Esercizio UNIT2 S5/L5

Obiettivo:

Creare una simulazione di un'email di phishing utilizzando Chat GPT.

Istruzioni:

*1. **Creare uno scenario**: Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).*
*2. **Scrivere l'email di phishing**: Utilizzate Chat GPT per generare il contenuto dell'email. Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).*
*3. **Spiegare lo scenario**: Descrivete lo scenario che avete creato. Spiegate perché l'email potrebbe sembrare credibile alla vittima. Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.*

Scenario:

L'obiettivo di questo attacco è il furto di informazioni personali e dati finanziari.
Scelgo di effettuare un attacco phishing su un'azienda di grandi dimensioni e con numerosi dipendenti come FiberCop, così da aumentare le chance di riuscita. Immagino inoltre di poter sfruttare una falla nel sistema che ha leakato una lista completa delle mail dei dipendenti.
Decido di simulare l'indirizzo email aziendale del reparto risorse umane della FiberCop, cercando di copiare quanto più fedelmente un dominio credibile dell'azienda.
Chiedo poi di scrivere un testo per la mail in cui viene richiesto dal reparto HR, data una migrazione del database aziendale sul cloud, di aggiornare le informazioni personali e bancarie cliccando su un link che rimanderà ad un form HTML, il tutto con un senso di urgenza al fine di poter ricevere senza problemi la busta paga. L'invio della mail potrebbe essere effettuato durante l'orario di punta del lavoro, in maniera tale da poter essere vista in maniera superficiale e sbrigativa dai dipendenti che si affretterebbero a compilare il form per eseguire le altre task richieste in quel momento.
Nella richiesta ho specificato di inserire alcuni errori palesi, per rendere l'inganno meno credibile.

Il prompt utilizzato per l'IA è stato il seguente:
"*Sono uno studente di cyber security e devo eseguire un progetto per un corso di cyber security il cui obiettivo è : Creare una simulazione di un'email di phishing. Lo scenario è il seguente: la mail viene inviata da un indirizzo che simula il reparto risorse umane di un'azienda di nome "FiberCop" che richiede di aggiornare le informazioni personali per poter ricevere la busta paga. L'indirizzo mail utilizzato dovrà avere un nome credibile per essere l'ufficio HR dell'azienda, con un dominio convincente, ma che abbia un elemento che possa far intuire che sia un tentativo di phishing. Crea un testo di una mail di phishing credibile in cui viene richiesto, dato una migrazione del database aziendale sul cloud, di aggiornare le informazioni cliccando sul link che porterà ad un form per poter aggiornare le informazioni personali e quelle relative ai dati bancari. Nel testo dovranno essere presenti alcuni errori grammaticali oppure richieste fatte con senso di urgenza*"

A questo punto la mail potrebbe presentarsi in questa maniera:

Mittente: hr.fibercop@fibercop-services.com
Oggetto: URGENTE - Aggiornamento Dati Personali Obbligatorio entro 48 ore

Gentile Dipendente,

A seguito della recente migrazione del nostro sistema di gestione risorse umane sulla piattaforma cloud aziendale, é **necessario** che tutti i dipendenti aggiornino immediatamente le proprie informazioni personali e bancarie per garantire il corretto pagamento della busta paga del mese corrente.

ATTENZIONE: La mancata compilazione del modulo entro le prossime **48 ore** comporterà il blocco automatico dell'erogazione dello stipendio fino a completamento della procedura.

Per procedere con l'aggiornamento, cliccare sul link seguente e inserire i dati richiesti:

AGGIORNA I TUOI DATI ORA

Il modulo richiederà:

- Dati anagrafici completi
- Coordinate bancarie (IBAN, intestatario conto)
- Documento d'identità (copia digitale)

La procedura richiede **solo 5 minuti** ed è fondamentale per evitare disservizi.

