# PROGETTO S3 L5

Davide Andreozzi

# Introduzione

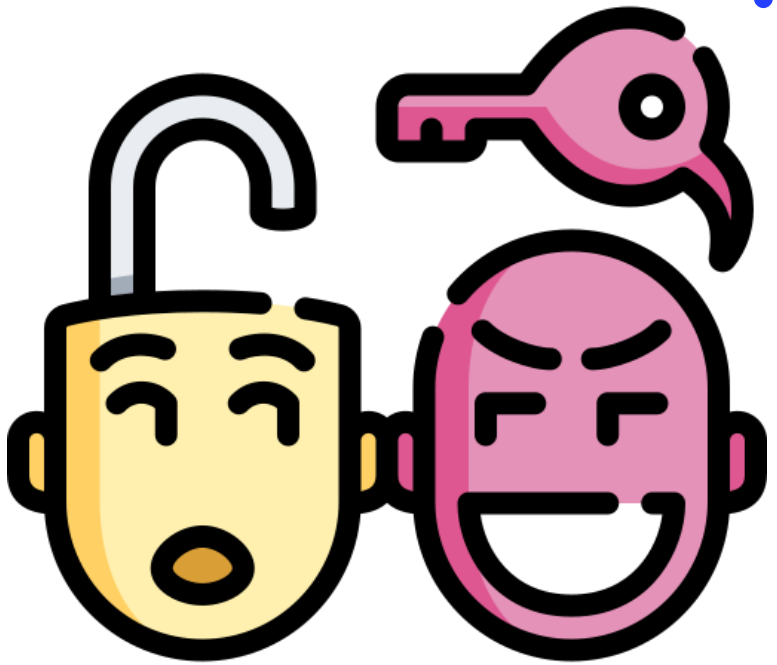
Siete stati chiamati da un'azienda di nome Epicodesecurity.

Questa azienda ha un sito web suo personale con il nome di dominio www.Epicodesecurity.it. un server email con l'email aziendale Epicodesecurity@semoforti.com

- Il vostro ruolo è quello di spiegare e informare i dipendenti dell'azienda Epicodesecurity sui rischi di attacchi di ingegneria sociale, in particolar modo contro il phishing.
- Come impostate la formazione? (spiegare cos'è il phishing ).
- Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?( quali parametri vedere per identificarlo. Esempio: SPF).

Il direttore vi dà il permesso di creare un phishing controllato.

- Descrivere come agireste.
- L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.



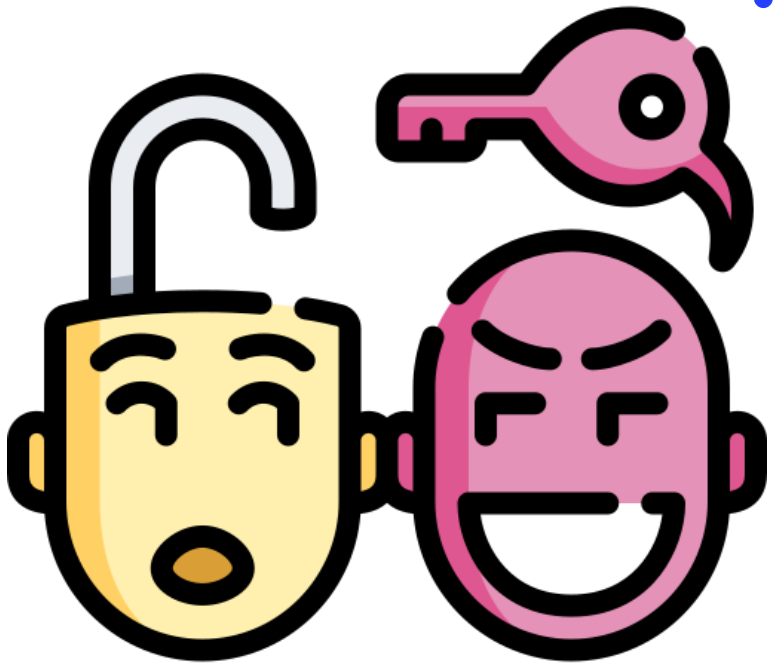
# Ingegneria Sociale

Andremo a organizzare dei corsi formativi per i dipendenti sui rischi dell'ingegneria sociale.

Cos'è l'ingegneria sociale?
Per Ingegneria Sociale si intende l'insieme di attacchi informatici che sfruttano la persona come punto di vulnerabilità per l'accesso a sistemi informatici, informazioni personali, dati di accesso, ecc.

