Scheda informativa

Internet ed e-banking: come proteggersi dalle truffe

Di cosa si tratta

Il numero dei casi di truffa sale di anno in anno – il che è davvero preoccupante. I criminali informatici sono sempre più astuti rendendo ancora più complicato riconoscere a colpo d'occhio una truffa o un attacco al conto in banca oppure alla carta di credito. Molti truffatori del web utilizzano degli stratagemmi di natura psicologica mettendo sotto pressione le vittime. Nel peggiore dei casi, riescono ad ottenere l'accesso alle password, ai dati di accesso ai conti bancari nonché alle informazioni personali e confidenziali dei clienti. Questa scheda informativa riporta gli errori più frequenti e le modalità per evitarli.

E-banking: occhio agli attacchi di phishing

Al giorno d'oggi, molti utenti in Svizzera effettuano le proprie operazioni bancarie online sul proprio PC, tablet o smartphone. Le banche ce la mettono tutta per fornire ai clienti dei sistemi di e-banking sicuri. Gli attacchi non sono in genere diretti alle banche stesse, ma ai dispositivi dei clienti. Le seguenti modalità di raggiro sono particolarmente note e diffuse.

Phishing: significa letteralmente «pescare» e allude all'uso di tecniche per appunto «pescare» le password. I criminali cercano di captare i dati riservati dei clienti bancari per attingere ai loro risparmi. Le analisi svolte dalla Prevenzione Svizzera della Criminalità (PSC) mostrano che gli attacchi di phishing possono assumere forme sempre diverse. Vi sono però alcuni tratti identificativi comuni, come illustrato qui di seguito.

- I truffatori inviano e-mail ingannevoli in cui si spacciano ad esempio per collaboratori di una banca. In queste e-mail, i clienti sono indotti a credere che le informazioni del loro conto e i dati di accesso non sono più al sicuro – e che quindi devono essere aggiornati cliccando sul link fornito nell'e-mail.
- Il presunto link non porta però al sito web ufficiale della banca, ma a una pagina fittizia e ingannevolmente simile a quella originale. Tutti i dati personali inseriti vengono trasmessi direttamente ai truffatori.
- I criminali utilizzano poi i dati di accesso rubati per effettuare trasferimenti di denaro in men che non si dica – spesso si tratta di diverse decine di migliaia di franchi sottratti indebitamente dai conti bancari delle vittime: si tratti di soldi che perlopiù non possono essere poi rivendicati oppure recuperati.

Consigli: presti attenzione a questi punti quando utilizza il suo e-banking

Segua le consuete raccomandazioni comportamentali per utilizzare il suo e-banking in modo sicuro. Qui di seguito trova un riepilogo conciso delle principali indicazioni e accortezze da seguire.

- Digiti sempre manualmente l'URL della pagina di login dell'e-banking nella barra degli indirizzi del suo browser. Non cerchi queste pagine tramite i motori di ricerca come Google, Bing, ecc.
- In caso di incertezza in merito all'autenticità della pagina di login, verifichi che sia stata stabilita una connessione SSL sicura (protocollo di comunicazione «https://», icona del lucchetto).
- L'indirizzo Internet corretto è riportato accanto al lucchetto o dopo aver cliccato su di esso.
- Si assicuri che l'indirizzo Internet della pagina di login sia riportato correttamente. I truffatori spesso modificano solo singole lettere dell'indirizzo.
- Interrompa immediatamente la procedura di login e la connessione se si verifica un'interruzione del sistema (ad esempio, una schermata bianca improvvisa) o se appaiono messaggi di errore insoliti (ad esempio: «Il sistema è attualmente sovraccarico. La invitiamo ad attendere qualche istante e a riprovare»).
- Se si trova in viaggio o, in generale, fuori casa, digiti i dati di accesso con circospezione e soprattutto lontano da occhi indiscreti.
- Acceda al suo portale e-banking solo tramite dispositivi sicuri e noti. Tutti i dispositivi e supporti Internet aperti e accessibili al pubblico, come quelli degli alberghi, sono sconsigliati per questo genere di operazioni.
- Contatti immediatamente la sua banca se nota qualcosa di insolito.

Phishing sui motori di ricerca: molti clienti delle banche accedono all'e-banking cercando prima la pagina di login della loro banca su Internet, ad esempio su Google, Bing o Yahoo. Sottovalutano quanto sia pericoloso, perché i criminali promuovono le loro pagine web fraudolente di e-banking anche attraverso i motori di ricerca più popolari.

