Lista di controllo
Il phishing

Come proteggere i propri dati personali

I messaggi e-mail dei truffatori che vogliono accedere ai propri dati personali (credenziali del conto, password, PIN) sembrano spesso autentici. Con un po' di cautela e sapendo a cosa prestare attenzione, si riescono però a individuare i messaggi di «phishing» di questi criminali.

1. Usate particolare prudenza con i messaggi e-mail che non aspettavate.
2. Nei messaggi di phishing vi viene richiesto di fornire informazioni riservate quali password, TAN, PIN, numeri cliente e codici di accesso relativi al proprio conto.
3. L'e-mail contiene spesso font diversi di dimensioni diverse.
4. L'e-mail presenta errori grammaticali e ortografici.
5. Gli accenti non sono scritti correttamente.
6. L'e-mail si rivolge al destinatario in modo impersonale (Gentile cliente della banca ABC).
7. La formula di saluto è impersonale (La Sua banca ABC).
8. Un messaggio di phishing non è indirizzato a voi personalmente, ma ad esempio a una casella di posta condivisa (clienti@istitutodicredito-abc.ch).
9. Il mittente vi minaccia (ad esempio di bloccare il conto).
10. L'e-mail ha in allegato un modulo o contiene un link a un modulo in cui dovreste inserire dei dati personali (PIN, TAN, numero del conto, numero cliente e codice di accesso).
11. L'e-mail contiene un link che a una prima occhiata sembra normale. Parti insolite o non corrette della URL rimandano però a un indirizzo Internet falso.

Prestare attenzione ai seguenti aspetti

Per accedere al sito del vostro istituto finanziario non utilizzate mai un link inviato per e-mail o che debba essere letto con un codice QR.

Inserite sempre manualmente l'indirizzo del sito del vostro istituto finanziario.

Non compilate mai moduli inviati per e-mail che richiedono le informazioni di accesso al conto.

Non fornite informazioni riservate al telefono.