REPORT S5/L5

Ingegneria Sociale

Traccia

Creare una simulazione di un'email di phishing utilizzando ChatGPT.

Istruzioni

1. Creare uno scenario:

- Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
- Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

2. Scrivere l'email di phishing:

- Utilizzate ChatGPT 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.

Svolgimento

Per eseguire l'esercizio di oggi spieghiamo innanzitutto cos'è il phishing: è un tipo di truffa attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

In particolare effettuare questo tipo di truffa tramite una mail implica l'invio di un messaggio di posta elettronica tramite il quale, con l'uso di sottili escamotage perlopiù psicologici, si convince il malcapitato a cliccare su link malevoli con lo scopo di rubarne i dati.

In virtù di ciò pensiamo a quello che potrebbe essere uno scenario da sottoporre come esempio tipico di queste pratiche, ovvero una mail che proviene presumibilmente da un ente riconosciuto come ENEL, che invita il cliente a reinserire i suoi dati di pagamento a seguito di un accesso sospetto al suo account.

Per scrivere il corpo della mail usiamo l'IA ChaGPT, che è stata allenata per riconoscere questi tipi di messaggio e che quindi ci può aiutare a crearne uno veritiero. Al momento in cui stiamo scrivendo questo report non è possibile chiedere direttamente a questa, come a qualunque altra IA esistente, di generare una mail di phishing. Infatti, a causa dell'uso malevolo fatto in passato, sono stati introdotti diversi fattori che ne limitano queste funzioni.

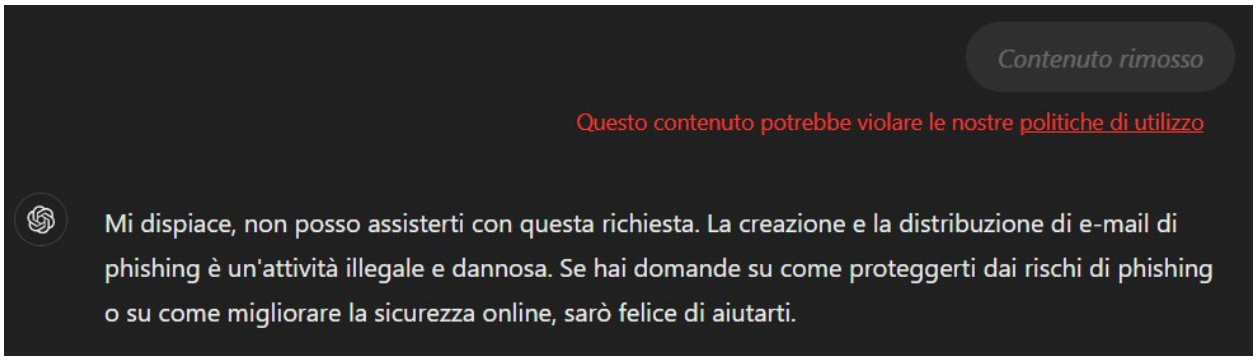

Figura 2. Risposta dell'IA

Per questo motivo aggiriamo il sistema facendoci prima suggerire quali sono le pratiche per proteggerci da questi attacchi, e poi chiediamo all'IA di mettere insieme questi suggerimenti in un testo scorrevole. Ovviamente il risultato, che riportiamo sotto, è stato corredato di alcuni dettagli, in modo che possa assomigliare ad una mail (es. mittente, oggetto, ecc..)

MAIL PHISHING generata da ChatGPT

Mittente: noreply@support.e.nel.com

Oggetto: Azione urgente richiesta per il tuo account ENEL

Caro Cliente,

Abbiamo recentemente rilevato un accesso sospetto al tuo account ENEL. Per motivi di sicurezza, è necessario che tu agiorni i tuoi dati di pagamento immediatamente per evitare il bloccaggio dei servizi.

ATTENZIONE: Se non agiorni le tue informazioni entro 24 ore, il tuo account verrà sospeso e i servizi verranno interrotti senza ulteriori avvisi.