- Quando si lancia una ricerca, la finta pagina di login della banca salta subito all'occhio. Infatti, l'esperienza dimostra che appare in cima all'elenco dei risultati di ricerca ed è spesso contrassegnata come «Sponsorizzata», «Pubblicità» o «Annuncio».
- Chiunque clicchi su un link di questo tipo tra i risultati visualizzati, finisce su una pagina di e-banking fittizia che sostanzialmente assomiglia alla pagina autentica e legittima della banca.
- Chiunque inserisca i dati di accesso personali dell'e-banking non sa quindi che questi dati finiscono direttamente nelle mani dei truffatori.
- Con i dati di login, i truffatori possono poi accedere all'effettivo portale di e-banking dell'istituto in questione e sottrarre denaro al titolare del conto.

Phishing tramite SMS (smishing): anche i servizi di messaggistica, come SMS e WhatsApp, sono bersagli di pericolosi attacchi, perché i criteri per riconoscere le e-mail di phishing non sono spesso efficaci.

- I truffatori inviano alle vittime messaggi di testo fittizi spacciandosi per collaboratori della banca o del servizio tecnico di un istituto finanziario.
- Ai destinatari di questo tipo di messaggi fittizi viene fatto credere che le informazioni e i dati di accesso relativi al proprio conto non siano più in sicurezza.
- Con questo pretesto, i clienti vengono ingannati e indotti ad «aggiornare» i propri dati di accesso all'e-banking tramite un link nel messaggio di testo.
- Questo link conduce però a un sito web fraudolento che assomiglia alla solita area di login della banca.
- I criminali informatici poi «pescano» i dati di accesso immessi dai clienti su questa pagina fittizia.

Phishing vocale (vishing): i truffatori non esitano a contattare i clienti delle banche per telefono. Questi attacchi sono noti come «vishing» e sono in aumento.

- I truffatori chiamano i clienti e fingono una falsa identità. Ad esempio, fanno finta di essere funzionari di un'autorità pubblica, come la polizia, o dipendenti di una banca – o collaboratori di una grande società come Microsoft o Swisscom.
- Nel corso della conversazione, i truffatori intimidiscono e mettono le vittime sotto pressione utilizzando una serie di astute tecniche manipolatorie e minacciando gravi danni e conseguenze. E tutto ciò con il fine di spingere i clienti delle banche a compiere azioni e gesti del tutto irrazionali.
- Al cliente di una banca può essere chiesto, ad esempio, di installare immediatamente un presunto programma di sicurezza di nuova generazione, perché il suo computer è stato infettato da un virus.
- Nella maggior parte dei casi, si tratta di un malware, ossia un software intrusivo e malevolo. Una volta che un programma del genere è stato installato sul computer del malcapitato, i criminali informatici possono appropriarsi dei dati di accesso (login e password) dei clienti – e quindi attingere anche ai loro conti e risparmi in men che non si dica.

Consigli: come proteggersi dagli attacchi di phishing

I truffatori e i criminali informatici affinano continuamente i loro metodi e stratagemmi e cercano di sfruttare appieno il potenziale della tecnologia di riferimento. Spesso utilizzano una potente combinazione di phishing, vishing e smishing. Quindi, tenga conto e faccia tesoro dei seguenti consigli e spunti di riflessione.

- Nessuna banca o organizzazione rispettabile la contatterà via e-mail, SMS, WhatsApp o telefono per chiederle i suoi dati di accesso.
- Pertanto, non comunichi in nessun caso informazioni e dati riservati tramite telefono, e-mail o siti web sconosciuti.
- Elimini i messaggi sospetti e svuoti subito il cestino del dispositivo in questione. Lo faccia anche se non ha la totale certezza che un messaggio sia autentico o fraudolento.
- Guardi con occhio sospetto alle e-mail inaspettate nella posta in arrivo.
- Non si lasci intimidire se qualcuno richiede i suoi dati personali e la minaccia di ripercussioni come la sottrazione di denaro, accuse penali o il blocco della carta.
- Utilizzi password sicure e mantenga sempre aggiornati il sistema operativo, il browser e il client di posta elettronica. Aggiorni regolarmente il suo programma antivirus.
- I filtri antispam o i software anti-phishing sono validi strumenti per riconoscere i siti e le e-mail sospetti. Scarichi i software solo dai portali di distribuzione ufficiali.
- Controlli regolarmente gli estratti conto della banca e della carta di credito e comunichi immediatamente alla banca eventuali discrepanze.