L'ingegneria sociale si concentra sulla manipolazione e persuasione psicologica dell'individuo.
Una delle tecniche più diffuse e in continua evoluzione da parte dei criminali informatici è il phishing.

Vedremo nella successiva slide cos'è.



# Phishing

Il Phishing è una delle forme più utilizzate di attacco nell'ingegneria sociale

L'attacco di solito si concentra sul presentarsi come entità legittime o persone fidate e trarre in inganno la vittima per farsi rivelare informazioni sensibili.

Una delle forme più utilizzate di phishing è l'invio di email che a primo impatto possano sembrare inviate da fonti affidabili.
Facciamo un esempio:

Una mail inviata apparentemente dal nostro istituto bancario che ci chiede di controllare un accesso insolito o non autorizzato.

In questo caso l'utente poco consapevole cliccando sul link nella mail (che ricorderà in tutto o quasi l'istituto legittimo) potrebbe scaricare codice «infetto» oppure essere rimandato a un sito clonato del proprio istituto bancario dove gli viene chiesto di accedere per bloccare l'accesso non autorizzato.

Inserendo le informazioni di accesso, esse verranno viste dal criminale informatico che le userà di sicuro per scopi abbastanza ovvi, come  lo svuotamento del conto corrente in questo caso.

# Esempi di Phishing

**Posteitaliane**

**Gentile Cliente ,**

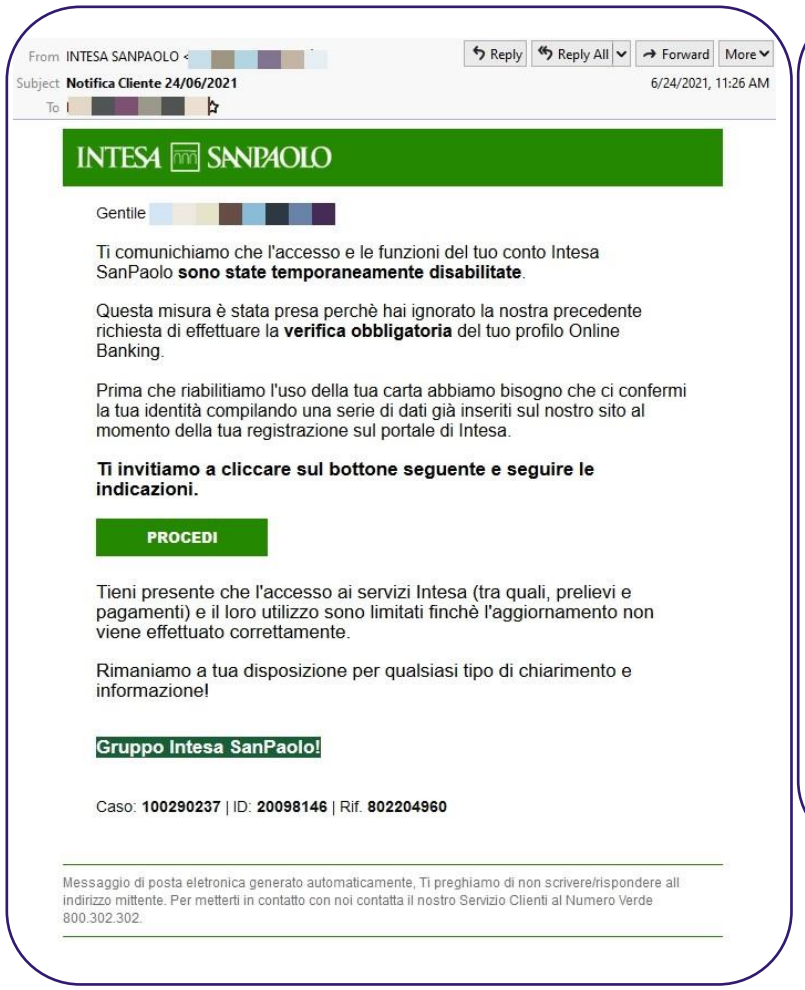
Abbiamo notato dell'attività insolita nella sua carta
Il suo accesso al portale carte titolari è stato temporaneamente bloccato per la sua tutela