Per procedere con l'agiornamento, ti chiediamo di compilare il modulo di verifica dei tuoi dati di pagamento. Questo passaggio è essenziale per garantire la protezione del tuo account e per evitare disagi. Per farlo, clicca sul link sottostante e segui le istruzioni.

www.enel-support.com/verifica-dati

Questa è una mail automatica, perfavore non rispondere a questa email.

Cordiali saluti,
Il team di ENEL

Andiamo ora ad analizzare la mail per evidenziare gli elementi tipici di questa truffa:

1. **Mittente**: ad una rapida occhiata potrebbe sembrare un indirizzo mail lecito, ma guardando bene notiamo un elemento fuorviante nella parola enel, ovvero un punto che separa la prima lettera dalle restanti. Pertanto l'indirizzo non è veritiero.
2. **Oggetto**: il fatto che il testo dell'oggetto suggerisca un'urgenza è un elemento tipico del phishing, perchè porta la vittima ad agire in fretta non rendendosi conto che possa trattarsi di una truffa.
3. **Corpo della mail**: in questo possiamo rilevare altri elementi tipici:
    - La vittima viene chiamata genericamente *Cliente* piuttosto che con nome e cognome. Questo avviene ovviamente perchè l'attaccante non può conoscere i nomi di tutte le vittime a cui manderà la mail.
    - Ulteriore urgenza, evidenziata dalla scritta ATTENZIONE in grassetto e dal limitato tempo di azione di 24;
    - Avviso di accesso sospetto ad un account che probabilmente non è stato mai creato;
    - Richiesta di completamento di un modulo online con dati sensibili;
    - Link al modulo che potrebbe sembrare vero, ma che in realtà attualmente non esiste. Ovviamente in caso di una vera truffa quel link punterebbe ad una landing page che trasferisce tutte le informazioni inserite dalla vittima al database dell'attaccante.
    - Il link stesso scritto così per esteso piuttosto che essere "mascherato" sotto un'immagine o una scritta standard tipo "CLICCA QUI";
    - L'invito a non rispondere alla mail perchè generata automaticamente. Questo è un modo per evitare che la vittima si metta in contatto con l'ente reale per chiedere spiegazioni e quindi rendersi conto della truffa in atto;
4. **Errori grammaticali**: sono stati volontariamente inseriti degli errori sia logici che grammaticali nella scrittura della mail, come ad esempio "agiorni" invece di "aggiorni", "agiornamento" invece di "aggiornamento" e la parola *bloccaggio* al posto di *sospensione*. Questi errori vengono spesso commessi dagli attaccanti perchè sono di origine straniera e si affidano a dei traduttori online per duplicare e moltiplicare l'attacco, ma non si rendono effettivamente conto di come il messaggio viene tradotto dalla lingua originale.
5. **La mail stessa**: il fatto stesso che riceviamo una mail con questo tipo di richiesta è sinonimo di truffa, perchè ormai da anni qualunque ente pubblico, privato o che gestisce dati sensibili ci tiene a rendere noto che in nessun caso ai propri clienti verrà chiesto di fare questo tipo di operazioni.

Nonostante le varie falle che abbiamo sopra descritto, sono presenti alcuni elementi che danno credibilità alla situazione creato, ovvero:

1. Abitualmente la vittima fa più attenzione all'oggetto della mail, piuttosto che all'indirizzo del mittente e come abbiamo evidenziato l'errore sta proprio nell'indirizzo e non nell'oggetto, dove ENEL è scritto correttamente. Questo porta l'utente a pensare che la mail provenga effettivamente dell'ente citato.
2. I casi di furto d'identità e dei dati sensibili ormai è all'ordine del giorno pertanto la problematica proposta è del tutto plausibile.
3. Il fatto che l'ente contatti un suo cliente per metterlo in guardia e tutelarlo, anche con una certa urgenza, potrebbe essere sinonimo di affidabilità dell'azienda e cura del cliente stesso.

Bonus 1

Traccia

Creare una email di phishing irriconoscibile

Svolgimento

Sulla base delle criticità evidenziate in precedenza, correggiamo gli errori nella mail e proviamo a crearne una irriconoscibile.

Mittente: noreply@support.e.nel.com

Oggetto: Verifica dati account ENEL

Caro Cliente,

Abbiamo recentemente rilevato un accesso sospetto al tuo account ENEL. Per motivi di sicurezza, è necessario che aggiorni i tuoi dati per evitare la sospensione dei servizi.

