PROGETTO SETTIMANALE S5 BONUS 1

TRACCIA: Creare una mail di phishing irriconoscibile.

In questo esercizio, ci occuperemo della creazione di una e-mail di phishing, in questo caso però la mail deve essere irriconoscibile e quindi non deve contenere elementi che possano far scattare nell'utente campanelli d'allarme.

Scenario

Contesto: Un'azienda di software invia una comunicazione ai propri clienti riguardo una "verifica annuale" obbligatoria per garantire il corretto funzionamento del prodotto acquistato. L'email include un link che sembra portare al sito ufficiale, ma in realtà è un sito fraudolento progettato per rubare le credenziali di accesso dell'utente.

Obiettivo del phishing: Ottenere le credenziali di accesso a un sistema software, che potrebbero essere utilizzate per accedere a dati sensibili o a sistemi aziendali.

MAIL DI PHISHING IRRICONOSCIBILE:

Oggetto: Verifica della tua licenza software - Azione necessaria

---

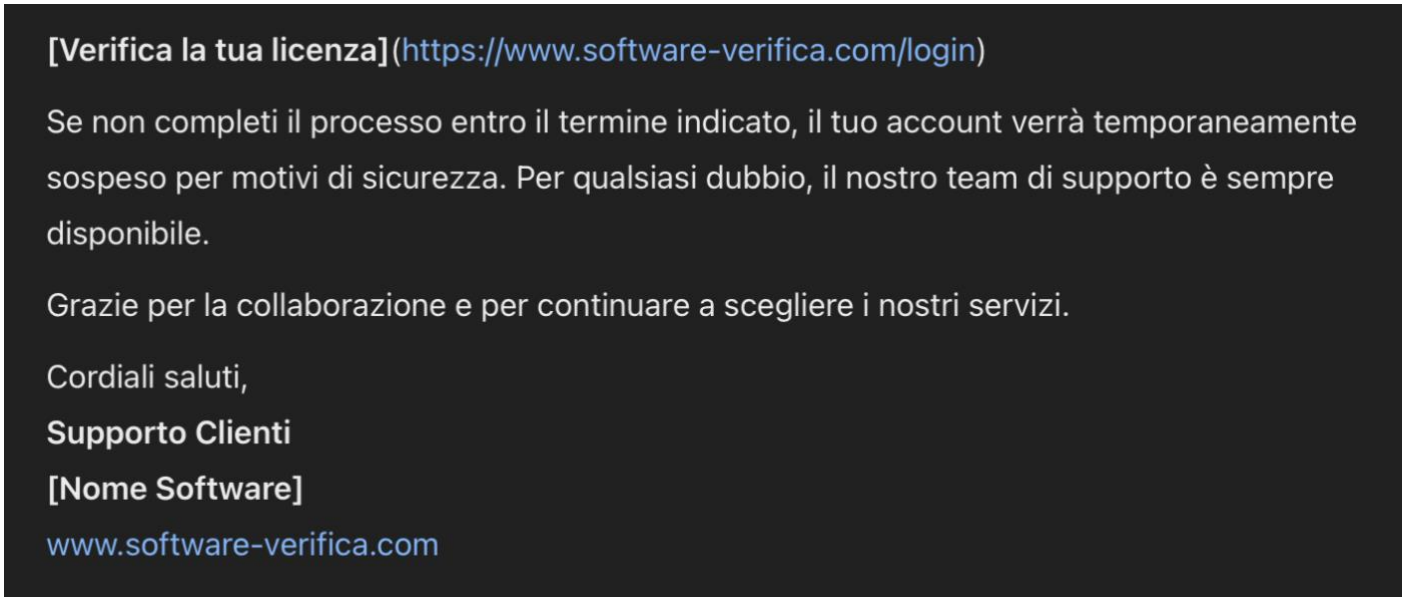
Caro [Nome del cliente],

Ti scriviamo per informarti che, come parte della nostra politica di sicurezza, tutti i nostri utenti devono completare una **verifica annuale** della licenza del prodotto. Questo processo aiuta a garantire che tu stia utilizzando la versione più recente del nostro software, riducendo il rischio di vulnerabilità.

