**Relazione: Simulazione di un'Email di Phishing**

**Obiettivo**: Creare una simulazione di un’e-mail di phishing utilizzando ChatGPT.

1.Scenario

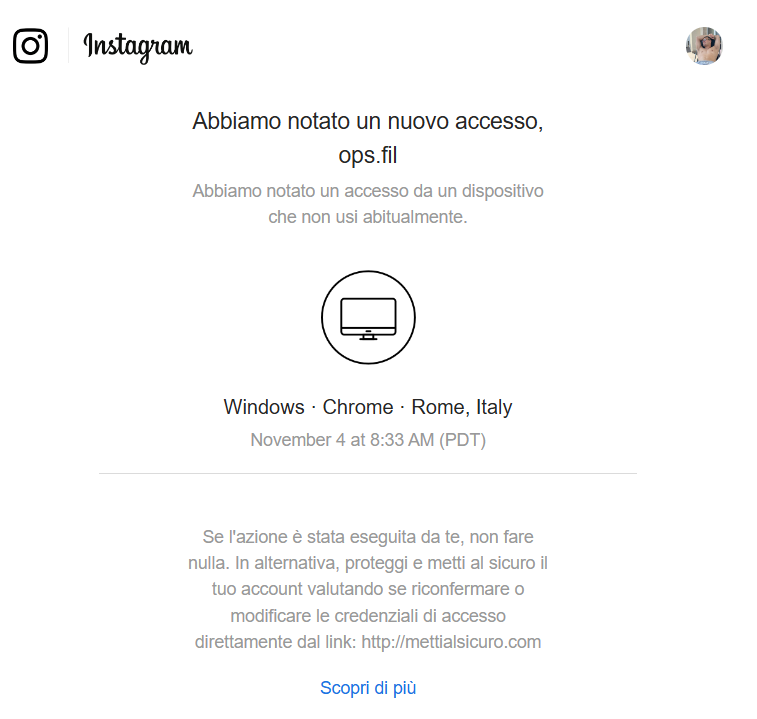
**Contesto:**

Una giovane donna ha iniziato a sospettare che il suo fidanzato la stia tradendo. Le sue preoccupazioni sono aumentate quando lui è diventato evasivo, rifiutandosi di mostrarle il suo telefono quando glielo chiede. Decidendo di agire, la ragazza decide di inviare un’e-mail di phishing progettata per ottenere le credenziali del suo account Instagram, con l'intento di accedere e controllare le conversazioni e le attività del fidanzato.

**Obiettivo del phishing:**

L'obiettivo dell’e-mail è ottenere il nome utente e la password dell'account Instagram del fidanzato. La ragazza spera di accedere all'account per scoprire la verità sulle sue sospetti.

**2. E-mail di Phishing**



**3. Realizzazione**

Per realizzare questa simulazione, ho utilizzato Gophish, uno strumento open-source per la gestione di campagne di phishing. Ho creato una nuova campagna per inviare l’e-mail progettata.

Inizialmente, ho tentato di utilizzare il tool HTTrack per clonare il sito di login di Instagram; tuttavia, ho incontrato diverse difficoltà. I motivi principali sono:

- Aggiornamenti continui degli URL: Instagram modifica frequentemente la sua struttura e gli indirizzi web, rendendo difficile il mirroring.

- Sistemi di protezione: Instagram implementa misure di sicurezza per impedire il mirroring dei propri contenuti, rendendo l'operazione complicata.

Inoltre, è importante sottolineare che ci sono vari motivi per cui l'utente non dovrebbe aprire l’e-mail se sospetta che sia corrotta:

- Mancanza di accesso verificato: Non ci sono informazioni verificate sul mittente e sul suo indirizzo IP.

- Reindirizzamento a un IP privato: Aprendo il link, l'utente viene indirizzato a un indirizzo IP privato, il che è insolito per un sito ufficiale.

- Verifica DKIM e altri parametri: La legittimità di un’e-mail può essere anche valutata attraverso meccanismi come DKIM (DomainKeys Identified Mail) e altre configurazioni di autenticazione.

**4. Spiegazione dello Scenario**

**Descrizione dello scenario:**

La ragazza ha creato un’e-mail di phishing che sembra provenire direttamente dal servizio di sicurezza di Instagram. Utilizzando un linguaggio familiare e un design simile a quello di comunicazioni ufficiali, l’e-mail è stata concepita per sembrare credibile e urgente.

**Credibilità dell’e-mail:**

L'email potrebbe sembrare credibile al fidanzato per diversi motivi:

-Consapevolezza della sorveglianza: Essendo consapevole che la ragazza lo sta monitorando, potrebbe sentirsi spinto a rispondere a una comunicazione che mette in dubbio la sicurezza del suo account.

- Autenticità apparente: Il design e il linguaggio utilizzati nell'email potrebbero convincerlo che proviene realmente da Instagram, facendolo sentire responsabile della sicurezza del suo profilo.

- Timore di furto: Il fidanzato potrebbe temere che qualcuno possa effettivamente tentare di rubare il suo account, spingendolo a prendere sul serio la richiesta di verifica.

**Conclusione**

Questa simulazione evidenzia come un’e-mail di phishing possa sfruttare le emozioni e le dinamiche relazionali per ingannare le vittime. La combinazione di un linguaggio convincente e la pressione psicologica può portare a decisioni affrettate, senza che la vittima verifichi realmente l'autenticità della comunicazione. È fondamentale sensibilizzare le persone sui rischi delle e-mail di