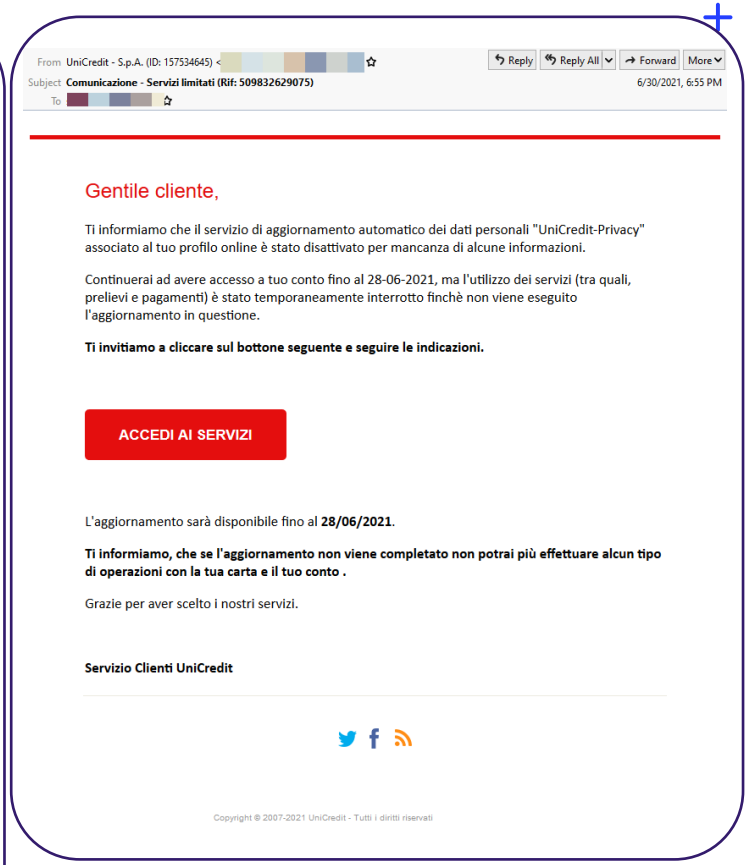
Si prega di confermare la propria identità attraverso il nostro collegamento sicuro

Accedi a collegamento sicuro

*Grazie*

*Per favore, non rispondere a questa e-mail.*



# Come difendersi

Bisogna sempre controllare il corpo della mail, analizzare dettagli come errori di ortografia, loghi sbagliati o richieste particolarmente sospette (info sensibili).

- Verifica le fonti

- Utilizza metodi di accesso con autenticazione multifattoriale:

si ha un In questo modo anche se le credenziali di accesso verranno scoperte ulteriore grado di sicurezza e si può limitare/evitare un danno maggiore.

- Analizzare il codice dell'email sul vostro client di posta elettronica

in particolare verificare se il mittente sia effettivamente chi dice di essere analizzando l'ortografia della mail del mittente e il nome del dominio se corrisponde con quello legittimo.

- Controllare in particolare i filtri: **SPF**, **DKIM**, **DMARC**.

SPF: Verifica che l'indirizzo IP che invia un'email sia autorizzato a farlo per conto del dominio specificato.

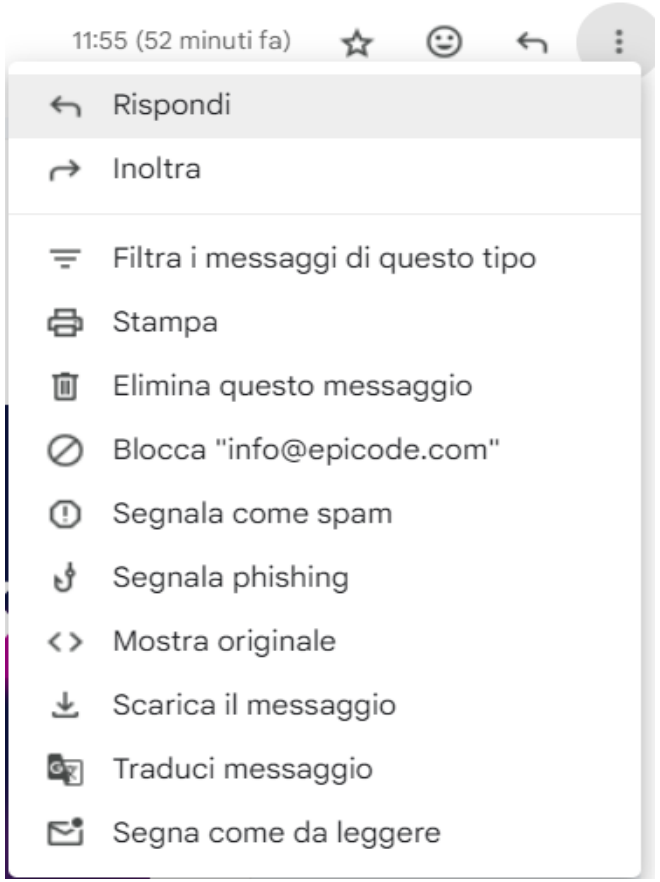
DKIM: Garantisce l'integrità e l'autenticità del contenuto di un'email mediante la firma digitale

DMARC: unisce SPF e DKIM, richiedendo che entrambi siano autenticati correttamente o che nessuno dei due sia superato.

