario un colloquio con il proprio referente personale presso la banca. Come si può organizzare in modo sicuro un incontro di questo tipo?

In molti casi è possibile e sufficiente una telefonata al vostro consulente alla clientela. Tuttavia, se bisogna mostrare documenti – p. es. un contratto – o spiegare programmi, la questione si complica. Attualmente le banche offrono la possibilità di avviare una videoconferenza o una sessione di assistenza remota. A questo riguardo vi invitiamo a leggere le nostre indicazioni sull'uso sicuro dell'assistenza remota (https://www.ebas.ch/it/uso-sicuro-dellassistenza-remota/) .

Occorre prestare maggiore prudenza quando si ricevono e-mail, SMS, messaggistica istantanea o telefonate inaspettate – anche se sembrano provenire da una persona o una ditta conosciuta. Attualmente, p. es., circolano e-mail di phishing dall'aspetto ingannevole e aventi come mittente una banca tedesca, con le quali si invitano i clienti a inserire i propri recapiti su un sito Internet contraffatto. Come pretesto viene citata la chiusura di determinate filiali. Si può prevedere che simili tentativi di phishing avverranno anche a nome di istituti finanziari svizzeri.

In generale, i criminali non esitano ad approfittare con grande sfrontatezza della situazione attuale legata al coronavirus:

- e-mail contraffatte inviate la settimana scorsa a nome dell'Ufficio federale della sanità pubblica (UFSP) miravano a indurre gli utenti a installare un malware mascherato da documento innocuo allegato al messaggio, il quale consente l'accesso completo al computer della vittima.
- Già il giorno successivo i truffatori hanno provato, di nuovo a nome dell'UFSP, di carpire informazioni sensibili al telefono.
- Non molto tempo dopo, hanno cominciato a circolare e-mail aventi come allegato una presunta mappa sulla diffusione del coronavirus o un e-book su come proteggersi dal contagio, quando in realtà si trattava di un cavallo di Troia.
- Dallo scorso fine settimana sono in circolazione e-mail di ricatto con le quali i criminali minacciano di infettare il destinatario con il coronavirus, perché indicano di sapere di preciso dove vive.
- Da ultimo, ma non per importanza, si moltiplicano i negozi online contraffatti, che offrono prodotti altrimenti esauriti come le mascherine protettive, ma non consegnano nessuna merce dopo aver incassato il pagamento anticipato.

Proteggetevi dai truffatori gestendo con grande attenzione tutti i messaggi elettronici, non aprendo gli allegati che

contengono né facendo clic su nessun link, se non potete verificare con certezza chi è il mittente. E non condividete in linea di massima nessuna informazione sensibile su di voi e i vostri accessi online con terzi od offerenti sconosciuti, né in Internet né al telefono.

Ulteriori informazioni su altre forme di protezione si possono trovare nei nostri articoli sul phishing (https://www.ebas.ch/it/phishing/) e sulle telefonate fraudolente dall'assistenza (https://www.ebas.ch/it/telefonate-fraudolente-dallassistenza/) .