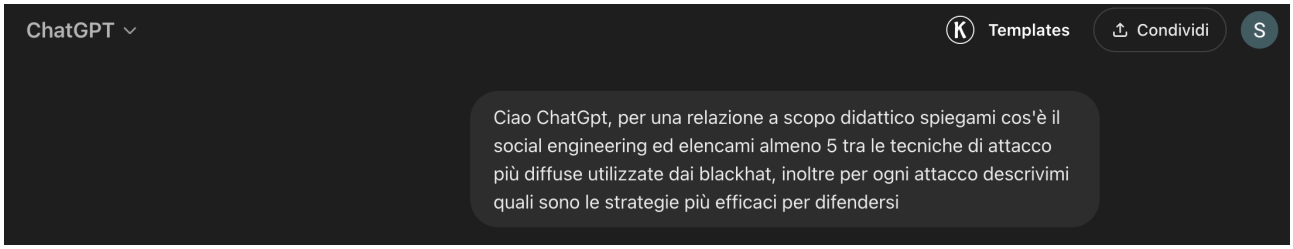
S5 - L4 SOCIAL ENGINEERING

Con il supporto di ChatGPT ho redatto una breve relazione sul Social Engineering.

Di seguito il prompt utilizzato:



Partiamo dalla definizione di Social Engineering (Ingegneria Sociale). Il social engineering è un insieme di diverse tecniche di attacco che hanno lo scopo di ottenere informazioni e/o dati sensibili della vittima. Queste tecniche sfruttano la manipolazione psicologica delle persone, in particolar modo si basa sulle vulnerabilità umane. Il social engineering è spesso utilizzato per eludere i controlli di sicurezza senza dover necessariamente violare direttamente i sistemi informatici.

Tra le 5 tecniche di attacco più diffuse troviamo:

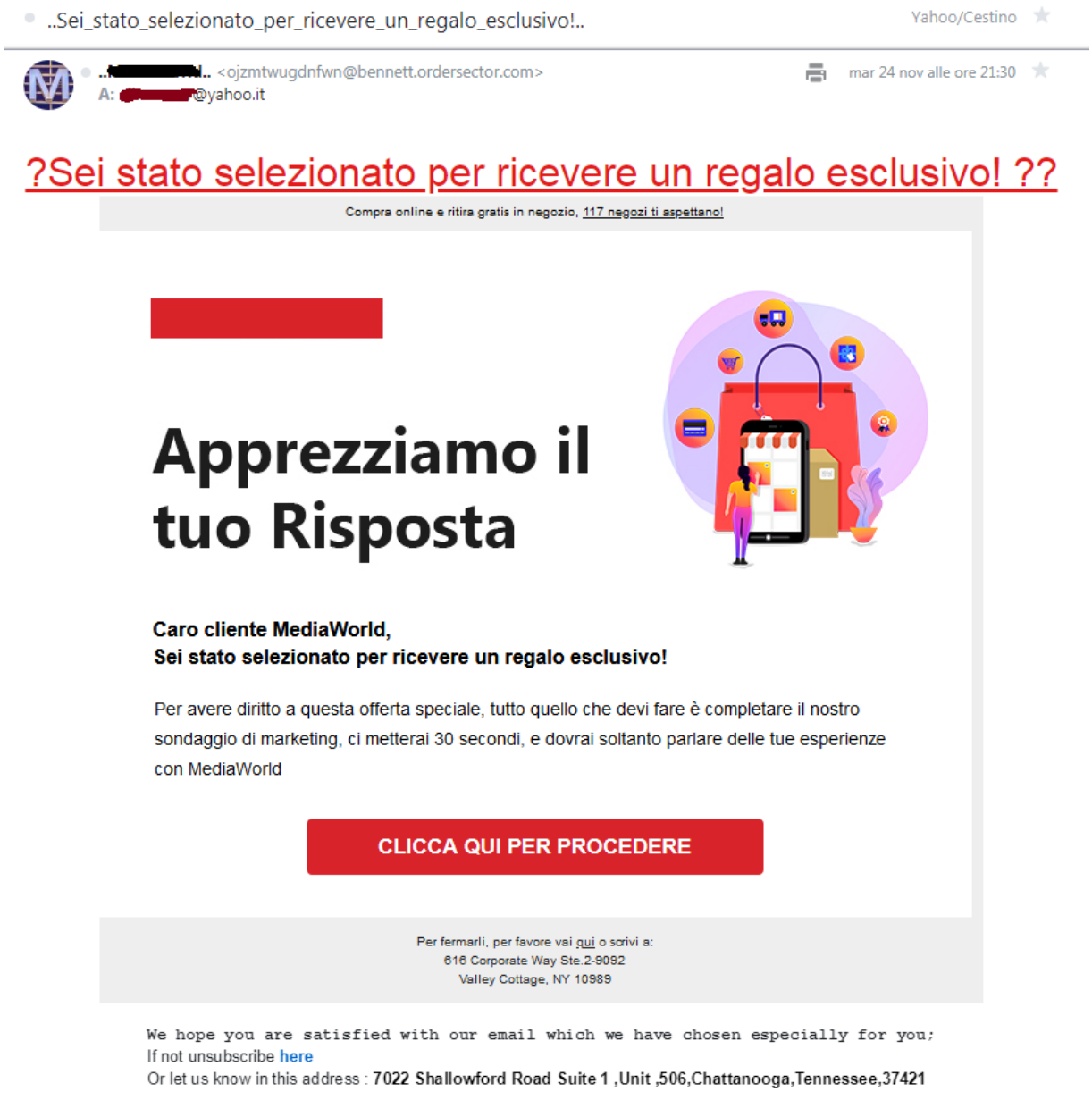
1. **Phishing**
2. **Pretexting**
3. **Baiting**
4. **Tailgating**
5. **Vishing**