Fonti: Svizzera. Prevenzione della criminalità, Fondazione per la protezione dei consumatori, www.ebas.ch/it/phishing

Investimenti e immobili: occhio alle truffe

I criminali informatici si rimboccano le maniche e utilizzano le tecnologie più recenti per ingannare i clienti delle banche, i consumatori e gli utenti del web. Secondo l'Ombudsman bancario svizzero, è opportuno adottare molta cautela. Questo anche perché coloro che, ad esempio, effettuano volontariamente pagamenti senza rendersi conto di essere stati vittime di frode, devono poi fare i conti con le conseguenze in prima persona, visto che le banche non si assumono in genere la responsabilità per questi casi. Queste truffe sono diffuse a macchia d'olio.

Truffa dell'investimento online: i criminali utilizzano annunci aggressivi via e-mail e sui social media per pubblicizzare presunte piattaforme di investimento che promettono profitti rapidi o addirittura una fortuna milionaria. Per guadagnarsi la fiducia delle vittime, falsificano i siti web dei media affidabili. Secondo le autorità cantonali, chi si registra su queste piattaforme fraudolente, viene contattato tramite e-mail o telefono nell'arco di poco tempo. L'obiettivo dei truffatori è quello di convincere le vittime a versare denaro quanto prima. Questi fondi verrebbero poi investiti in prodotti di investimento o in criptovalute. Ma alla fine della fiera, non viene investito o negoziato proprio nulla, perché il denaro finisce direttamente nelle tasche dei truffatori. Dietro queste elaborate macchinazioni si cela una rete di criminali attivi a livello internazionale che è sempre all'avanguardia della tecnologia e gestisce addirittura i propri call center. Presti attenzione e non si lasci ingannare dalle apparenze. Nessun fornitore di servizi finanziari affidabile garantisce profitti superiori alla media nel breve termine. Segua anche le raccomandazioni delle autorità e della polizia. L'Autorità federale di vigilanza sui mercati finanziari (FINMA) gestisce una lista di allerta (www.finma.ch/it/finma-public/lista-di-allerta). Segnali le offerte sospette alla FINMA.

Truffa dell'agente finanziario: i truffatori cercano spesso persone che possono essere strumentalizzate impropriamente come «agenti finanziari». Si rivolgono a soggetti in cerca di lavoro e in difficoltà finanziarie presentando loro interessanti offerte di lavoro – tramite portali online, social media e annunci sui giornali. I criminali spesso hanno un sito web dall'aspetto legittimo e credibile o usano impropriamente il nome di un'azienda di tutto rispetto. Però attenzione, perché di solito dietro a tutto ciò si prospettano intenzioni di natura criminale. I truffatori utilizzano i conti bancari delle vittime che reclutano, ad esempio, per spostare le somme illecite. Anche il trasferimento di beni in una criptovaluta come il Bitcoin viene richiesto sempre più spesso. In contropartita, verrebbe offerto un compenso finanziario sotto forma di provvigione. Faccia attenzione se le viene promesso del denaro veloce per un'esigua mole di lavoro. Chi viene coinvolto in operazioni di questo tipo può anche essere accusato di riciclaggio di denaro.

Truffa del pagamento anticipato: è opportuno essere prudenti anche quando si cerca una casa o una proprietà interessante da acquistare. Le autorità segnalano sempre più spesso casi di frode dovuti ad annunci fraudolenti. Ad esempio, i truffatori copiano annunci di appartamenti in affitto esistenti e li offrono come appartamenti in proprietà a un prezzo allettante – su noti portali immobiliari, sui social media o su siti web all'apparenza autentici ma in realtà fraudolenti. Le pubblicità fungono da esca. Chi risponde viene poi contattato da truffatori professionisti. Ad esempio, gli autori chiedono una copia del passaporto o della carta d'identità. Per sembrare affidabili, si identificano anche con quello che dicono essere il loro documento d'identità – che spesso è però falso o appartiene a una vittima precedente. I truffatori fingono di prenotare l'immobile per il potenziale acquirente. Prima di far visionare la proprietà, richiedono però il versamento di un deposito, il quale poi sparisce senza alcuna possibilità di rintracciare i colpevoli. Consiglio: diffidi da qualunque inserzione troppo bella per essere vera. Non invii mai soldi tramite un servizio di trasferimento di denaro se non ha sottoscritto un contratto legalmente valido e non ha mai visionato la proprietà in questione. Inoltre, per fugare ogni dubbio, mostri sempre le inserzioni di natura sospetta a uno specialista.

Altre comuni forme di truffa

Esistono anche altre forme di truffa. Le persone dai 55 anni in su sono particolarmente bersagliate, come dimostra uno studio condotto da Pro Senectute. L'organizzazione stima l'ammontare dei danni provocati dalle frodi a circa 675 milioni di franchi all'anno. Tuttavia, persino i fondatori di imprese emergenti (startup) possono cadere vittime dei perfidi tranelli orditi dai truffatori. Vi sono alcune tipologie di truffa molto diffuse che vanno sempre tenute a mente.

