Scenario di Phishing: "Fiamme di Speranza"

Contesto:

Nell'estate del 2024, una serie di incendi boschivi devastanti ha colpito diverse aree, causando danni significativi sia agli habitat naturali sia alle comunità locali.

In risposta a questa tragedia, viene lanciata una campagna di raccolta fondi da un'organizzazione fittizia chiamata **"Fiamme di Speranza"**, che sfrutta l'urgenza e l'emotività della situazione per attuare un tentativo di phishing. La campagna, apparentemente benefica, è finalizzata a sottrarre informazioni personali e bancarie delle vittime attraverso l'uso di email fraudolente.

Obiettivo del Phishing:

L'obiettivo principale dell'operazione è raccogliere dati personali e informazioni bancarie degli utenti, indotti a fornire queste informazioni attraverso una finta donazione online. Viene utilizzato il pretesto di acquistare un amigurumi (un piccolo pupazzo fatto a mano) raffigurante uno scoiattolo, simbolo della resilienza della fauna colpita dagli incendi, come incentivo per le donazioni.

Descrizione dello Scenario:

L'organizzazione fittizia "Fiamme di Speranza" invia un'email ben strutturata e convincente con l'oggetto: **"Adotta uno Scoiattolo di Speranza e Aiuta le Vittime degli Incendi!"**. L'email contiene un messaggio toccante che descrive le conseguenze degli incendi e fa appello alla sensibilità del destinatario, proponendo di effettuare una donazione per sostenere le operazioni di salvataggio e la ricostruzione.

Nel testo dell'email, viene presentata la possibilità di fare una donazione minima per ricevere un amigurumi come simbolo di sostegno alla causa. L'email include immagini accattivanti, un linguaggio emotivo e riferimenti a partner fittizi come il WWF per aumentare la percezione di credibilità. Tuttavia, il link contenuto nell'email reindirizza l'utente a un sito fraudolento creato per raccogliere informazioni sensibili quali dati personali e bancari.

Elementi che avvalorano la credibilità

Uso di un tema emotivo e nobile

- **Causa sociale**: L'email fa leva su una causa emotiva molto potente, ovvero aiutare gli animali e le persone colpite dagli incendi. Temi come la protezione degli animali o il sostegno a vittime di disastri naturali sono altamente convincenti perché risvegliano la sensibilità del destinatario.

Aspetto tecnico dell'email

- **Autenticazione SPF, DKIM e DMARC**: I protocolli di sicurezza sono tutti positivi. Questo fa sembrare che l'email sia autentica dal punto di vista tecnico, perché non è stata alterata e proviene da un server di posta autorizzato. Questo aspetto potrebbe indurre un destinatario meno esperto a fidarsi.

Provenienza da ProtonMail

- **Servizio email sicuro**: ProtonMail è noto per la sua sicurezza e crittografia. Il fatto che l'email provenga da un indirizzo ProtonMail potrebbe dare l'idea che sia un'email sicura e protetta, quando in realtà chiunque può usare ProtonMail, anche per scopi fraudolenti. Molte persone associano ProtonMail a legittimità e riservatezza, aumentando la fiducia.

Richiamo al WWF

- **Organizzazione riconosciuta**: L'email sembra provenire dal WWF, un'organizzazione ambientalista internazionale molto conosciuta e rispettata.

Elementi che dovrebbero allarmare il destinatario

Per analizzare nel dettaglio gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità eseguiamo un’analisi approfondita del suo sorgente.

1. Indirizzo del mittente e autenticazione

- **Mittente**: fiammedisperanza@proton.me
- **Dominio**: ProtonMail è un servizio di posta elettronica crittografato noto per la sua sicurezza e privacy. Anche se legittimo, è importante notare che può essere utilizzato da chiunque, anche da persone con cattive intenzioni, proprio a causa della sua riservatezza.
- **Autenticazione**:
    - **SPF** (Sender Policy Framework): Passato, il dominio proton.me è stato confermato come un dominio autorizzato a inviare email.
    - **DKIM** (DomainKeys Identified Mail): Firmato correttamente, il che significa che l'email non è stata alterata durante il trasferimento.
    - **DMARC** (Domain-based Message Authentication, Reporting & Conformance): Passato, che assicura che il dominio mittente non sia stato contraffatto.

Questi protocolli indicano che l'email è probabilmente autentica dal punto di vista tecnico, ma questo non garantisce la legittimità del contenuto.

2. Oggetto e Contenuto

- **Oggetto**: "Aiuta gli animali e le persone colpite dagli incendi - Adotta uno Scoiattolo di Speranza!"
    - L'oggetto fa leva su una causa emotiva, il che è un tipico schema utilizzato in email di phishing o truffe, che mirano a sfruttare la generosità delle persone.
- **Contenuto**:
    - Il messaggio è scritto in uno stile emotivo, chiedendo donazioni per aiutare animali e persone colpite dagli incendi, con un focus su una campagna specifica per "adottare uno scoiattolo di speranza". Tuttavia, il messaggio è relativamente vago riguardo ai dettagli specifici dell'iniziativa e sembra puntare a convincere emotivamente il destinatario a fare una donazione senza fornire informazioni chiare e verificabili.
    - Viene inoltre fornito un link, che potrebbe essere potenzialmente pericoloso se non verificato attentamente. Viene anche suggerito di visitare un sito, presumibilmente per fare una donazione, ma è fondamentale evitare di cliccare su link non verificati.

3. Formato e struttura

- L'email è formattata in **MIME** con contenuti sia in **plain text** che in **HTML**, il che è normale per le email, ma viene incluso anche un file immagine (immagine.png), che potrebbe essere un tentativo di rendere l'email più accattivante o nascondere altre finalità. Bisogna essere cauti con file di immagine inclusi in email da fonti sconosciute.

4. Elementi sospetti

- **Indirizzo mittente**: Anche se il dominio ProtonMail è stato autenticato, è difficile verificare la vera identità del mittente. Le organizzazioni affidabili spesso usano domini dedicati che corrispondono al loro brand (es. @wwf.org per WWF), invece di servizi di posta generici.
- **Chiamata all'azione**: La richiesta di una donazione attraverso un link, senza troppe informazioni o trasparenza, è un tipico segnale d'allarme nelle truffe di beneficenza. Le email di questo tipo dovrebbero fornire una chiara documentazione dell'organizzazione, come dettagli sulla missione, modalità di contatto e trasparenza finanziaria.
- **Immagini** e **contenuti HTML**: L'uso di immagini potrebbe essere una tecnica per rendere l'email più coinvolgente, ma talvolta può anche essere un veicolo per contenere tracking pixel o link fraudolenti nascosti.

- **Dall'analisi del testo dell'email, si notano alcuni errori e imperfezioni grammaticali e stilistiche che possono destare sospetti, soprattutto in una comunicazione che si presenta come proveniente da un'organizzazione di rilievo come il WWF**