venerdì 10 gennaio 2025

PROGETTO S5/L5

L’obiettivo dell’esercizio di oggi è creare un’email di phishing utilizzando ChatGPT.

1. ***CREAZIONE DELLO SCENARIO***

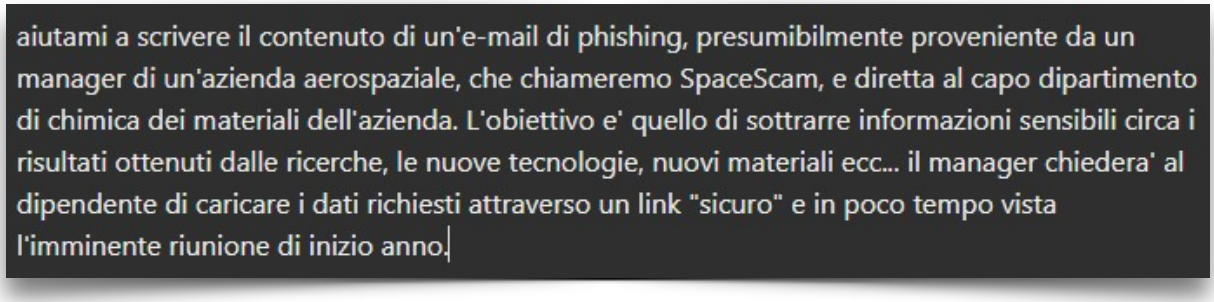
- Ho immaginato uno scenario nel quale il manager di un’azienda operante nell’ambito aerospaziale richiede delle informazioni molto importanti ad un dipendente, in particolare il capo dipartimento di chimica dei materiali, il quale è in possesso di tutti i dati e lo storico delle ricerche effettuate.

- Sono senz’altro informazioni molto sensibili che se sottratte possono creare un grande vantaggio nella “corsa allo spazio” da parte di un paese rispetto ad un altro.

- L’obiettivo è quindi quello di sottrarre lo storico delle ricerche, delle tecnologie, dei nuovi materiali ecc…

2. ***CREAZIONE DELLO SCENARIO***

- Per creare il contenuto dell’e-mail ho usato Chat-Gpt dando le seguenti istruzioni:



- Una volta generato il contenuto ho aggiunto giusto qualche piccolo errore grammaticale che potesse aiutare a riconoscere l'e-mail come sospetta, questo il risultato finale:

Oggetto: Urgente - Dati Ricerca Chimica dei Materiali 2024

Mittente: j.howard@spacescam-dept.com

Corpo dell'e-mail:

Gentile Lucas,

Spero tutto bene. Ti scrivo per richiedere la tua assistenza in merito alla revisione dei risultati delle ricerche del **Dipartimento di Chimica dei Materiali** svolte in 2024**.** Questo materiale è fondamentale per la nostra **riunione di inizio anno con i partner**, prevista per la prossima settimana.

Ti preghiamo di caricare i seguenti dati tramite il nostro portale sicuro **entro oggi**:
1. **Risultati delle ricerche principal**i condotte nel 2024.
2. **Descrizione dei nuovi materiali sviluppati**, incluse le loro proprietà chimiche.
3. Eventuali **rapporti tecnici** o dati sperimentali di rilievo.

Puoi caricare i dati al seguente link sicuro:
Carica Dati Ricerca 2024

Ti ringrazio per la tua tempestivita. Questo messaggio è cruciale per finalizzare i documenti che verranno presentati durante la riunione.

Grazie per la tua collaborazione. Se hai domande, non esitare a contattarmi.

Cordiali saluti,
James Howard
Manager Operativo - SpaceScam Inc.

3. ***SPIEGAZIONE***

- *Perché potrebbe sembrare credibile?*

1. **Contesto realistico**: Viene menzionata una situazione plausibile e concreta, una riunione con i partner ad inizio anno per discutere di quanto fatto nel 2024 in previsione del 2025.

2. **Tono professionale**: Il tono usato è professionale, tipico delle dinamiche interne di grandi aziende.

3. **Richiesta allineata con il ruolo della vittima**: La richiesta è pertinente alle responsabilità e competenze della vittima.

4. **Urgenza giustificata**: L'imminenza di una riunione così importante giustifica l'urgenza della richiesta e spinge la vittima ad agire senza pensare troppo.

5. **Autorità**: Il fatto che l'e-mail provenga da una figura superiore e molto importante nell'azienda fa leva sulla gerarchia aziendale.

6. **Responsabilità**: La comunicazione dell'imminente riunione spinge la vittima ad agire velocemente per evitare di essere causa di ritardi.
7.

- *Quali sono invece i campanelli d'allarme?*

1. **Dominio sospetto**: L'indirizzo del mittente utilizza il dominio "@spacescam-dept.com" invece del dominio ufficiale dell'azienda "spacescam.com".

2. **Urgenza eccessiva**: La richiesta di fornire dati così sensibili entro poco tempo potrebbe insospettire la vittima, nelle grandi aziende non è usuale richiedere informazioni tanto sensibili senza il minimo preavviso.

