# Social Engineering – Phishing Mail

L'esercitazione chiede la creazione di una simulazione di email phishing.

- **Scenario**:
  - Contesto: fornitore di riviste digitali (Corriere della Sera, Il Messaggero, ..) ha una clientela ad abbonamento, quindi è necessaria l'iscrizione al portale del fornitore e ovviamente necessita di dati veritieri.
  - Obiettivo: ottenere dati sensibili (credenziali, dati personali, dati finanziari.
  - Pretesto: a seguito di un aggiornamento del sistema informatico , si richiede alla vittima di accedere tramite link proposto nel proprio account per confermare la fruizione di tale tramite aggiornamento dei dati personali e finanziari.
- **Email**:

  Oggetto: Aggiornamento Importante del tuo Account [nome del giornale]

  Corpo: Gentile Cliente [se la campagna è mirata inserire nominativo della vittima, altrimenti lasciare vuoto]

  Ti informiamo che il nostro sistema informatico è stato aggiornato per offrire un'esperienza online migliore, ancor più sicura ed affidabile. A seguito di questo importane aggiornamento, è necessario confermare che il suo account è ancora in uso.

  Per evitare che venga eliminato, ti invitiamo a seguire il link sottostante per aggiornare i suoi dati personali e dayi finanziari entro le prossime 24 ore.
  Questo passaggio di permetterà di continuare a godere del nostro servizio senza problemi; altrimenti il suo account verrà eliminato.

  [link di phishing]

  Grazie per la collaborazione.
  Cordiali saluti,
  Il team di [nome del giornale]

- **ReCap**:
  - Contesto: ho notato che le principali aziende giornalistiche, come Corriere della Sera, il Messaggero ed altre, chiedono a chi ne visita il sito

di accedere e abbonarsi per poter ottenere notizie on diretta ma anche solo per visualizzare online.
Ho pensato di prendere come target la generazione che ha vissuto il cambiamento tecnologico “drasticamente” quindi per stare al passo non comprano più il giornale di carta ma bensi se lo leggono tramite il proprio dispositivo.
L’attacante si immedesima in un’azienda giorjnalistica, contatta la vittima via mail per ottenere i dati personali e i dati finanziari (carte c/c, insomma ogni metodo di pagamento esistente), al fine di farne un uso malevolo.

- Attendibilità e credibilità:
  - Oggetto: L'oggetto "Aggiornamento Importante del tuo Account [nome del giornale]" è generico ma accattivante. Suggerisce un'azione necessaria per mantenere l'account attivo, senza suscitare sospetti immediati.
  - Tono formale: Il tono formale, con frasi come "Gentile Cliente" e "Cordiali saluti", crea un'impressione di professionalità e legittimità.
  - Motivazione plausibile: L'email presenta una motivazione plausibile per l'aggiornamento: migliorare la sicurezza e l'affidabilità del servizio. Questo è un argomento che molte persone trovano importante e accettabile.
  - Urgenza: L'email crea un senso di urgenza, sottolineando la necessità di aggiornare i dati entro 24 ore per evitare la disattivazione dell'account. Questo può spingere le persone ad agire rapidamente senza riflettere troppo.
  - Link di phishing: Il link di phishing è presentato come un'azione necessaria per completare l'aggiornamento. Questo può sembrare logico e naturale, soprattutto se la vittima è già abituata a cliccare sui link nelle email.

- Campanello d’allarme:
  - Urgenza: L'email mette in evidenza un'urgenza eccessiva, minacciando la disattivazione dell'account se non si agisce entro 24 ore. Le aziende affidabili raramente impongono scadenze così brevi per azioni importanti.
  - Richiesta di informazioni personali: L'email chiede di aggiornare i "dati personali e dati finanziari" tramite un link esterno. Le aziende legittime non richiedono mai informazioni sensibili tramite email.

- Link sospetto: Il link fornito nell'email non è un URL riconoscibile e non è collegato al sito web ufficiale del giornale. Un'azienda affidabile non userebbe un link esterno per questo tipo di aggiornamento.
- Errori grammaticali: L'email presenta alcuni errori grammaticali, come "dayi finanziari" invece di "dati finanziari" e "Questo passaggio di" invece di "Questo passaggio". Le aziende affidabili prestano molta attenzione alla grammatica e all'ortografia nelle loro comunicazioni.
- Mancanza di dettagli specifici: L'email non fornisce dettagli specifici sull'aggiornamento, come ad esempio la natura dell'aggiornamento o il motivo per cui è necessario aggiornare i dati. Le aziende affidabili sono chiare e trasparenti nelle loro comunicazioni.