PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5380 di Martedì 02 maggio 2023

Vishing: come proteggersi dal phishing telefonico?

Cos'è il vishing? Una scheda del Garante spiega perché può essere molto pericoloso e fornisce alcuni suggerimenti utili per imparare a riconoscerlo e a difendersi.

Il vishing (o phishing vocale) è una forma di truffa, sempre più diffusa, che utilizza il telefono come strumento per appropriarsi di dati personali - specie di natura bancaria o legati alle carte di credito - e sottrarre poi somme di denaro più o meno ingenti.

Una nuova scheda informativa del Garante privacy spiega perché può essere molto pericoloso e fornisce alcuni suggerimenti utili per imparare a riconoscerlo e a difendersi. Perché la consapevolezza è la prima linea di difesa dei nostri dati personali.

Di solito le vittime vengono contattate telefonicamente da finti operatori (di banche o di società che gestiscono bancomat o carte di credito) i quali, con la scusa di presunte "anomalie", chiedono alle persone, nel loro stesso interesse, di collaborare a mettere in campo necessarie (e false) "procedure di sicurezza".

Nel caso più frequente, i truffatori (i "visher") chiedono direttamente di **fornire i riferimenti del conto corrente o della carta di credito** (come il PIN del bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza sul retro della carta, i dati dell'OTP cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.).

È un metodo apparentemente banale, ma che purtroppo funziona, con una certa efficacia, specie con le persone anziane.

In altri casi - durante o dopo la finta telefonata di allarme - **viene inviato sul cellulare un messaggio con un codice di conferma e viene chiesto alla vittima di leggerlo ad alta voce all'operatore**. Tale codice serve in realtà ad autorizzare trasferimenti di denaro a vantaggio dei truffatori, entrati precedentemente in possesso dei dati bancari o della carta di credito (ad esempio, attraverso altre azioni di phishing o tramite altri cybercriminali).

Può anche capitare che il messaggio inviato dai visher contenga un **link per accedere ad un form** dove è richiesto di inserire

- i dati bancari o della carta di credito;

- oppure il presunto "codice di sicurezza" ricevuto dai truffatori (che, come detto, serve in realtà ad autorizzare versamenti a vantaggio dei visher).

Alle vittime può anche essere chiesto di **scaricare e installare app e programmi**, che ufficialmente dovrebbero servire per proteggere conti e carte di credito, ma che in realtà possono operare come trojan (cioè **programmi malevoli**) utili a carpire dati personali o addirittura capaci di accedere alle app e ai programmi con cui si gestiscono internet banking e carte di credito. Spesso i truffatori chiedono alle loro vittime di inserire nella app malevola dati bancari o della carta di credito, per poi appropriarsene.

I truffatori operano anche tramite **messaggi** (inviati sullo smartphone o via e-mail, o lasciati in segreteria telefonica) **per spingere le vittime a richiamare urgentemente determinati numeri**, contattati i quali si parla con un operatore o si ascolta un messaggio registrato: in entrambi i casi, la vittima è invitata a fornire, per la propria sicurezza e in modo urgente, informazioni di vario tipo, compresi dati bancari e/o della carta di credito.

PERCHÉ IL VISHING È COSÌ PERICOLOSO?

I visher fanno leva sul timore legato ad un rischio incombente per convincere le vittime ad abbassare il livello di prudenza e a reagire d'impulso. Una particolare forma di **ingegneria sociale** che dimostra una elevata efficacia.

Il danno purtroppo può essere a volte anche molto ingente, perché prima che la vittima si accorga delle sottrazioni di denaro può passare del tempo, durante il quale i truffatori sono in grado di effettuare numerosi prelievi e transazioni, oppure possono rivendere i dati ad altri cyber criminali.