Abbiamo rilevato che la tua licenza è stata selezionata per questa verifica. Per procedere con l'aggiornamento, ti chiediamo gentilmente di completare il controllo delle informazioni del tuo account. Ti invitiamo a farlo entro **48 ore** per evitare l'interruzione dei tuoi servizi.

Passaggi per completare la verifica:

1. Accedi al tuo account tramite il link sottostante.
2. Conferma i tuoi dati di registrazione e aggiorna le informazioni mancanti.
3. Una volta completata la verifica, riceverai una conferma via email.



Spiegazione dello Scenario

Credibilità dell’e-mail:

L'email è progettata per sembrare provenire da una comunicazione ufficiale di un'azienda di software che il cliente potrebbe già utilizzare. Il tono è formale, professionale e non contiene errori evidenti. La richiesta di aggiornare la licenza sembra legittima, soprattutto considerando che molte aziende richiedono aggiornamenti annuali per motivi di sicurezza.

Elementi di phishing:

Link sospetto: Il link "Verifica la tua licenza" sembra portare a un sito ufficiale, ma in realtà è un dominio ingannevole simile a quello originale (ad esempio, software-verifica.com anziché software ufficiale.com). Un clic sul link porta a una pagina che replica perfettamente il sito legittimo.

Pressione: La minaccia di sospensione dell'account in caso di mancata azione entro 48 ore crea un senso di urgenza, spingendo l'utente ad agire senza riflettere.

Richiesta di informazioni personali: Anche se l'e-mail non chiede esplicitamente informazioni sensibili nell'email stessa, il link porta a una pagina dove vengono richieste credenziali di accesso o altre informazioni, come il numero di carta di credito o i dettagli del profilo.

Perché l'email potrebbe sembrare credibile:

E-mail professionale: Il linguaggio e la formattazione dell'e-mail sono impeccabili, il link sembra autentico. Le aziende di software spesso inviano comunicazioni simili riguardo la verifica delle licenze o gli aggiornamenti annuali.

Tono e linguaggio chiari: L'e-mail è diretta e chiara, con una comunicazione molto simile a quelle legittime di aziende di software che informano i clienti riguardo aggiornamenti o controlli periodici.

Senso di urgenza e scadenza: La scadenza di 48 ore è un elemento classico del phishing, che mira a spingere l'utente ad agire rapidamente senza prendere il tempo per verificare la legittimità dell'e-mail.

Elementi che dovrebbero far scattare un campanello d'allarme:

Verifica del dominio: Anche se il link appare credibile a una prima occhiata, è importante controllare attentamente l'URL. Un dominio simile ma non identico a quello originale è sempre un segnale di allarme.

Richiesta di azione immediata: Le vere aziende di software non inviano e-mail con minacce di sospensione immediata o con una scadenza così ravvicinata, soprattutto senza fornire informazioni più dettagliate sui motivi per cui è necessaria la verifica.

Controllo delle informazioni richieste: Le aziende legittime di solito non chiedono credenziali sensibili via e-mail, né chiedono di accedere a un link per aggiornare informazioni di pagamento o di profilo. È sempre meglio andare direttamente al sito ufficiale tramite il browser e accedere tramite il portale di login ufficiale.

Errori sottili: Un controllo approfondito potrebbe rilevare errori sottili, come l'assenza di una lettera nel nome dell'azienda nel dominio, o l'uso di un nome generico come "Supporto Clienti" senza altre informazioni di contatto (telefono o indirizzo fisico).

Conclusione:

Questo esempio di phishing sembra praticamente indistinguibile da una comunicazione legittima. Ma, prestando attenzione ai dettagli, come il dominio del link e l'assenza di informazioni aggiuntive di contatto, un utente attento potrebbe scoprire che si tratta di un tentativo di truffa. La consapevolezza e la prudenza sono fondamentali per evitare di cadere in queste trappole.