

17.03.2023

È possibile che qualcuno entri nel mio conto dell'e-banking avendo il mio codice IBAN, l'indirizzo e una copia della carta d'identità? No, ma...

Per molti tipi di truffe, gli hacker cercano dati personali come nome, indirizzo e numero di telefono. A volte chiedono anche l'IBAN, oppure una copia del passaporto o della carta d'identità.

Visto che le procedure di sicurezza delle banche migliorano continuamente, i trasgressori ricorrono quasi sempre al «social engineering», ossia all'acquisizione di informazioni attraverso ricognizioni, inganni e manipolazione delle vittime. Ciò avviene anche sfruttando e-mail e siti Internet contraffatti.

Se si considerano gli account e-banking esistenti, i dati non servono per compiere la truffa ma solo per ottenere la fiducia delle vittime e sottolineare la presunta serietà di un'offerta – magari di un rimborso o di una distribuzione degli utili, per esempio. Con un codice IBAN e la copia di una carta d'identità non è possibile prelevare denaro da un conto. Però si può compiere un illecito sfruttando l'IBAN, ad esempio richiedendo un addebito diretto su quel conto in uno shop online. Per i truffatori, tuttavia, questa procedura non è redditizia, dato che i mandati di pagamento di questo tipo possono essere contestati e stornati alla banca anche per un anno.

Detto questo, se si considera che gli indirizzi e le copie di passaporti o carte d'identità raccolti potrebbero essere usati per aprire nuovi conti presso banche e istituti di credito stranieri, le cose cambiano un po'. Infatti, una richiesta presentata dai truffatori utilizzando l'indirizzo e un documento altrui viene elaborata e conclusa senza difficoltà. La banca registra i computer o i cellulari dei truffatori, quindi nemmeno il passaggio della doppia autenticazione rappresenta un ostacolo. Il malintenzionato può disporre in tutto e per tutto del conto – un conto intestato alla vittima. Conti aperti in questo modo vengono sfruttati per compiere atti criminali senza che entri in gioco il proprio nome ma quello della vittima, contro la quale saranno poi rivolte eventuali denunce. Ne può derivare una procedura complicatissima e interminabile per dimostrare che non è stata la vittima a commettere il reato, ma che si tratta piuttosto di una frode.

Come regola generale, bisogna agire con scetticismo e reticenza quando si comunicano i propri dati personali. Se si notano delle irregolarità, bisogna segnalarlo immediatamente alla banca e alla polizia.