Lettere false di presunti istituti finanziari

Con una certa frequenza si trovano in circolazione lettere fraudolente dall'aspetto ingannevole che sembrano provenire dalla vostra banca. Ma le contraffazioni si possono smascherare.

Punti principali:

- Per svolgere operazioni di e-banking utilizzate sempre il sito Internet ufficiale o l'app per il Mobile Banking del vostro istituto finanziario.
- Verificate l'autenticità delle comunicazioni ricevute con la posta cartacea – come fate per quelle elettroniche – e segnalate eventuali lettere sospette al vostro istituto finanziario.
- Controllate l'indirizzo Internet dei codici QR letti con la fotocamera prima di seguire il link.

I truffatori fanno di tutto per dare alle lettere false l'apparenza più autentica possibile, usando anche loghi che sembrano corretti e layout professionali. Il loro scopo è ottenere informazioni sensibili o dati d'accesso di vittime che non sospettano nulla, ad esempio per entrare nel loro sistema di e-banking e arricchirsi illecitamente.

Lo scenario tipico è questo: un codice QR contenuto nella lettera apre un sito Internet contraffatto che assomiglia alla pagina di accesso del vostro portale di e-banking. Lì vi viene chiesto di inserire informazioni sensibili come i vostri dati di login. Se lo fate, i criminali ottengono l'accesso ai vostri conti.

La procedura corrisponde a quella del phishing (https://www.ebas.ch/it/phishing) classico, con la differenza che invece di un messaggio elettronico (tramite e-mail, SMS o servizio di messaggistica) viene inviato un documento cartaceo. Spesso si fa anche pressione sulla vittima, ad esempio indicando che il conto verrà bloccato se l'operazione – a loro dire necessaria – non sarà eseguita entro breve tempo.

Dal punto di vista del malintenzionato, l'uso di codici QR offre il vantaggio che la vittima non riconosce immediatamente quale indirizzo Internet è codificato nell'immagine a mosaico. Se così non fosse, la contraffazione sarebbe riconoscibile a prima vista.

La truffa può essere smascherata se, dopo aver letto il codice QR con la fotocamera, controllate l'indirizzo Internet visualizzato prima di aprire il sito corrispondente. O ancora meglio: digitando l'indirizzo Internet del vostro istituto finanziario sempre a mano, nella barra degli indirizzi del browser, oppure avviando l'app di Mobile Banking, che vi permette di accedere in tutta sicurezza al portale di e-banking originale della vostra banca.

I criminali falsificano comunicazioni scritte di aziende serie come gli istituti finanziari, con risultati che spesso sembrano davvero autentici. Si tratta di lettere che invitano la clientela a intraprendere azioni importanti per la sicurezza. È uno stratagemma usato dai truffatori per ottenere informazioni sensibili o le credenziali d'accesso delle vittime.