Cybersecurity II - Andare a pesca di dati: il phishing

di **Emil Dari**
10/09/2025

CYBERSECURITY PHISHING PRIMO BIENNIO

Il **phishing** è una delle **truffe informatiche** più **diffuse** e si presenta in forme diverse: via telefono (vishing), SMS (smishing) o e-mail (spray e spear phishing). L'obiettivo è indurre l'utente a fornire **dati riservati**, spesso attraverso messaggi che imitano banche, corrieri o enti pubblici. Anche se molti tentativi vengono riconosciuti e ignorati, basta un attimo di distrazione per cadere nella trappola.

Campagne recenti hanno sfruttato loghi di istituzioni e aziende note, da Poste Italiane a Trenitalia. Difendersi richiede attenzione al mittente, ai link sospetti e alla consapevolezza che, se un messaggio sembra troppo bello per essere vero, probabilmente non lo è.

Tutti siamo incappati almeno una volta in un SMS di *smisching*, una e-mail di *spray phishing* o una chiamata telefonica di *vishing*. Sono tutte sottodenominazioni del ***phishing***, ovvero la pesca a strascico dei dati dell'utente incauto. Vediamo quali tipologie esistono di questo tipico attacco informatico, che spesso è il primo passo di offensive ben più strutturate e pericolose.

Le diverse tipologie di phishing

Il phishing prende il nome dal termine inglese che significa *pesca* e si suddivide in varie categorie, esiste quello **telefonico** (voice phishing o vishing), quello **via SMS** (smishing), quello mirato a un certo **target specifico** (spear phishing) ma il più diffuso resta lo spray phishing via **posta elettronica**, ovvero quello che più di tutti assomiglia alla pesca a strascico: vengono gettate le reti su un'area più ampia possibile e si cerca di catturare tutto il catturabile, ovvero, per rispettare l'analogia, vengono inviate decine di migliaia di e-mail malevole e **si conta sul fatto che sui grandi numeri qualcuno abbocchi**.

Cos'è il phishing

Sul sito della Polizia Postale il phishing viene definito come "una particolare tipologia di **truffa realizzata sulla rete Internet attraverso l'inganno degli utenti**" e che "si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli". In pratica gli attaccanti generano delle **e-mail falsificate** in modo da risultare simili a quelle che un utente potrebbe ricevere dalla propria banca, da un sito di e-commerce, da un corriere o anche da un sito istituzionale, per spingere l'utente a fidarsi e cliccare su un link o scaricare un allegato.

I link generalmente portano l'utente su un **sito malevolo simile al sito web originale** del servizio a cui l'utente crede di accedere; su questo sito l'utente viene spinto da tecniche di ingegneria sociale a inserire dei dati riservati o rilevanti per gli attaccanti, nel caso peggiore le proprie password o i propri codici bancari.

Alcuni esempi

Tutti abbiamo almeno una volta avuto a che fare con il phishing, nella periodica pulizia delle e-mail di spam o in quel messaggio Whatsapp di uno sconosciuto a cui non abbiamo risposto o in quel SMS che abbiamo ignorato e che ci diceva che il corriere tal dei tali non è stato in grado di consegnare il nostro pacco, solo che noi non avevamo ordinato nulla e non ci aspettavamo l'arrivo di nessun corriere.

Magari nella maggior parte dei casi questi tentativi di attacco sono stati innocui, li abbiamo ignorati perché abbiamo fatto attenzione o magari semplicemente perché non eravamo il target giusto. Ed è questo il punto: facendo moltissimi tentativi

prima o poi il messaggio malevolo raggiunge quel tale che sta aspettando un'e-mail dalla banca o che sta aspettando un pacco proprio da quel corriere ed è sufficiente un momento di disattenzione per rimanere intrappolati.

Approfondimenti

Se non abbiamo in mente nessun messaggio ricevuto che possa apparire sospetto, vediamo alcuni esempi direttamente sul sito del CSIRT Italia, una branca dell'Agenzia per la cybersicurezza nazionale (ACN) che si occupa di incidenti informatici. Le seguenti sono solo alcune delle campagne di phishing segnalate dal CSIRT da gennaio a marzo 2024:

- **Campagna phishing a tema "verifica account" che imita una mail di Roma Capitale**
- **Campagna phishing a tema "liquidazione fatture" che esorta a visualizzare un pdf**
- **Campagna phishing a tema "Sondaggio Trenitalia" che sfrutta il logo dell'azienda**
- **Campagna di smishing legata al mancato recapito di corrispondenza di Poste Italiane**

Come difendersi

Difendersi non è semplice ma ci sono alcune tecniche e alcuni fattori a cui prestare attenzione per non essere sviati: il primo è il **mittente del messaggio**, è utile verificare che sia il dominio email del mittente che la firma del messaggio non siano [illegible] te o contengano errori; il secondo è l'**URL del sito** a cui il link ci porta: occorre verificarlo spostando il mouse sul link senza cliccare; sono sospetti URL che non rimandano a un sito che inizia per "https://", che non fanno riferimento al servizio citato nel messaggio o che contengono errori ortografici.

In ultimo, la consapevolezza dell'esistenza e della pervasività di questo fenomeno ci permette di esercitare la giusta attenzione: se per esempio avvertiamo che un messaggio punta a metterci fretta o pressione psicologica, probabilmente non è un messaggio legittimo, o se un messaggio sembra troppo bello per essere vero, probabilmente è perché non lo è!