Non sempre i visher si fingono operatori di banche o carte di credito. Ecco alcune varianti del vishing:

? un **finto** impiegato del servizio clienti di una società (di solito di software) che chiama per segnalare un problema (di sicurezza, di presunto uso non regolare del software, ecc.);

? un **finto** impiegato di una società che comunica che la vittima potrà ricevere un premio o ha diritto a particolari sconti o agevolazioni, a patto di fornire i dati del conto bancario e altre informazioni;

? un **finto** ufficio pubblico contatta la vittima per imposte o multe da pagare con urgenza pena l'applicazione di ingenti sanzioni, convincendola a fornire informazioni di vario tipo.

COME DIFENDERSI DAL VISHING?

Ci sono alcuni indizi che ci aiutano a sospettare che una chiamata nasconda un possibile tentativo di vishing.

Ad esempio:

? istituzioni e aziende chiamano di solito da numeri fissi e comunque con prefissi nazionali: chiamate provenienti, ad esempio, da **numeri anonimi, da numeri di cellulare o da prefissi stranieri** possono essere considerate anomale e dovrebbero renderci prudenti (anche se il ricevere la chiamata da un numero apparentemente "ordinario" non è ovviamente garanzia di sicurezza);

? meglio **diffidare delle chiamate con toni ultimativi o intimidatori,** che ad esempio minacciano la chiusura del conto bancario, il blocco della carta di credito o eventuali sanzioni se non si compie subito una certa azione: possono essere subdole strategie per spingere il destinatario a fornire informazioni e dati personali senza rifletterci troppo. Gli operatori telefonici hanno normalmente un atteggiamento cortese nei confronti dei clienti: sono quindi da considerare sospette le chiamate di operatori che si rivolgono a noi con toni poco educati o troppo confidenziali, non consoni all'azienda o all'istituzione che dovrebbero rappresentare.

Dati e informazioni personali, codici di accesso, PIN password, dati bancari e della carta di credito non dovrebbero mai essere comunicati a sconosciuti. È importante tenere presente che amministrazioni pubbliche, banche e aziende fornitrici di carte di credito:

? conoscono già determinate informazioni (numero di conto o numero della carta, ecc.);

? non ci dovrebbero chiedere quelle informazioni che, di solito, esse stesse ci invitano a mantenere riservate (PIN, password, codici di autorizzazione, ecc.).

Se si ricevono mail o messaggi (anche in segreteria telefonica) che chiedono di richiamare determinati numeri di aziende o istituzioni, **controllare SEMPRE prima se tali numeri corrispondono a quelli ufficiali** (ad esempio consultando i siti web ufficiali). Per estrema sicurezza, invece di chiamare i numeri indicati nel messaggio, ci si può rivolgere al centralino o all'URP dell'azienda o dell'istituzione per farsi mettere in contatto con l'ufficio che dovrebbe aver inviato il messaggio.

Altra buona cautela è quella di **evitare di richiamare numeri sconosciuti**, soprattutto nel caso di telefonate mute con caduta immediata della linea e se la numerazione ci appare anomala.

Per proteggere conti bancari e carte di credito è bene **controllare spesso le movimentazioni** e attivare sistemi di alert automatico che avvisano l'utente di ogni operazione effettuata.

Se si ha il dubbio di essere stati (e in generale di phishing) riguardo dati bancari e/o della carta di credito, è consigliabile contattare immediatamente la banca o il gestore della carta di credito attraverso canali di comunicazione conosciuti e affidabili per segnalare l'accaduto e, in caso di sottrazione di denaro, richiedere il blocco delle transazioni. In questa seconda ipotesi, si può anche segnalare la truffa subita alle autorità di polizia.

VADEMECUM

I suggerimenti del Garante per proteggersi dal phishing (pdf)

La scheda ha mere finalità divulgative e sarà aggiornata in base alle evoluzioni tecnologiche e normative

Per saperne di più sul phishing, segui anche la campagna informativa del Garante " Finalmente un po' di privacy"

Vishing: come proteggersi dal phishing telefonico?

GUARDA IL VIDEO - Versione Televisiva da 30'' - Versione web da 60''

ASCOLTA LA VERSIONE RADIOFONICA

Fonte: Garante Privacy

---

www.puntosicuro.it