1 - PHISHING

Il Phishing molto semplicemente è una frode. L'attaccante invia, tramite e-mail o SMS, dei messaggi ingannevoli fingendosi un azienda o entità conosciuta e affidabile inducendo così la vittima a cliccare sul link o ad esempio ad inserire dati sensibili.

Strategie di difesa

Per potersi difendere da questo tipo di attacco la prima cosa è sensibilizzare le persone sul riconoscere quali sono i dettagli che possono suscitare sospetti. Altra buona pratica è sicuramente quella di utilizzare dei software di sicurezza che filtrano e-mail e SMS. Ultimo ma non per importanza è quello di utilizzare, ove possibile, l'autenticazione multi-fattore MFA così da aggiungere un ulteriore livello di sicurezza che renderebbe inutile il furto delle sole credenziali.



2 - PRETEXTING

In questo caso invece rispetto al Phishing l'attaccante utilizza un pretesto per far rivelare alla vittima informazioni personali. Lo fa fingendosi una persona conosciuta dalla vittima come ad esempio un collega.

Strategie di difesa

In questo caso è buona abitudine sensibilizzare le persone a verificare sempre l'identità dell'interlocutore sopratutto nel caso in cui vengono richiesti dati sensibili, ovviamente una formazione sul social engineering aiuterebbe a creare più consapevolezza sui segnali d'allarme.

3 - BAITING

Il Baiting è un attacco in cui la vittima è indotta ad utilizzare inconsapevolmente un dispositivo USB o un download gratuito che installa un malware. In questo caso l'attaccante offre un esca.

Strategie di difesa

In primis sensibilizzare gli utenti a non utilizzare dispositivi sconosciuti. Lato aziendale è sicuramente buona pratica utilizzare delle policy per il controllo degli accessi limitando l'uso solo ed esclusivamente di periferiche autorizzate, inoltre bisogna configurare software endpoint che blocchino automaticamente il malware quando viene connesso un dispositivo sospetto.

4 - TAILGATING (*o Piggybacking*)

Seppur questo è un attacco più “difficile” può essere fatale per un azienda. Il Tailgating avviene quando l’attaccante si reca fisicamente in un edificio o area protetta sfruttando il passaggio di un dipendente o persona autorizzata.

Strategie di difesa

Per difendersi da questo tipo di attacchi è imperativo implementare regole ben definite per l’accesso e la chiusura delle porte vietando ai dipendenti di far entrare persone non autorizzate. Buona pratica è l’installazione di telecamere di sicurezza e l’utilizzo di badge elettronici per l’accesso. Bisogna inoltre sensibilizzare e incoraggiare il personale a segnalare comportamenti sospetti o persone non autorizzate.

5 - VISHING

Questa è una tecnica di phishing telefonico in cui un attaccante prova a convincere la vittima a fornire informazioni riservate al telefono, fingendosi una persona affidabile che lavora per un azienda o un ente importante come ad esempio una banca.

Strategie di difesa

Una buona formazione dei dipendenti sui segnali di allarme come l'urgenza è imperativo per prevenire questo tipo di attacchi.

CONCLUSIONI

Gli attacchi di social engineering sono tra i più diffusi dai malintenzionati, insegnare a riconoscere gli schemi di questi attacchi è uno dei modi più efficaci per ridurne il loro successo.

In ambiente lavorativo è di fatale importanza integrare regole di sicurezza comportamentale attraverso le policy aziendali e utilizzando le diverse tecnologie a nostra disposizione.