3. **Link sospetto**: Il link non mostra un dominio chiaro e riconoscibile, l'uso di link abbreviati e anonimi dovrebbe immediatamente destare sospetti.

4. **Errori grammaticali**: Sono presenti errori grammaticali basilari che possono insospettire la vittima e far pensare che siano frutto di una traduzione sbagliata (es. svolte in 2024, tempestivita). È inoltre abbastanza strano che un manager di un'azienda dimentichi l'utilizzo degli accenti o sbagli la formulazione di frasi semplici.

5. **Firma incompleta**: Mancano dei dettagli verificabili, come l'indirizzo fisico aziendale o numero di pratica.

6. **Caricamento insolito**: Nelle grandi aziende le informazioni vengono caricate su piattaforme conosciute o canali sicuri predefiniti e non tramite link generici inviati via e-mail.

ESERCIZIO BONUS 1

Nel primo esercizio bonus ho modificato l'e-mail vita sopra per rendere quanto più difficile possibile il riconoscimento del phishing.

- Per farlo ho innanzitutto modificato il dominio aziendale rendendolo autentico (spacescam.com), eliminando sospetti legati a domini sconosciuti.

- Dopodiché ho incluso informazioni credibili come un numero di telefono, indirizzo aziendale ecc.

- Ho aggiunto un ipotetico allegato PDF che rende più autentico e formale il tutto.

- Ho ovviamente corretto ogni errore grammaticale.

- Il link dove viene richiesto di caricare i dati, ora appartiene ad un dominio credibile come spacescam.com, lo stesso dell'indirizzo e-mail del mittente.

- Ridotto leggermente l'urgenza lasciandola sottintendere in parte dalla richiesta stessa.

- Aggiunto un riferimento alle politiche di sicurezza che lasci intendere la preoccupazione a tale riguardo da parte del mittente.

Oggetto: Richiesta prioritaria - Dati Ricerca Chimica dei Materiali 2024

Mittente: j.howard@spacescam.com

Corpo dell'e-mail:

Gentile Lucas,

Spero tutto bene. Ti scrivo per richiedere la tua assistenza in merito alla revisione dei risultati delle ricerche del **Dipartimento di Chimica dei Materiali** svolte nel 2024**.**
Il resoconto finale sarà presentato nella **riunione tecnica con i nostri partner** il prossimo lunedì.

Per garantire che tutti i dati siano aggiornati e accurati, abbiamo bisogno che tu ci fornisca:
1. **Risultati delle ricerche principal**i condotte nel 2024.
2. **Descrizione dei nuovi materiali sviluppati**, incluse le loro proprietà chimico/fisiche.
3. **Rapporti tecnici** e dati sperimentali di rilievo.

Ti chiediamo di caricare i dati attraverso il nostro portale sicuro entro le 19:00 di oggi.
Puoi accedere al portale al seguente link:
https://portal.spacescam.com/departments/chemical-materials/upload

Peer ulteriori dettagli su come organizzare i file, ti invitiamo a consultare il documento allegato.

Ti ringrazio per il tuo impegno nel garantire che tutto sia pronto per la revisione.

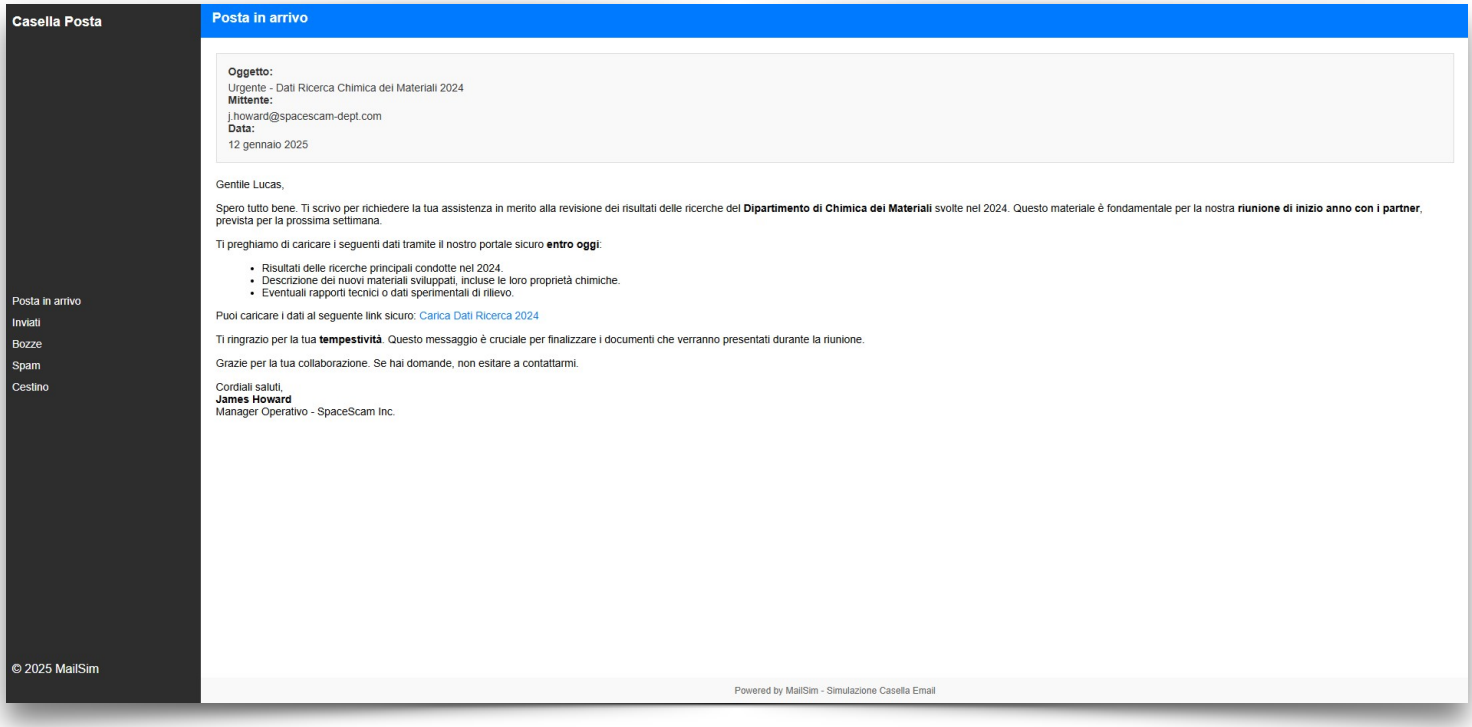
Cordiali saluti,
James Howard
Manager Operativo - SpaceScam Inc.
Space Blvd, Suite 500 Los Angeles, CA 90001
Tel +1 (555)987-6543

