**Scenario**

---

Sei un analista della sicurezza presso una società di investimenti chiamata Imaginary Bank. Un dirigente dell'azienda ha recentemente ricevuto un'email di spear phishing che sembra provenire dal consiglio di amministrazione di Imaginary Bank. **Lo spear phishing** è un attacco email dannoso che prende di mira un utente o un gruppo di utenti specifico, apparentemente proveniente da una fonte attendibile. In questo caso, al dirigente viene chiesto di installare un nuovo software di collaborazione, ExecuTalk.

Il dirigente sospetta che questa email possa essere un tentativo di phishing, poiché ExecuTalk non è mai stato menzionato durante l'ultima riunione del consiglio di amministrazione. Hanno inoltrato il messaggio al tuo team per verificarne la legittimità. Il tuo supervisore ti ha incaricato di indagare sul messaggio e stabilire se debba essere messo in quarantena.

**ESEMPIO:**

***a:*** *imaginarybank@gmail.org*

***Inviato:*** *sabato 21 dicembre 2019 15:05:05*

***A:*** *cfo@imaginarybank.com*

***Oggetto:*** *RE: Sei stato aggiunto ai gruppi di un esecutore*

*Conglaturazioni! Sei stato aggiunto al gruppo di collaborazione "Execs".*

*Scarica ExecuTalk sul tuo computer.*

***Mac® | Windows® | Android™***

*Il tuo team ha bisogno di te! Questo invito scadrà tra 48 ore, quindi affrettati.*

*Sinceramente,*

***ExecuTalk©***

*Tutti i diritti riservati.*

**RIFLESSIONE:**

Il primo sospetto deriva dal fatto che l'email proviene dal dominio gmail.org, che non esiste e non è un dominio ufficiale di Google.

**CORPO DALLA MAIL**

*Conglaturazioni! Sei stato aggiunto al gruppo di collaborazione "Execs".*

*Scarica ExecuTalk sul tuo computer.*

***Mac® | Windows® | Android™***

*Il tuo team ha bisogno di te! Questo invito scadrà tra 48 ore, quindi affrettati.*

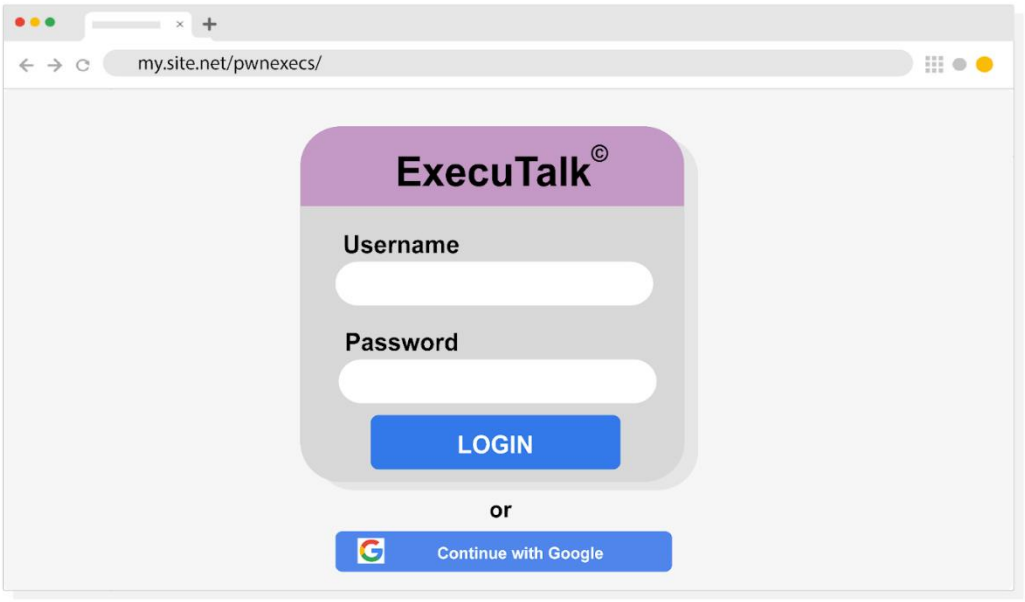
*Sinceramente,*

***ExecuTalk©***

**RIFLESSIONE:**

Dal corpo della mail si nota subito l'errore nella parola *'Congratulazioni'*, che rappresenta già un segnale d'allarme. Inoltre, è evidente il tentativo dell'autore di rendere il messaggio più credibile inserendo finte opzioni di download per i principali sistemi operativi e utilizzando una falsa etichettatura del marchio. Questi elementi, combinati tra loro, indicano un chiaro tentativo di camuffare la natura fraudolenta dell'email.

**LINK DOVE CI HA INDIRIZZZATO LA MAIL**




**RIFLESSIONE:**

Guardando l'URL del sito, si nota subito che manca il protocollo sicuro HTTPS, quindi la connessione non è protetta. Questo è un chiaro segnale di rischio per la sicurezza. Per questo motivo, il sito va considerato potenzialmente pericoloso e conviene evitare di effettuare il login, così da non mettere a rischio i dati aziendali.