

## Sommario

<b>1. Obiettivo.....</b>	<b>2</b>
<b>2. Ruolo ipotizzato.....</b>	<b>2</b>
<b>3. Contesto.....</b>	<b>2</b>
<b>3.1 Target dell'attacco.....</b>	<b>2</b>
<b>3.2 Modalità dell'attacco .....</b>	<b>2</b>
<b>4. E-mail di phishing generate con l'IA.....</b>	<b>3</b>
<b>5. Elementi che rendono le e-mail credibili.....</b>	<b>5</b>
<b>6. Elementi sospetti nelle e-mail.....</b>	<b>5</b>
<b>7. Alternative possibili .....</b>	<b>6</b>
<b>8. Simulazione tecnica con SEToolkit e pagina di login personalizzata .....</b>	<b>7</b>
<b>9. Conclusioni .....</b>	<b>9</b>

## 1. Obiettivo

In questa esercitazione ho simulato un attacco di phishing mirato (spear phishing) all'interno della rete di un'azienda fittizia, con l'obiettivo di valutare il livello di consapevolezza degli utenti aziendali di fronte a minacce informatiche che utilizzano canali interni compromessi e linguaggi aziendali autentici.

## 2. Ruolo ipotizzato

Mi sono calato nel ruolo di SOC Analyst impegnato in un'attività di simulazione offensiva in **modalità black box**, agendo come se fossi un attaccante esterno privo di conoscenze preliminari sull'ambiente aziendale.

L'attacco parte da un presupposto: l'account email del reparto Risorse Umane è stato compromesso (es. tramite spear phishing o credenziali esposte). Questo accesso iniziale mi permette di inviare comunicazioni aziendali legittime e attendibili a nome del reparto HR. Questo mi permette di sfruttare la fiducia dei dipendenti verso tale reparto.

## 3. Contesto

L'azienda target è *ProgeT S.p.A.*, una realtà fittizia del settore costruzioni, strutturata in diversi livelli: ruoli dirigenziali, amministrativi e operativi. Come attaccante simulato, ho ottenuto l'accesso all'account email compromesso: [risorse.umane@project.it](mailto:risorse.umane@project.it).

Sfruttando questo accesso, ho messo in atto una finta campagna di welfare natalizio, con lo scopo di indurre i dipendenti a cliccare su un link esterno e inserire le proprie credenziali aziendali, permettendomi così di ottenere accesso remoto ai loro sistemi aziendali.

### 3.1 Target dell'attacco

L'attacco è stato suddiviso in due campagne diverse, una per ciascun segmento di utenti:

- **Livello alto:** Project Manager, Capi Reparto, Dirigenti
- **Livello basso:** Impiegati amministrativi, operai, staff tecnico

### 3.2 Modalità dell'attacco

A ogni gruppo ho inviato una mail personalizzata, con linguaggio, tono e contenuto adattati al profilo professionale del destinatario, mantenendo la coerenza stilistica con le comunicazioni HR interne.

Entrambe le email propongono un *voucher natalizio* come benefit aziendale, richiedendo però l'accesso a un portale esterno (finto), graficamente simile a un sito ufficiale, dove è necessario inserire le proprie credenziali aziendali per ottenere lo sconto.

URL utilizzati

- Per i dipendenti di alto livello: <https://benefit.proget-hr.com/voucher2025a>
- Per i dipendenti di basso livello: <https://benefit.proget-hr.com/voucher2025b>

Il dominio è pensato per sembrare coerente con i canali ufficiali aziendali, sfruttando un nome credibile e struttura simile ai siti reali.

L'obiettivo dell'attacco è quello di raccogliere credenziali valide da utilizzare per tentare *l'accesso ai dispositivi aziendali o risorse interne*, simulando un'*escalation* successiva all'ingresso in rete.

Tutte le email riportano una scadenza credibile, coerente con l'oggetto (voucher natalizio). Questa scadenza è stata inserita per aumentare un senso di urgenza non troppo marcato e spingere l'utente a compiere l'azione rapidamente, senza sospetti.

## 4. E-mail di phishing generate con l'IA

Per la redazione delle email ho utilizzato ChatGPT, un modello linguistico basato su intelligenza artificiale sviluppato da OpenAI. Lo strumento è stato impiegato non solo per generare comunicazioni verosimili, coerenti con il contesto aziendale simulato, ma anche per aiutarmi a strutturare un prompt più specifico ed efficace rispetto agli obiettivi dell'esercitazione.