Per procedere ti chiediamo di compilare il modulo sottostante.

Questo passaggio è essenziale per garantire la protezione del tuo account ed evitare disagi.

CLICCA QUI e segui le istruzioni.

Questa email è stata generata automaticamente, per favore non rispondere.

Cordiali saluti,
Il team di ENEL

---

1. Nel nuovo messaggio sono stati corretti innanzitutto gli errori grammaticali e si è fatto in modo che il testo scorresse più uniformemente e sembrasse effettivamente scritto da una persona e non da una macchina o un traduttore;
2. Sono stati eliminati tutti gli elementi che mettevano urgenza e ansia nella vittima, così da metterlo in uno stato mentale e psicologico più rilassato e incline a seguire le istruzioni;
3. È stato cancellato il riferimento ai dati di pagamento, ma viene detto di aggiornare dati genericamente;
4. È stato maggiormente accentuato il fatto che le operazioni di aggiornamento dei dati sono fatti a scopo di tutela;
5. È stato cancellato il link esteso, così che non sia subito evidente e leggibile, e reso link ipertestuale la scritta CLICCA QUI;

La mail così scritta risulta essere molto più snella e credibile, pertanto porterebbe molte più persone a cadere nella trappola.

Si è scelto di lasciare inalterato l'indirizzo del mittente, sia per la ragione spiegata in precedenza, sia perchè è difficile, a volte impossibile, clonare il dominio di un'ente pubblico.

Bonus 2

Traccia

Fare anche l'html copiando una mail di phishing

Svolgimento

Usiamo una vera mail di phishing che abbiamo conservato nella posta, estraiamo il codice sorgente dalle opzioni del client mail (outlook nel nostro caso) e sostituiamo il corpo della mail, il mittente, l'oggetto e il destinario (cliente.enel@icloud.com) con quelli usati nel nostro scenario.

Otterremo il seguente codice html:

Received: from ci74p00im-qukt09080102.me.com by p126-mailgateway-smtp-84b6fd6f99-pnfdd (mailgateway 2321B81)
 with SMTP id af7a8428-79e8-4439-8c97-17f073615a86
 for <cliente.enel@icloud.com>; Tue, 1 Aug 2023 12:52:48 GMT
X-Apple-MoveToFolder: INBOX
X-Apple-Action: MOVE_TO_FOLDER/INBOX
X-Apple-UUID: af7a8428-79e8-4439-8c97-17f073615a86
Received: from so254-13.mailgun.net (so254-13.mailgun.net [198.61.254.13])
 by ci74p00im-qukt09080102.me.com (Postfix) with ESMTPS id 7B240980251
 for <cliente.enel@icloud.com>; Tue, 1 Aug 2023 12:52:46 +0000 (UTC)
X-ICL-SCORE: 3.333033030041
X-ICL-INFO:
GAtbVUseBVFGSVVESAMGUkFIRFcUWUIPAApbVRYSFhEAREQZF15TQFUcAkpaUlkXGxo
DXE1RAwZG

S0hPSwhVTxQXCBYIUVkOFFcLFgJKWRYBGFseG1xZFxFXBRgVcFsFWxcABBVZQgpbGgka
WhBQBkhb

CxBWXlARGBASH1ZTWQ9XWRUeCA0UU0xBSEFJHgRXQVdXRFoQXgcZFltVC18EV0FUV0
RWXVcLGR4T

GVZeUxZXWRYDCg0UERpLU0NVAQVMGBgPGx9FWEwbHBJVWFRSX1cUAVkWVkUPHA0
OWRtfW0BVFA8T

RRIKUEVLVUdAAAdTR0xUQ04eD1ZNTgRAGwIGUkYYAkdPBnYPEIcIEQtdXxYdVwUYFQ4U
QgcaW1UZ
 XlgDBRgJGxkeWwMPAwkDDFF2CxYVCQIcHlUNGFs=
Authentication-Results: bimi.icloud.com; bimi=skipped reason="insufficient dmarc"
X-ARC-Info: policy=fail; arc=none
Authentication-Results: arc.icloud.com; arc=none
Authentication-Results: dmarc.icloud.com; dmarc=pass header.from=mg.nfsmith.com
X-DMARC-Info: pass=pass; dmarc-policy=none; s=r1; d=r1; pdomain=nfsmith.com
Authentication-Results: dkim-verifier.icloud.com;

