Scenario:

Una dipendente che lavora in amministrazione riceve una mail dalla sua collega (che è in realtà un attaccante) di domenica, quando non è in orario di lavoro. La collega inoltra una mail fittizia apparentemente proveniente dal capo dell'azienda, che sembra molto arrabbiato con l'intero reparto amministrativo. Il capo minaccia di licenziare qualcuno se il problema non viene risolto immediatamente. La collega/attaccante chiede alla vittima di fornire i dati di accesso per risolvere la questione al più presto.

Obiettivo del phishing:
Ottenere le credenziali di accesso della vittima per poter entrare nei sistemi amministrativi dell'azienda.

Email di phishing

Mail reali:

collega-in-real-attaccante@mail.compito

capo-take@mail.compito

Da: collega-in-realtà-attaccante@mail.compito (mail reale: collega-in-real-attacchante.....
A: segretaria-vittima@mail.compito
Oggetto: Fwd: URGENTE – Risolvi subito o ci saranno conseguenze!

Ciao Marianna,

Mi dispiace disturbarti di domenica, ma come puoi vedere dal messaggio che ci ha inviato il capo, la situazione è molto grave. Non riesco a risolvere questo problema da sola e non ho idea dei tuoi dati di accesso sul pc aziendale che utilizzi, pensavo fossero tutti identici, ma evidentemente gli hai cambiati, ti ricordo che è un computer aziendale, e proprio per queste situazioni bisogna comunicare assolutamente se si fanno modifiche di questo genere. Comunque lo chiedo a te e non al capo perché non l'ho mai visto così arrabbiato e non voglio metterti in una situazione scomoda o farti riprendere in questa situazione. Il capo ha detto che se non risolviamo entro oggi, qualcuno perderà il lavoro, e non voglio che nessuno di noi sia nei guai.

Per favore, inviami le tue credenziali così posso entrare subito e risolvere. Grazie mille per la collaborazione, so che è domenica, ma devo sbrigarmi.

Margherita

Inoltro del messaggio del capo:

Da: capo-fake@mail.compito
A: amministrazione@mail.compito
Oggetto: RISOLVERE IMMEDIATAMENTE O LICENZIAMENTO IN VISTA

Buongiorno,

Non sono per nulla soddisfatto di come l'amministrazione ha gestito l'ultima questione con i conti aziendali. C'è stato un errore gravissimo e DEVE essere risolto entro oggi. Se non vedo i risultati subito, qualcuno verrà licenziato. Non ci sono scuse. Non mi importa se è domenica, questo problema è prioritario. Lo sapete che se mi fanno un controllo per un errore del genere mi fanno multe esagerate???

Aspetto una soluzione **IMMEDIATA**.

ELENO
CEO, pishingcorporation s.p.a.

Spiegazione dello scenario

Perché l'email potrebbe sembrare credibile:

1. **Pressione emotiva:** L'inoltro di una presunta email arrabbiata del capo potrebbe creare ansia nella vittima, spingendola ad agire rapidamente per evitare conseguenze gravi come il licenziamento.
2. **Orario non lavorativo:** Essendo domenica, la segretaria potrebbe sentirsi in dovere di rispondere velocemente per evitare problemi al rientro in ufficio il lunedì.
3. **Richiesta diretta:** La collega (in realtà l'attaccante) non chiede esplicitamente soldi, ma semplicemente i dati di accesso, il che potrebbe sembrare una richiesta interna legittima per risolvere un problema aziendale urgente.

Elementi che dovrebbero far scattare l'allarme:

- **Email del capo non professionale:** L'email del capo contiene un tono molto aggressivo e minacce esplicite, cosa che raramente avviene in comunicazioni formali interne.
- **Richiesta di credenziali:** Nessun collega dovrebbe mai chiedere dati di accesso personali via email, specialmente in un contesto di sicurezza.
- **Orario inusuale:** L'invio dell'email fuori dall'orario lavorativo è sospetto, soprattutto se c'è una pressione a risolvere qualcosa immediatamente senza preavviso.

- Questa simulazione mostra come un attaccante possa sfruttare lo stress lavorativo e l'autorità percepita per ottenere accesso non autorizzato ai sistemi aziendali.