Di seguito riporto il prompt completo utilizzato per ottenere le email phishing personalizzate:

Sono uno studente di cybersecurity e sto realizzando un'esercitazione di phishing interno. L'obiettivo è simulare un attacco realistico inviato da un account compromesso del reparto HR di un'azienda fittizia chiamata ProjeCT S.p.A., azienda del settore costruzioni.

Voglio generare due email distinte, inviate dallo stesso mittente (l'HR), ma dirette a:

Dipendenti di alto livello (Project Manager, Capi Reparto)

Dipendenti di basso livello (impiegati, operai, staff)

Entrambe le email annunciano la possibilità di ricevere un voucher natalizio scontato come iniziativa aziendale di welfare.

Specifiche comuni alle due email:

Il tono dev'essere istituzionale e credibile, come in una vera comunicazione interna aziendale.

Le email contengono un link a un sito esterno (finto) dove viene richiesto l'inserimento delle credenziali aziendali per ottenere il voucher.

Le email contengono un link a un sito esterno (finto) dove viene richiesto l'inserimento delle credenziali aziendali per ottenere il voucher.

Il link ha due percorsi differenti:

Per i dipendenti di alto livello: <https://benefit.proget-hr.com/voucher2025a>

Per i dipendenti di basso livello: <https://benefit.proget-hr.com/voucher2025b>

Le percentuali di sconto sono diverse:

80% per alto livello

60% per basso livello

La scadenza dell'iniziativa è il 20 dicembre 2025.

Email 1 – Target: Dipendenti alto livello  
Tono leggermente più esclusivo

Enfasi su benefit dirigenziali

Percentuale sconto 80%

Link: /voucher2025a

Email 2 – Target: Dipendenti basso livello  
Tono accessibile, più amichevole ma sempre professionale  
Enfasi sul regalo aziendale per tutti

Percentuale sconto 60%

Link: /voucher2025b

Scrivimi le due email complete (senza nomi personalizzati), pronte per essere copiate e incollate in un sistema di simulazione di phishing. Non usare icone, ma solo testo e grassetto. Inserisci anche email mittente con dominio @project.it.

Riporto le due e-mail di phishing generate.

**Email 1 – Target: Dipendenti di alto livello (Project Manager, Capi Reparto)**

Mittente: [risorse.umane@project.it](mailto:risorse.umane@project.it)

Oggetto: Iniziativa Welfare Natale 2025 – Voucher riservato alla Dirigenza

Gentili Colleghi,

in vista delle festività natalizie, Project S.p.A. è lieta di annunciare un'iniziativa esclusiva rivolta al management e ai profili dirigenziali dell'azienda, come riconoscimento per l'impegno e la responsabilità dimostrati nel corso dell'anno.

È stato predisposto un **voucher natalizio a tariffa agevolata**, usufruibile per una selezione di beni e servizi convenzionati. Il **valore del contributo aziendale** previsto per la vostra categoria corrisponde all'**80% del valore nominale del voucher**.

Per ottenere il voucher, è necessario accedere al portale riservato e completare la procedura di richiesta entro il **20 dicembre 2025**.

👉 **Accedi ora al portale dedicato:**

<https://benefit.proget-hr.com/voucher2025a>

L'accesso è consentito unicamente tramite autenticazione con le **credenziali aziendali**.

Per ulteriori informazioni, potete contattare il team HR.

Cordiali saluti,

**Ufficio Risorse Umane**

Project S.p.A.

[risorse.umane@project.it](mailto:risorse.umane@project.it)

**Email 2 – Target: Dipendenti di basso livello (impiegati, operai, staff)**

Mittente: [risorse.umane@project.it](mailto:risorse.umane@project.it)

Oggetto: Voucher di Natale 2025 – Un piccolo pensiero per te

Gentili Collaboratori,

anche quest'anno Project S.p.A. desidera ringraziarvi per il lavoro svolto con dedizione, proponendo un'iniziativa speciale pensata per tutti i dipendenti.