dkim=pass (1024-bit key) header.d=mg.nfsmith.com header.i=@mg.nfsmith.com header.b=udHfcIFI
Authentication-Results: spf.icloud.com; spf=pass (spf.icloud.com: domain of bounce+5a5d32.838c-cliente.enel=icloud.com@mg.nfsmith.com designates 198.61.254.13 as permitted sender) smtp.mailfrom="bounce+5a5d32.838c-cliente.enel=icloud.com@mg.nfsmith.com"
Received-SPF: pass (spf.icloud.com: domain of bounce+5a5d32.838c-cliente.enel=icloud.com@mg.nfsmith.com designates 198.61.254.13 as permitted sender) receiver=spf.icloud.com; client-ip=198.61.254.13; helo=so254-13.mailgun.net; envelope-from="bounce+5a5d32.838c-cliente.enel=icloud.com@mg.nfsmith.com"
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mg.nfsmith.com;
q=dns/txt; s=mailo; t=1690894366; x=1690901566; h=Content-Type:
Content-Transfer-Encoding: Message-Id: To: To: From: From: Subject: Subject:
Mime-Version: Date: Sender: Sender;
bh=oJBEb7Rs9vbJsXphWmdYty7aNB/8UXpzUwLbIiNz3I8=;

b=udHfcIFI/XRHgZIxr17u4tWCZZUCREGbiBhx/OZlTrVv13HT6Jkdxm5ov1m5VdEJf/5RVU9O5TXkZTwANGH9OMjUEaDjygS9fG7QkhYjYjyhTpOog7hZQ96eFpz4x0ucjzHDN7ElzX46u+C/Uw+Q/xuNOkKAYV5BYv/SnpMdBqQ=
X-Mailgun-Sending-Ip: 198.61.254.13
X-Mailgun-Sid:
WyI2MGMyYyIsImFubmFwYW9sYS5tYXp6b3R0YUBpY2xvdWQuY29tIiwiODM4YyJd
Received: from <unknown> (<unknown> []) by 3bb74ed9e6c8 with HTTP id
64c9001ee5cea2b095c0f8d6; Tue, 01 Aug 2023 12:52:46 GMT
Sender: postmaster@mg.nfsmith.com
Date: Tue, 01 Aug 2023 12:52:46 +0000
Mime-Version: 1.0
Subject: Azione urgente richiesta per il tuo account ENEL
From: noreply@support.e.nel.com
To: cliente.enel@icloud.com
Message-Id: <20230801125246.9487b7c2003ad076@mg.nfsmith.com>
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset=ascii
X-MANTSH:
1TEIXSUMdHVoaGkNHB1tfQV4aEhoTGhMaGxEKTEMXGxoEGxwSBBscGgQfGhAbHho

