Telefonate fraudolente dall'assistenza

I criminali non si limitano a Internet per carpire informazioni riservate. Sempre più spesso viene usato anche il telefono – una pratica criminale nota come «vishing».

Proteggetevi così:

- Interrompete immediatamente le chiamate indesiderate di presunti collaboratori di Microsoft, altre società di assistenza informatica o istituti finanziari.
- Non date per scontato che il numero visualizzato sul display del telefono sia corretto.
- Non comunicate mai a un'altra persona dati personali come le password o i numeri delle carte di credito.
- Se avete domande da rivolgere all'assistenza, componete sempre i numeri di telefono ufficiali di Microsoft o delle società di assistenza informatica.
- Per contattare il vostro istituto finanziario utilizzate esclusivamente i numeri di telefono ufficiali, quelli riportati p. es. sugli estratti conto.

Il termine «vishing» sta a significare «Voice-Phishing». Come con il phishing tradizionale, la gente viene spinta per mezzo di circostanze dissimulate a rivelare informazioni riservate o installare presunti programmi di sicurezza, quando in realtà si tratta di software dannoso.

Spesso chi chiama afferma di lavorare per Microsoft, altre società di assistenza informatica o un istituto finanziario. Per esempio, è stata rilevata un'infezione da virus o è sorto qualche problema tecnico. L'intenzione dei truffatori è convincere l'altra persona o a scaricare qualche programma da Internet o a visitare una pagina Internet contraffatta ma che sembra autentica.

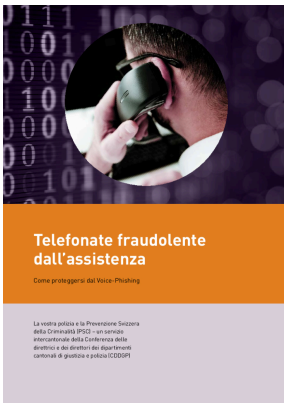
In entrambi questi modi, i criminali possono accedere direttamente al dispositivo della vittima e, per esempio, impadronirsi delle password ad insaputa dell'utente oppure visualizzare, copiare e modificare tutti i dati memorizzati nel computer. In alcuni casi, i truffatori addebitano persino delle commissioni per questa cosiddetta «prestazione di assistenza», da pagare indicando un numero di carta di credito, che naturalmente poi verrà sfruttata in modo improprio.

Spesso chi chiama parla un inglese grossolano. Visto che dal punto di vista tecnico i numeri di telefono possono essere manipolati, sul display del telefono della vittima potrebbe comparire anche il numero di telefono vero dell'azienda.

Se è già troppo tardi e avete già autorizzato chi vi ha chiamato ad accedere al vostro dispositivo, scollegatelo immediatamente da Internet o spegnetelo. Riaccendetelo solo dopo aver disattivato la connessione di rete (p. es. dopo aver spento il router Wi-Fi) ed effettuate immediatamente una scansione dell'intero disco rigido con un programma antivirus. Cambiate anche tutte le vostre password. Se ne sentite la necessità o avete dei dubbi, rivolgetevi a uno specialista. Se avete già fornito dati sensibili (p. es. i dati della carta di credito o altri dati bancari), contattate subito la società della vostra carta di credito e/o il vostro istituto finanziario, come pure la polizia locale.

*Microsoft, altre società di assistenza informatica o istituti finanziari non effettuano **mai** chiamate non richieste agli utenti privati per fornire supporto tecnico! Quando sorge un'esigenza di questo tipo, l'iniziativa deve provenire sempre dai clienti stessi.*

Promemoria:



(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_it.pdf)