È disponibile un **voucher natalizio con sconto del 60%**, da utilizzare su una selezione di prodotti e servizi in convenzione. Si tratta di un piccolo gesto che riflette la nostra volontà di promuovere il benessere e il senso di appartenenza all'interno dell'azienda.

La richiesta del voucher può essere effettuata online, in pochi passaggi, entro il **20 dicembre 2025**.

👉 **Richiedi il tuo voucher qui:**

<https://benefit.proget-hr.com/voucher2025b>

Per accedere, sarà sufficiente autenticarsi con le **credenziali aziendali**.

Per qualsiasi dubbio, il team HR rimane a disposizione.

Un cordiale saluto,

**Ufficio Risorse Umane**

Project S.p.A.

[risorse.umane@project.it](mailto:risorse.umane@project.it)

## 5. Elementi che rendono le e-mail credibili

Gli elementi principali che contribuiscono alla loro credibilità sono:

- **Mittente attendibile**

Le comunicazioni provengono dall'indirizzo [risorse.umane@project.it](mailto:risorse.umane@project.it), apparentemente legittimo e coerente con il reparto deputato a gestire benefit, welfare e iniziative rivolte ai dipendenti. La firma finale ("Ufficio Risorse Umane") rafforza la fiducia, facendo apparire l'email come parte di una comunicazione ufficiale aziendale.

- **Linguaggio e tono professionale personalizzato**

Lo stile delle email è coerente con quello utilizzato normalmente nelle comunicazioni aziendali: tono formale e linguaggio professionale. È stato inoltre personalizzato in base al target:

Per i dirigenti: tono più esclusivo, enfasi sul beneficio riservato a ruoli apicali.

Per lo staff operativo: tono più accessibile, benefit presentato come premio collettivo.

Questa differenziazione rende il messaggio più credibile e aumenta la rilevanza percepita.

- **Contenuto contestuale e attraente**

La proposta di un *voucher natalizio scontato* risulta credibile per tempistiche (in prossimità delle festività) e coerente con pratiche comuni di welfare aziendale. Lo sconto proposto (60% o 80%) rappresenta un beneficio concreto e desiderabile.

Inoltre, periodi come Natale o l'estate sono notoriamente caratterizzati da chiusure di bilancio e picchi operativi, che aumentano la distrazione e abbassano l'attenzione dei destinatari, rendendo il phishing più efficace.

A livello psicologico, la promessa di un premio stimola il rilascio di dopamina, generando una sensazione di piacere e spingendo all'azione senza riflettere troppo.

- **Urgenza percepita**

Le email inseriscono una scadenza realistica e "soft" (es. **20 dicembre 2025**) che genera senso di urgenza senza apparire aggressiva. Questo crea **pressione implicita** e stimola un comportamento impulsivo, riducendo il tempo a disposizione per valutare la legittimità del messaggio.

## 6. Elementi sospetti nelle e-mail

Gli elementi principali che invece riducono la loro credibilità sono:

- **Dominio del link sospetto**

Il dominio del link è *proget-hr.com*, diverso dal dominio aziendale reale *project.it*. Questo può destare sospetti in un utente esperto o con formazione sulla sicurezza informatica.

- **Nessun riferimento personalizzato**

Le e-mail non includono riferimenti personali come il nome o il cognome del destinatario, ma utilizzano una formula generica rivolta a un gruppo indistinto di collaboratori. Questo approccio può ricordare le campagne di phishing non mirate, riducendo la percezione di autenticità del messaggio.

- **Assenza di documenti ufficiali**

Non c'è alcun allegato (PDF, circolare interna, policy HR) che può accompagnare vere iniziative aziendali. Tutta la comunicazione è interamente basata su un link esterno, senza ulteriori spiegazioni né riferimenti a piattaforme interne che di solito gestiscono questi tipi di benefit.

- **Richiesta anomala di inserimento credenziali aziendali**

Anche se presentata in modo indiretto, la richiesta di inserire le proprie credenziali aziendali per ottenere un semplice voucher può risultare anomala. Normalmente, l'accesso a benefit aziendali avviene tramite sistemi interni o portali già noti ai dipendenti, senza necessità di reinserire le credenziali su un sito esterno.

- **Comunicazione eccessivamente formale**

Una comunicazione troppo formalizzata e priva di errori può apparire artificiale. Ciò potrebbe far insospettare gli utenti più esperti, abituati a ricevere e-mail HR con un tono leggermente più umano, informale o con elementi distintivi legati alla cultura aziendale.