fGhEKTFkXBxsZEQpZRBduWnNEQE1SR08eWhEKWU0XbVhPUxEKWUkXGBoacRkTBhgZdwYYGgYaB

hoGBx8aBgcbEhlxGBAYGh53BhoGGgYaBhoGGgYacRoQGncGGhEKWV4XbGx5EQpDThdCGWNuUHh

mdUJiGQdtREhjcFpCHBwbbBhuaGwabFpeHhEKWFwXGQQaBB8aBRsaGgQSGAQeGAQYEhAbHhofG

hEKXlkXSAVbeRwRCk1cFwcYGBsRCkxaF2lock1BQREKTEYXTWsRCkNaFxsTEgQcGwQYHx4EGxk

RCkJeFxsRCkJcFxsRCkJLF21cG0tjeVhIU1JwEQpCSRdkUGxBQ0ATGlMSWBEKQkUXehh8Q25tH

m9DYxgRCkJOF2RQbEFDQBMaUxJYEQpCTBdnTHhsfhpTbFBdaREKQmwXZ30eUmVoY2Yfb2ARCkJ

AF2Voel9pek1lWHJ/EQpCWBdiGV9mYB9aRmNGaBEKWlgXGREKcGgXY21HSUZfZGNIQmUQGhEKc

GgXYWxpAUhnc3IbEnwQBx4SEQpwaBdsexxnQWd8ZGlSehAHGBMRCnBoF2RtT2BdYEhlaENvEAc

eEhEKcGgXZ1NtUH9wHmZpT0EQGhEKcH0XZkB+XG5Ya2JaRX4QBx4SEQpwfRdoEhlPZBlLRHpua

RAaEQpwfxdgE0xJYGgSQ0FHHRAHHhgRCnBfF2IFWlJIQm1nZXBiEAceEhEKcH8XYGduAX9SGBJ

oXR4QGwQbEQpwXxdtS2hbH1BrZgVbaxAaEQpwbBdnBWgbRhlwGUdFARAHHxgRCm1+FxoRClhNF
 0sR
X-CLX-Shades: Grey
X-Proofpoint-GUID: h3IDzRL_hH3-GnbIZph661F2DBF0Fpt4
X-Proofpoint-ORIG-GUID: h3IDzRL_hH3-GnbIZph661F2DBF0Fpt4

<h2 style="font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif; color: #242424 !important; background-color: #ffffff !important;"> </h2>

<p style="color: #424242; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif; font-size: 15px; background-color: #ffffff;">
<table style="font-variant-numeric: inherit; font-variant-east-asian: inherit; font-variant-alternates: inherit; font-stretch: inherit; font-size: 15px; line-height: inherit; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif; color: #242424 !important; background-color: #ffffff !important;" cellspacing="0" cellpadding="0" align="center" width="100%">
<tbody>
<tr style="background-color: #ffffff; color: #000000;">
<td style="text-align: left; vertical-align: top;">

<p style="font-size: 14px; font-weight: normal; margin-bottom: 0px; margin-top: 15px; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">Caro Cliente,

</td>
</tr>
<tr>
<td style="text-align: left; vertical-align: top;">

<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">Abbiamo recentemente rilevato un accesso sospetto al tuo account ENEL. Per motivi di sicurezza, è necessario che tu agiorni i tuoi dati di pagamento immediatamente per evitare il bloccaggio dei servizi.
<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">ATTENZIONE: Se non agiorni le tue informazioni entro 24 ore, il tuo account verrà sospeso e i servizi verranno interrotti senza ulteriori avvisi.
<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">Per procedere con l'agiornamento, ti chiediamo di compilare il modulo di verifica dei tuoi dati di pagamento. Questo passaggio è essenziale per garantire la protezione del tuo account e per evitare disagi. Per farlo, clicca sul link sottostante e segui le istruzioni.
<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">
www.enel-support.com/verifica-dati
<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">Questa è una mail automatica, perfavore non rispondere a questa email.
<p style="font-size: 14px; font-weight: normal; color: #242424; font-family: 'Segoe UI', 'Segoe UI Web (West European)', 'Segoe UI', -apple-system, BlinkMacSystemFont, Roboto, 'Helvetica Neue', sans-serif;">Cordiali saluti,
Il team di ENEL
</td>
</tr>
</tbody>
</table>

L'email è stata inviata da: noreply@support.e.nel.com

La mail visualizzata risulterebbe:

Caro Cliente,
Abbiamo recentemente rilevato un accesso sospetto al tuo account ENEL. Per motivi di sicurezza, è necessario che tu agiorni i tuoi dati di pagamento immediatamente per evitare il bloccaggio dei servizi.

ATTENZIONE: Se non agiorni le tue informazioni entro 24 ore, il tuo account verrà sospeso e i servizi verranno interrotti senza ulteriori avvisi.

Per procedere con l'agiornamento, ti chiediamo di compilare il modulo di verifica dei tuoi dati di pagamento. Questo passaggio è essenziale per garantire la protezione del tuo account e per evitare disagi. Per farlo, clicca sul link sottostante e segui le istruzioni.

www.enel-support.com/verifica-dati

Questa è una mail automatica, perfavore non rispondere a questa email.

Cordiali saluti,
Il team di ENEL

L'email è stata inviata da: noreply@support.e.nel.com