19.12.2023

Attenzione – i tentativi di truffa si fanno subdoli

Autorità e banche lanciano l'allarme: i criminali cercano sempre più spesso di accedere all'e-banking dei consumatori. Con strumenti professionali e un discreto tasso di successo.

Sono tante e tutte ben architettate le truffe che in questo periodo tengono impegnati diversi istituti finanziari e la loro clientela.

Da un lato, si trovano online copie autentiche di pagine di banche (siti di phishing) cui si accede attraverso link contenuti in e-mail di phishing o risultati dei motori di ricerca. Se vi si inseriscono i propri dati di accesso, i malintenzionati li trasmettono in tempo reale alla pagina di accesso corretta della banca in questione. In un passaggio successivo, il secondo fattore di sicurezza proveniente dalla pagina reale della banca – ad esempio un codice QR, una combinazione di numeri o un'immagine a mosaico – viene anch'esso ripreso in tempo reale nella pagina contraffatta e confermato dalla vittima, ignara: a questo punto, i truffatori possono accedere all'e-banking. Un trasferimento illecito di denaro viene poi trasmesso alla vittima secondo lo stesso schema, affinché lo convalidi.

Un modello di truffa simile riguarda chi mette oggetti in vendita su piattaforme di annunci e d'asta. In questo caso, un truffatore si presenta come potenziale acquirente e chiede i dati di contatto della vittima per pagare l'articolo tramite fornitori di servizi di pagamento come PayPal. I dati così ottenuti vengono successivamente utilizzati per ulteriori fasi di attacco, che alla fine possono portare all'intrusione nel portale di e-banking del venditore.

In un altro caso ancora, i criminali si presentano telefonicamente come dipendenti o addetti alla sicurezza di un istituto finanziario per ottenere informazioni sensibili come le credenziali di accesso all'e-banking della o del cliente. Non di rado viene falsificato anche il numero di telefono per ottenere la fiducia della vittima. Anche in questo caso, spesso viene utilizzato il phishing in tempo reale descritto sopra per scardinare il sistema di doppia autenticazione dell'e-banking.

Anche le truffe sugli investimenti (in inglese «Investment Fraud») vanno per la maggiore. Spesso si comincia con un'offerta di lavoro redditizia o la rivelazione di presunti scandali di persone di spicco. Dopo un periodo di costruzione della fiducia, in genere le vittime sono incoraggiate a depositare una piccola somma su un portale di investimento apparentemente redditizio, dopo di che vengono mostrati sulla piattaforma dei profitti falsi per stimolare il deposito di ulteriori somme. In realtà, però, i soldi finiscono nel conto bancario dei criminali.

Proteggetevi dal phishing così:

- Non utilizzate mai un link ricevuto via e-mail, SMS o servizio di messaggistica o scansionato tramite codice QR per accedere a un istituto finanziario.
- Gestite con grande prudenza gli allegati delle e-mail e dei servizi di messaggistica breve.
- Durante le telefonate non comunicate mai informazioni riservate come le password.
- Inserite l'indirizzo della pagina di accesso del vostro fornitore di servizi online o istituto finanziario sempre manualmente, nella barra degli indirizzi del browser.
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario.

Per proteggervi dalle frodi sugli investimenti, seguite queste regole di condotta:

- Non lasciatevi abbindolare da promesse irrealistiche. Nessun fornitore di servizi finanziari affidabile promette profitti superiori alla media in breve tempo.
- Eseguite delle ricerche sul fornitore, ad esempio su Google, forum online o siti di informazioni per i consumatori. Verificate se l'offerente dispone di un'autorizzazione della FINMA (https://www.finma.ch/it/finma-public/istituti-persone-e-prodotti-autorizzati/) o figura nella lista di allerta della FINMA (https://www.finma.ch/it/finma-public/lista-di-allerta/) o nell'IOSCO Investor Alerts Portal (https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal) . Se si tratta di offerenti svizzeri, controllate anche l'estratto del registro di commercio (www.zefix.ch (https://www.zefix.ch/it/search/entity/welcome)).
- Contattate il consulente alla clientela della vostra banca se avete qualche dubbio.