Trucco del falso nipote: il truffatore spesso finge di essere un parente che si trova in difficoltà finanziarie e ha urgente bisogno di aiuto da parte della famiglia. Si mette in contatto telefonicamente con la vittima, chiede il nome e altre informazioni personali per poi manipolarle e sfruttarle a proprio vantaggio. Finge di essere il presunto parente che per vari fantomatici motivi non è in grado di prelevare il denaro autonomamente e invia quindi un amico o un conoscente.

Consiglio: faccia attenzione se non riconosce immediatamente un presunto parente al telefono. Se in dubbio, non esiti a riagganciare. E non consegni mai denaro o oggetti di valore a sconosciuti, anche se si presume che siano persone autorevoli come agenti di polizia, avvocati o collaboratori del tribunale.

Chiamata shock: in questa scenario di frode telefonica aggressiva, a chiamare la vittima è una presunta figura autoritaria come un primario, un avvocato o un poliziotto. Questo attore annuncia alla vittima una finta notizia scioccante ma che sembra del tutto credibile. Nella maggior parte delle versioni riportate, viene tirato in ballo un familiare che si trova presuntamente in una grave situazione d'emergenza o in grosso pericolo. I truffatori chiedono alle vittime di consegnare denaro e oggetti di valore a un messaggero per aiutare il familiare. A causa dello shock emotivo, le vittime spesso non sono in grado di pensare razionalmente e cadono ingenuamente nella trappola.

Consiglio: le chiamate shock si riconoscono dal messaggio stesso che è sempre associato a un'urgente richiesta di denaro. Si insospettisca se riceve un messaggio scioccante, se qualcuno le mette pressione e le chiede di versare immediatamente del denaro. Anche in questi casi, non ci pensi due volte e riagganci.

Iscrizioni nel registro: dopo l'iscrizione della nuova azienda nel registro di commercio, i neofondatori ricevono spesso posta per l'iscrizione nei vari registri. A colpo d'occhio, i moduli ricevuti sembrano documenti ufficiali delle autorità. Nella maggior parte dei casi, tuttavia, si tratta di contratti a pagamento per l'iscrizione in inutili registri aziendali, industriali o di marchi, elenchi telefonici, mappe locali e simili. Non deve mai sottoscrivere contratti di questo tipo. **Consiglio:** non cada nelle cosiddette «truffe degli annuari». Paghi sempre e solo le fatture ufficiali del registro di commercio del cantone di competenza e di eventuali partner quali notai e fiduciari.

Link importanti

Su Internet sono presenti le più disparate interfacce dove gli utenti hanno la possibilità di informarsi a fondo in merito alle questioni di sicurezza informatica e alle truffe attualmente in circolazione nonché di fare tesoro di preziosi consigli e spunti di riflessione su come proteggersi da queste minacce telematiche.

- Prevenzione Svizzera della Criminalità: **www.skppsc.ch/it/**
- «eBanking – ma sicuro!»: **www.ebas.ch/it/**
- Ufficio federale della cibersicurezza UFCS: **www.ncsc.admin.ch**

La consulenza migliore

VZ VermögensZentrum è il fornitore di servizi finanziari indipendente numero uno in Svizzera. I nostri clienti arrivano preparati alla pensione, investono il loro denaro in modo ponderato, finanziano la loro casa di proprietà a condizioni vantaggiose, sono assicurati al meglio, definiscono la successione secondo le proprie volontà e non versano più imposte del dovuto.

A VZ si affidano anche numerose aziende e casse pensioni: queste sono così in grado di ottimizzare le prestazioni assicurative e previdenziali, ottenere migliori profitti e, al contempo, risparmiare su premi, spese e imposte.

Quando si tratta di denaro, VZ è l'indirizzo giusto.

VZ VermögensZentrum SA (sede principale)
Riva Giocondo Albertolli 1, 6900 Lugano
Telefono 091 912 24 24
vzlugano@vzch.com
www.vzch.com

Aarau I Affoltern am Albis I Baden I Basilea I Bellinzona I Berna I Briga
Burgdorf I Coira I Friburgo I Ginevra I Horgen I Kreuzlingen I Losanna
Lenzburg I Liestal I Lucerna I Lugano I Meilen I Neuchâtel I Nyon I Olten
Rapperswil I Rheinfelden I San Gallo I Sciaffusa I Sion I Soletta I Sursee
Thun I Uster I Vevey I Wil SG I Winterthur I Zugo I Zurigo