## 7. Alternative possibili

Sulla base delle osservazioni precedenti relative agli elementi sospetti, sono state apportate alcune modifiche alle e-mail per aumentarne il livello di credibilità e realismo, simulando una campagna di phishing più sofisticata e difficile da rilevare.

- **Mascheramento del link**

Il collegamento al sito esterno non viene più mostrato direttamente nell'e-mail, ma è stato nascosto dietro un anchor testuale ("*Clicca qui per accedere alla piattaforma dedicata*"), riducendo l'impatto visivo del dominio.

- **Introduzione di errori di battitura controllati**

Sono stati inseriti errori (es. "adeisone", "convenzoinati", "idonetità"), con l'obiettivo di evitare la percezione di un messaggio automatizzato. Questo approccio mira a rendere l'e-mail più simile a una reale comunicazione interna, dove piccoli refusi possono essere tollerati o considerati normali.

- **Rimozione di elementi grafici potenzialmente sospetti**

Iconcine, pulsanti stilizzati o altri elementi sono stati rimossi per evitare che il messaggio venga percepito come generato tramite template automatizzati.

**Mittente:** risorse.umane@project.it

**Oggetto:** Voucher Natalizio Dirigenziale – Accesso Prioritario

**Gentili Colleghi,**

nell'ambito delle iniziative di welfare previste per il periodo natalizio, siamo lieti di comunicarvi l'attivazione di un **voucher dedicato ai dipendenti in posizione dirigenziale o gestionale**, con una **percentuale di sconto pari all'80%** su una selezione di prodotti e servizi convenzoinati.

L'iniziativa è frutto di una **collaborazione con un partner esterno**, selezionato per garantire la massima qualità dei benefit.

Per questo motivo, l'accesso alla piattaforma richiede l'autenticazione tramite **credenziali aziendali**, necessarie a verificare l'identità del personale autorizzato.

[Clicca qui per accedere alla piattaforma dedicata](#)

La scadenza per l'adeisone all'iniziativa è fissata al **20 dicembre 2025**.

Vi invitiamo a non condividere il link con altri utenti, in quanto la campagna è riservata esclusivamente ai profili dirigenziali.

Rimanendo a disposizione per eventuali chiarimenti, porgiamo cordiali saluti.

**Ufficio Risorse Umane**

ProjecT S.p.A.

**Mittente:** risorse.umane@project.it

**Oggetto:** Voucher Natalizio 2025 – Iniziativa Aziendale

**Gentili Dipendenti,**

come ogni anno, Project S.p.A. promuove un'iniziativa rivolta a tutto il personale per celebrare le festività natalizie e ringraziare per il lavoro svolto.

Anche per il 2025, è disponibile un **Voucher Scontato del 60%** su una gamma di prodotti e servizi selezionati.

L'iniziativa è realizzata in **collaborazione con un partner esterno**, per questo è necessario **accedere alla piattaforma dedicata tramite le proprie credenziali aziendali**, che servono ad autorizzare l'accesso e verificare l'idoneità dell'utente.

[Clicca qui per richiedere il tuo voucher](#)

La richiesta potrà essere effettuata fino al **20 dicembre 2025**.

