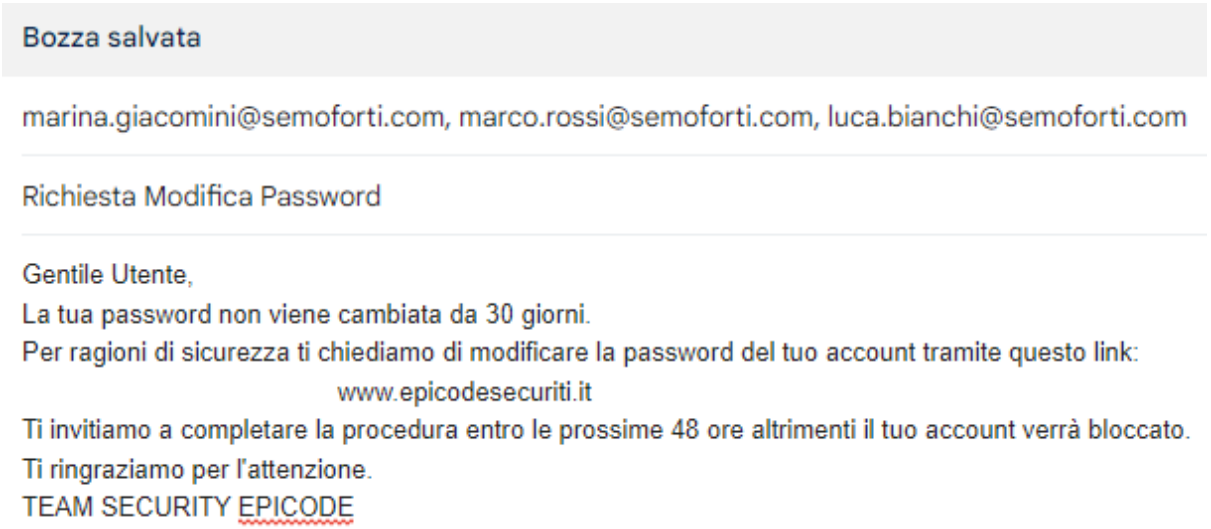
CREAZIONE DI UN PHISHING CONTROLLATO

Dopo il corso di Sicurezza Informatica, il Direttore di Epicodesecurity ci ha chiesto di realizzare un attacco phishing controllato allo scopo di valutare se i dipendenti abbiano appreso le competenze necessarie per riconoscere e gestire un tentativo di phishing.

Ecco come mi sono mosso per attuarlo:

- Per prima cosa, ho analizzato e riflettuto sul tipo di attacco di phishing da utilizzare; dopo un'accurata valutazione, ho deciso di inviare un'e-mail che chiede di cambiare la password attuale con una nuova. In questo falso processo di cambio password, sarebbe stata richiesta la vecchia password. In tal modo, avrei avuto l'opportunità, io come 'Malintenzionato', di accedere agli account aziendali delle vittime.
- Come passo successivo ho preparato l'e-mail


Bozza salvata

marina.giacomini@semoforti.com, marco.rossi@semoforti.com, luca.bianchi@semoforti.com

Richiesta Modifica Password

Gentile Utente,
La tua password non viene cambiata da 30 giorni.
Per ragioni di sicurezza ti chiediamo di modificare la password del tuo account tramite questo link:
www.epicodesecuriti.it
Ti invitiamo a completare la procedura entro le prossime 48 ore altrimenti il tuo account verrà bloccato.
Ti ringraziamo per l'attenzione.
TEAM SECURITY EPICODE

- Ho usato come e-mail del mittente:
  teamitsecurity@semoiforti.com
  aggiungendo al domino una “i” in quel punto per non far dubitare le vittime dell’ e-mail non ufficiale.
  come Link per il login falso ho creato:
  www.epicodesecuriti.it
  Che e molto simile al dominio del azienda.

Nel caso in cui uno dei dipendenti cliccasse sul link e inserisse la sua ‘vecchia password’, avrei ottenuto le credenziali per accedere alla piattaforma, mettendo a disposizione tutti i dati privati.