ESERCIZIO BONUS 2

Nel secondo esercizio bonus viene richiesto di fare l'html dell'e-mail copiando una e-mail di phishing.

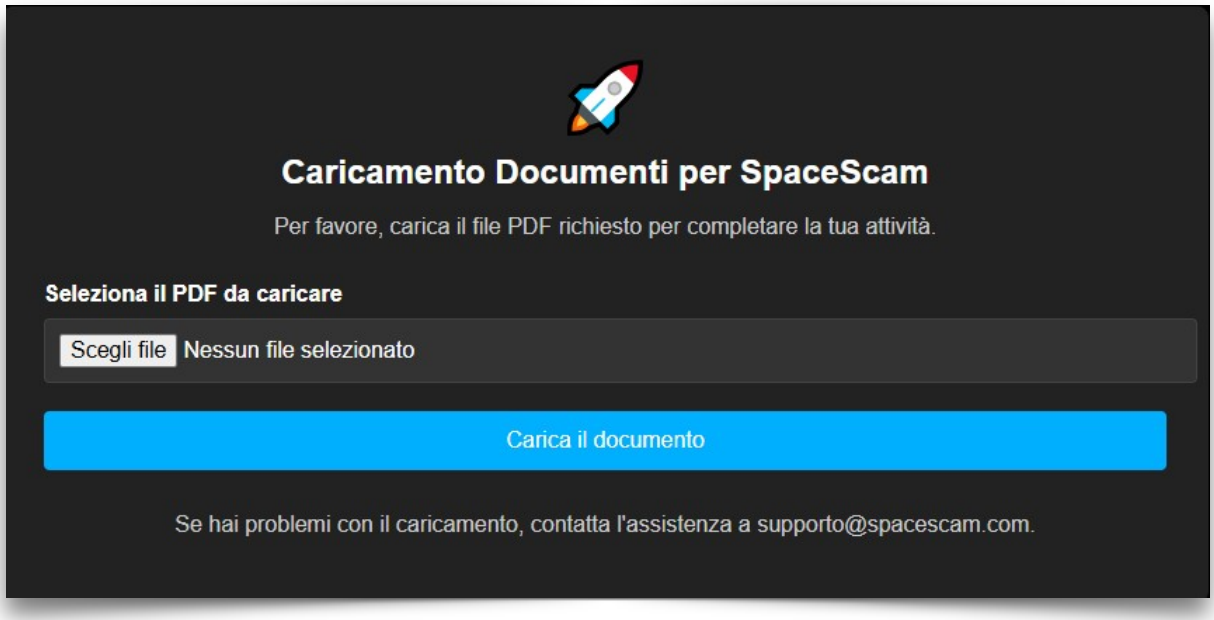
- Non disponendo di nessuna e-mail di phishing che fosse simile a quella del mio scenario ho provveduto, anche con l'aiuto di chatgpt, a crearne una da zero.

- Ho creato una pagina che fosse il più simile possibile ad una casella di posta elettronica classica, poi descritto il contenuto a mio piacimento e reso il link cliccabile:



- Il codice html è presente alla repository Github: https://github.com/RicVal6/Progetto-S5-L5/blob/main/casellamail.html

- Oltre a questo ho creato anche l'html della pagina di caricamento file che dovrebbe aprirsi una volta seguito il link:



- Codice html presente al link Github:
  https://github.com/RicVal6/Progetto-S5-L5/blob/main/link.html