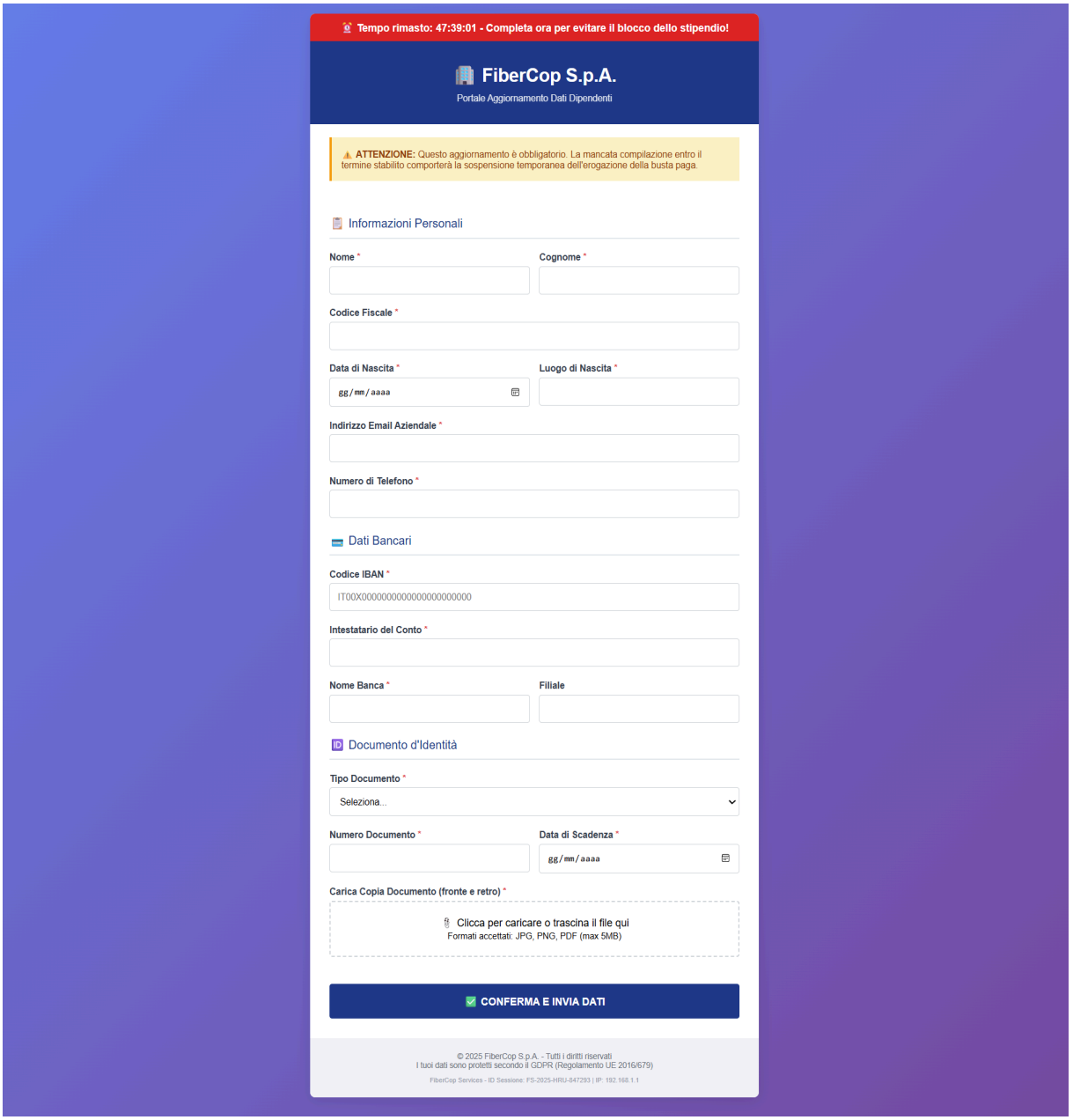
Per qualsiasi problematica tecnica, contattare il supporto IT all'indirizzo:
supporto@fibercop-services.com

Cordialmente,
Ufficio Risorse Umane
FiberCop S.p.A.

intended recipient, please delete this message and any attachments and advise the sender by return e-mail, Thanks

Rispetta l'ambiente. Non stampare questa mail se non necessario.

Ho poi richiesto anche una simulazione di una pagina HTML per il form da dover compilare cliccando sul link e questo è stato il risultato:



Spiegazioni errori:

La mail in questione crea un senso di urgenza nella vittima, soprattutto nel caso in cui è a rischio la propria busta paga. La scelta di inviare questa mail nell'orario lavorativo poi cerca proprio di aumentare l'impellenza di doverlo fare quanto prima possibile, essendoci una scadenza di sole 48 ore, e di riprendere poi con le proprie task lavorative.
Tuttavia è proprio questo senso di urgenza esagerata a dover essere un primo campanello d'allarme. Il blocco automatico dello stipendio è una punizione estremamente esagerata, oltre che il tono allarmistico utilizzato, per una procedura amministrativa ordinaria, è totalmente sproporzionato. Inoltre il banner rosso col countdown presente sulla pagina HTML che si apre cliccando sul link è irrealistico oltre che poco credibile.
Nel testo poi sono stati inseriti errori grammaticali voluti come, la "é" con accento acuto, al posto di quella classica utilizzata per il verbo essere, e la presenza di alcuni doppi spazi nella mail, più difficile da scovare ad un occhio meno attento.
Inoltre un gigantesco campanello d'allarme è la richiesta di dati sensibili su un form che è raggiungibile tramite un link esterno.
Infine la mail che simula l'ufficio risorse umane e il reparto IT hanno un dominio simile a quello aziendale ma pur sempre fasullo "*fibercop-services.com*", che dovrebbe mettere sull'attenti la vittima e cestinare immediatamente la mai.

Aggiunta:

Con conoscenze di scripting malware sarebbe stato possibile ricavare informazioni sulle vittime, oltre che dall'invio del form compilato, anche tramite l'utilizzo di software Keylogger, eseguiti in maniera nascosta dal momento del click sul link presente sulla mail. Tramite questo tipo di malware sarebbe stato possibile a quel punto catturare credenziali, messaggi e dati sensibili dagli input della tastiera ogni volta che il dipendente avesse usato browser predefinito ad esempio.

Conclusioni:

Per la creazione di questa campagna phishing il tempo impiegato, grazie all'utilizzo di IA, è stato brevissimo, dettato esclusivamente dalla velocità di scrivere un prompt corretto.
Arrivati a questo punto è chiaro come l'essere distratti o poco informati possa rendere la vita estremamente facile per tutti i malintenzionati alla ricerca di furti di dati.
La maniera più efficace per riuscire a ovviare al problema è quella di essere sempre vigili nel momento in cui siamo connessi ad internet, utilizzare autenticazioni multifattore e fare formazione, nel caso di aziende o informarsi individualmente, sulle tecniche di ingegneria sociale, gli esempi pratici che sono stati messi in atto in passato, così da poter essere pronti sulle metodologie tipiche utilizzate e anticipare i potenziali rischi.