**Ingegneria Sociale: Creazione di una email phishing utilizzando la ChatGPT**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |

L’**ingegneria sociale** è una tecnica di manipolazione psicologica che i malintenzionati usano per indurre le persone a rivelare informazioni sensibili o a compiere determinate azioni, come cliccare su un link o scaricare un file dannoso. Piuttosto che usare attacchi tecnici avanzati, l’ingegneria sociale sfrutta la fiducia, la paura, la curiosità e la fretta delle persone per ottenere ciò che il truffatore vuole.

Ecco i metodi e le tecniche più comuni di ingegneria sociale:

1. **Phishing**: Questo è uno degli esempi più diffusi. Avviene attraverso email o messaggi che sembrano provenire da fonti affidabili, come banche o aziende, e che invitano l’utente a cliccare su un link o fornire informazioni personali (come password e dati bancari).

2. **Spear Phishing**: Una forma di phishing mirata a persone specifiche, spesso basata su informazioni raccolte in precedenza sulla vittima per rendere l’attacco più credibile e personalizzato.

3. **Pretexting**: In questo caso, l’attaccante si inventa una falsa identità o storia per ottenere la fiducia della vittima e indurla a rivelare informazioni riservate. Ad esempio, potrebbe fingersi un dipendente di un’azienda e chiedere dettagli aziendali sensibili.

4. **Baiting**: Questa tecnica offre una sorta di “esca” per incuriosire la vittima. Ad esempio, un file intitolato “Buste paga dell’azienda” potrebbe spingere un dipendente a scaricarlo, trovandosi poi di fronte a un malware.

5. **Tailgating o Piggybacking**: Questo tipo di ingegneria sociale si verifica quando un intruso fisicamente entra in un’area riservata seguendo una persona autorizzata, ad esempio chiedendo di essere lasciato entrare “perché ha dimenticato il badge”.

**Perché l’ingegneria sociale è efficace?**

Gli attacchi di ingegneria sociale sono efficaci perché sfruttano le emozioni umane, come la fiducia, la paura, l’urgenza e persino la curiosità. Le persone tendono a fidarsi delle autorità o dei colleghi, e in situazioni di stress o urgenza possono agire impulsivamente. Questo permette ai malintenzionati di superare le difese tecnologiche puntando direttamente sul fattore umano.

**Come difendersi dall’ingegneria sociale?**

Alcune misure preventive includono:

• **Essere prudenti con le email** e i messaggi che richiedono azioni rapide o informazioni personali.

• **Verificare l’identità** di chi richiede informazioni, soprattutto se si tratta di richieste insolite.

• **Non cliccare link sospetti** o scaricare file da fonti non verificate.

• **Formazione e sensibilizzazione** sulla sicurezza per riconoscere i segnali d’allarme.

In sintesi, l’ingegneria sociale è un tipo di attacco che si basa sulla manipolazione psicologica più che su tecniche informatiche avanzate. Saper riconoscere questi tentativi è essenziale per proteggere le proprie informazioni e la propria sicurezza digitale.

**Di seguito un esempio di Phishing:**

**Oggetto:** Azione Richiesta: Verifica Urgente del tuo Account Bancario

**Testo dell’email:**

**Gentile Cliente,**

Abbiamo notato una recente attività sospetta sul tuo account bancario che richiede la tua immediata attenzione. Per garantire la sicurezza dei tuoi fondi e prevenire accessi non autorizzati, ti invitiamo a **verificare le tue informazioni** al più presto.

**Per favore, clicca sul link sottostante per confermare i tuoi dettagli entro le prossime 24 ore.** Se non procederai, il tuo account potrebbe essere temporaneamente bloccato per la tua protezione.

[**Conferma il tuo account**](http://banca-sicura-login.com/verify)

**Nota Bene:** Questo processo è rapido e richiede solo pochi minuti. La tua sicurezza è la nostra priorità.

In caso di domande, contatta il nostro Servizio Clienti al numero **800-123-456**, disponibile 24/7.

Cordiali saluti,

**Il team di Sicurezza della tua Banca**

*Questo è un messaggio automatico. Si prega di non rispondere a questa email.*



**Spiegazione scenario creato.**

**Scenario Creato:**

Il phishing simula un’email di notifica urgente da una banca. L’email avvisa l’utente di una presunta attività sospetta sul proprio conto e richiede una verifica immediata per evitare il blocco dell’account. L’email invita il destinatario a scansionare un codice QR (incluso nell’email) per confermare i propri dettagli di accesso.

Il link nel QR code porta a un sito di phishing che assomiglia a una pagina di login bancaria, ma reindirizza in realtà al sito di Amazon come esempio per questa simulazione.

**Perché l’Email Può Sembrare Credibile:**

**1. Tono Urgente e Minaccia di Blocco:** L’email dichiara che il conto potrebbe essere sospeso entro 24 ore se non viene verificato. Questo crea un senso di panico e urgenza che spinge la vittima ad agire immediatamente, senza pensarci troppo o fare verifiche ulteriori.

**2. Aspetto Formale e Brand della Banca:** Il messaggio è scritto in modo professionale e include il logo della banca e i termini di sicurezza, il che conferisce una parvenza di autenticità. Spesso, i phisher usano loghi e colori che richiamano l’aspetto ufficiale dell’istituto.

**3. Codice QR come “Shortcut” Sicuro:** Il QR code è presentato come un modo rapido per accedere alla verifica dell’account, un metodo che le persone potrebbero considerare sicuro. Il QR evita che la vittima veda il vero URL, aumentando la probabilità di cliccare senza sospetti.

**4. Dettagli di Contatto e Messaggio Automatica:** L’email include un numero di telefono fittizio e una nota che specifica che si tratta di un “messaggio automatico”, dissuadendo così la vittima dal rispondere. Questo elemento è comune nelle comunicazioni ufficiali, quindi aumenta la credibilità dell’email.

**Indizi che Potrebbero Suscitare Sospetti:**

**• Indirizzo Email del Mittente:** Di solito, le email di phishing provengono da indirizzi non ufficiali o con lievi variazioni rispetto all’indirizzo reale della banca.

**• QR Code in Situazioni Insolite:** Le banche raramente usano QR code per verifiche urgenti sui conti. Questo potrebbe insospettire un utente attento.

**• Errore nella URL se si analizza il QR Code:** Un utente esperto potrebbe controllare la URL sottostante e notare che non corrisponde a quella ufficiale della banca.

**Conclusione.**

Questo scenario è progettato per essere convincente e realistico, ma include alcuni segnali di phishing che potrebbero aiutare una persona attenta a identificare l’email come sospetta.

|  |  |
| --- | --- |
|  |  |