23.10.2020

Recenti tentativi di frode via phishing

Dalla fine dell'estate, i messaggi di phishing via e-mail ed SMS hanno visto un nuovo aumento esponenziale. I tentativi di truffa si fanno sempre più sofisticati, ma non lasciatevi ingannare!

I criminali di Internet dimostrano non solo una forte comprensione della tecnologia, ma anche un'enorme inventiva. Se durante il periodo del confinamento erano ancora ampiamente diffusi i messaggi di phishing legati al coronavirus, da agosto i truffatori hanno inventato continuamente nuovi schemi per trarre in inganno gli utenti in buona fede: presunti blocchi di account e carte, consegne di pacchi trattenute, coupon vinti e rimborsi di servizi di telecomunicazione sono alcune delle trappole di phishing più popolari al momento.

I messaggi falsificati giungono agli utenti principalmente via e-mail o SMS – e diventano sempre più credibili. Gli hacker scrivono senza fare nessun errore linguistico. Spesso si rivolgono alla vittima con il suo indirizzo e-mail se non addirittura chiamandola per nome. Anche l'indirizzo del mittente è spesso falsificato, e il sito Internet di phishing collegato è non di rado dotato di HTTPS e un nome di dominio che i non esperti possono tranquillamente trovare credibile. In alcuni casi, invece di link i truffatori utilizzano anche allegati di posta elettronica dannosi per fuorviare anche i destinatari più esperti.

Occorre fare attenzione – senza però cadere nel panico. Bastano infatti alcune semplici regole di condotta per proteggersi da tutti questi tentativi di frode:

- 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.
- Non compilate mai i moduli ricevuti via e-mail che chiedono di inserire i dati d'accesso.
- Gestire 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.
- Quando aprite la pagina di accesso, verificate che la connessione sia SSL (https://, icona a forma di lucchetto) e assicuratevi di trovarvi sulla pagina desiderata controllando l'indirizzo Internet nella barra degli indirizzi del browser.
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario.

Ulteriori informazioni sono disponibili nel nostro articolo «Phishing (https://www.ebas.ch/phishing) ».