Accesso di terze parti ai conti bancari

Diverse terze parti offrono servizi interbancari di pagamento e informazioni per i clienti dei servizi e-banking. Si tratta di un servizio comodo, ma non privo di rischi.

Proteggetevi così:

- Non comunicate i vostri dati d'accesso personali per l'e-banking (password, PIN, numero di identificazione ecc.) a nessuno, né ad altre persone né agli operatori di una terza parte.

Per accedere ai conti bancari solitamente vengono chiesti e utilizzati i dati d'accesso dei sistemi e-banking dei clienti. Trasmettendo le vostre credenziali d'accesso personali a terzi, come clienti vi esponete a un notevole rischio per la sicurezza. Inoltre i vostri dati di clienti bancari possono essere portati da queste terze parti in ambienti sottoposti a discipline meno rigide rispetto ai sistemi fortemente regolamentati cui sono sottoposti gli istituti finanziari svizzeri (FINMA, legge sulle banche ecc.).

Fate attenzione!

Tanto l'uso dell'impersonificazione quanto il trattamento e la memorizzazione dei dati dei clienti bancari in modo non conforme alle direttive celano rischi significativi per voi.

«eBanking – ma sicuro!» sconsiglia pertanto di trasmettere a terzi i propri dati d'accesso personali per i sistemi e-banking.

Maggiori informazioni:

Utilizzo rischioso dei servizi interbancari online

Tra i servizi offerti dalle terze parti che utilizzano i dati d'accesso personali ai sistemi e-banking dei clienti vi sono per esempio l'accesso ai conti bancari di diversi istituti finanziari tramite un'unica piattaforma. Bisogna però fare attenzione: trasmettendo le vostre credenziali d'accesso personali a una piattaforma di questo tipo vi esponete a un notevole rischio in termini di sicurezza.

L'impersonificazione come rischio per la sicurezza

Per accedere ai conti bancari dei loro clienti le terze parti utilizzano solitamente la procedura nota come impersonificazione (in inglese «impersonation», ossia il presentarsi come qualcun altro). A tal fine richiedono solitamente i dati d'accesso personali dei clienti (quali la password e il numero di identificazione) per accedere al rispettivo sistema e-banking; i dati vengono quindi utilizzati per accedere in modo illimitato ai conti operando come intermediario.

Se come clienti comunicate i vostri dati d'accesso personali in questo modo, è come se andaste a prenotare le vostre ferie all'agenzia di viaggio e per pagare decideste di far accedere l'impiegato al vostro account e-banking e poi ve ne andaste dal negozio – fidandovi ciecamente che lui davvero addebiterà soltanto l'importo concordato e poi eseguirà immediatamente il logout. Quella persona, però, potrebbe benissimo sfruttare l'occasione per andare a vedere che salario vi viene accreditato ogni mese, e persino essere tentata di pagarsi le ferie proprie con i soldi vostri. Tecnicamente l'uso dell'impersonificazione equivale a un furto dell'identità – segue la stessa procedura di un classico attacco di phishing (https://www.ebas.ch/it/phishing/) –, anche quando si tratta di una terza parte seria!

Se i dati d'accesso personali vengono utilizzati in modo non conforme alle direttive, l'istituto finanziario non ha alcun modo di sapere se sta comunicando con il cliente stesso, con una terza parte legittimamente incaricata o – nel peggiore dei casi – con un intermediario criminale. Di conseguenza l'istituto finanziario non può più adempiere adeguatamente ai propri obblighi di diligenza, quali ad esempio la protezione dei dati dei clienti bancari. In caso di danni, il cliente può trovarsi addirittura con le mani legate da clausole di esclusione della responsabilità.

Perdita di controllo sui dati dei clienti bancari

Mentre gli istituti finanziari svizzeri sono soggetti a una serie di rigide istruzioni riguardo alla protezione dei dati dei loro clienti bancari e alla sicurezza dei sistemi in uso, con il vostro consenso le terze parti possono memorizzare e trattare i dati in ambienti e sistemi meno disciplinati. In alcuni casi questi sistemi non sono né di proprietà né sotto il controllo delle terze parti. Spesso infatti vengono utilizzate cosiddette soluzioni cloud, con le quali non di rado non si conosce l'esatto luogo di memorizzazione dei dati. Solitamente per questi sistemi non è previsto nemmeno il segreto bancario svizzero!

È difficile stimare gli effetti di questa perdita del controllo sull'archiviazione dei dati personali. Non da ultimo, in questo modo è più semplice per i malintenzionati ottenere accesso ai dati personali dei clienti bancari.