**Vi invitiamo a completare la procedura entro i termini indicati.**

Cordiali saluti,

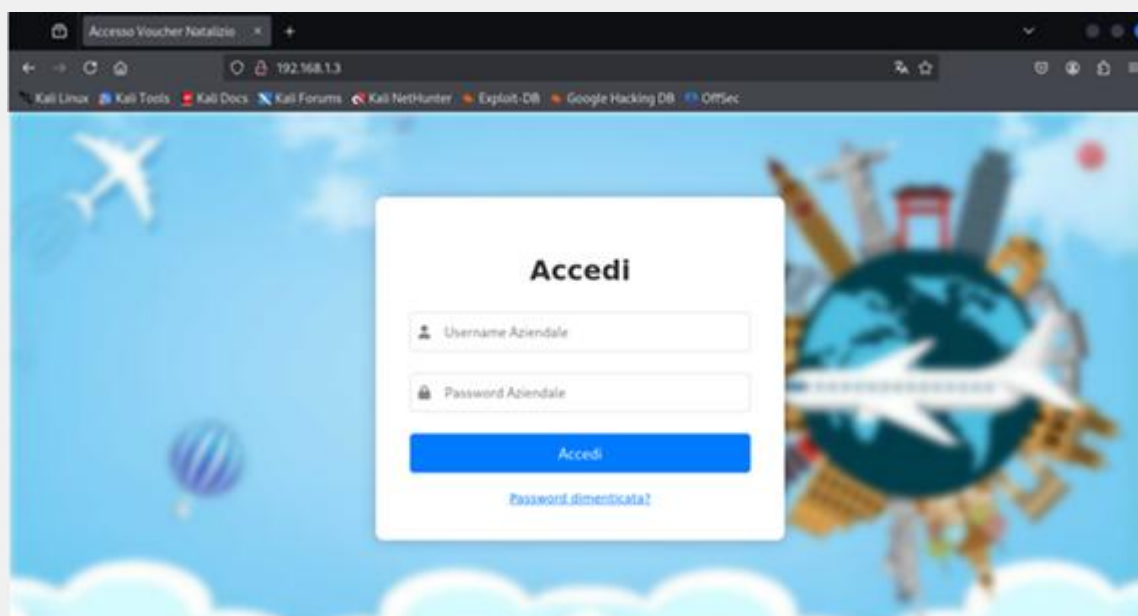
**Ufficio Risorse Umane**

Project S.p.A.

## 8. Simulazione tecnica con SEToolkit e pagina di login personalizzata

Per rendere l'esercitazione più completa, ho simulato una possibile azione di phishing sviluppando manualmente una pagina di login personalizzata, associata ai link precedentemente progettati per i dipendenti aziendali. La pagina è stata creata partendo da zero, con l'obiettivo di riprodurre un'interfaccia coerente con l'identità visiva di un portale aziendale dedicato ai benefit natalizi.

A supporto della realizzazione del codice HTML, ho utilizzato un modello generato tramite intelligenza artificiale, successivamente revisionato manualmente per garantirne il corretto funzionamento e l'aderenza allo scenario simulato.



Su **Kali Linux**, tramite **SEToolkit**, ho configurato la raccolta delle credenziali seguendo questi passaggi:

1. Avvio del terminale e dello strumento: **sudo setoolkit**
2. Navigazione nel menu:  
**Social-Engineering Attacks > Website Attack Vectors > Credential Harvester Attack Method > Custom Import**

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>3
```

3. Impostazione dell'IP locale come indirizzo del server d'attacco: *192.168.1.3*

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.3]: 192.168.1.3
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
```

4. Selezione dell'opzione 2. *Copy the entire folder* per importare tutte le risorse presenti nella cartella login\_site. Particolare attenzione merita il file con codice html poiché va nominato esattamente come richiesto "*index.html*". Data la presenza di immagini all'interno della pagina chiediamo di copiare l'intero contenuto della cartella.
5. Inserimento dell'URL visibile simulato: <https://benefit.proget-hr.com/voucher2025a>

```
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned: /home/kali/Downloads/login_site/
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported: https://benefit.proget-hr.com/voucher2025a
```

6. Una volta che l'utente inserisce le proprie credenziali, SEToolkit intercetta e visualizza i dati (email e password) direttamente nel terminale, simulando con successo un furto di identità aziendale.

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=salvatore.gifuni@proget.it
POSSIBLE PASSWORD FIELD FOUND: password=CiaoATutti!!
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Il codice HTML della pagina è disponibile sul mio [repository GitHub](#).



## 9. Conclusioni

L'utilizzo di ChatGPT per la creazione delle e-mail di phishing ha mostrato come l'intelligenza artificiale possa generare scenari realistici, adattando linguaggio e tono ai destinatari. Tuttavia, è fondamentale sottolineare che l'attenzione ai dettagli e il contesto aziendale sono essenziali per garantire la credibilità del messaggio.

Questa simulazione evidenzia anche l'importanza di una revisione umana nell'elaborazione finale, per affinare ulteriormente il contenuto e rilevare eventuali incoerenze o dettagli che un'AI potrebbe non cogliere.

Infine, comprendere le tecniche di ingegneria sociale è cruciale per migliorare la consapevolezza dei dipendenti e sviluppare difese adeguate contro attacchi reali.