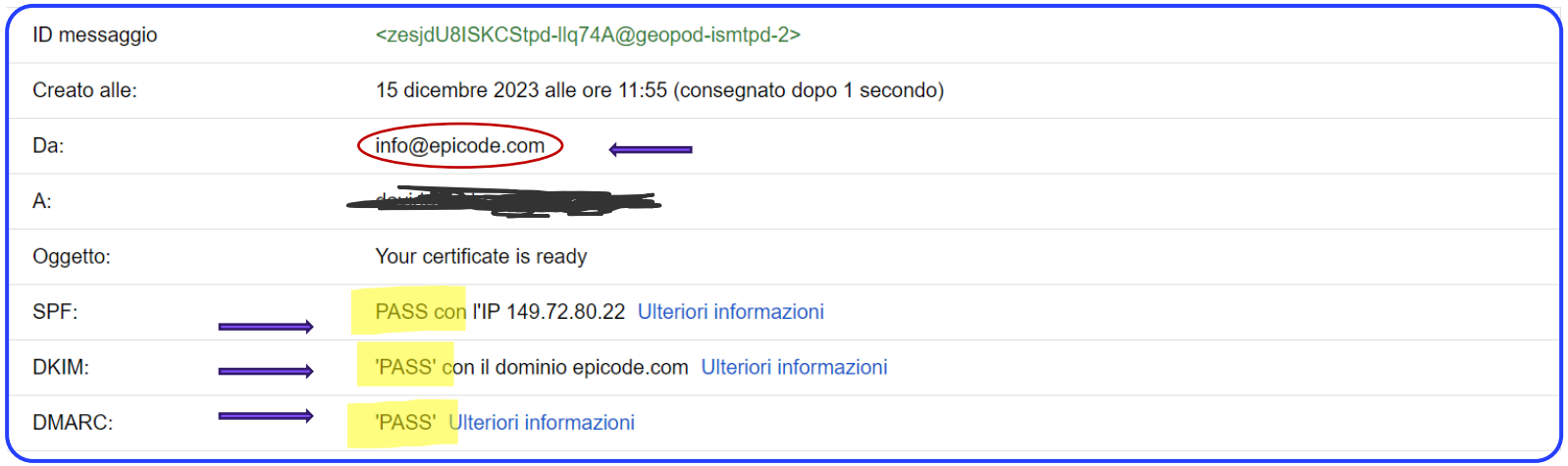
# Come difendersi

Su Gmail, all'interno della mail possiamo andare sui 3 pallini che si trovano a destra e tramite il menu cliccare su «Mostra originale.

Questo è il modo per aprire il codice del messaggio originale per poterne analizzare il contenuto



# Come difendersi




Questo spazio include il mittente del messaggio e da lì possiamo verificare se sia sospetto oppure autentico perché ne conosciamo dominio
SPF – DKIM – DMARC: Tutti su PASS. Quindi possiamo considerare la mail attendibile.
Inoltre possiamo anche verificare il codice sottostante alla schermata e vedere eventuali link se siano sicuri o meno.

# Come difendersi

- Nel caso sottostante il pulsante «Gestisci le tue app» riporta al link evidenziato. Questo può essere utile perché ci fornisce esattamente la destinazione del pulsante quando lo andiamo a cliccare.

```
bottom: 5px; padding-left: 20px; min-width:50px;"><a id="i5" style="font-family: 'Segoe UI Semibold', 'Segoe UI Bold', 'Segoe
Medium', Arial, sans-serif; font-size:14px; text-align:center; text-decoration:none; font-weight:600; letter-spacing:0.02em;
href="https://account.live.com/consent/Manage?fn=email">Gestisci le tue app</a></td></tr></table>
      </td></tr>
      <tr><td id="i6" style="padding:0; padding-top:25px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-si
```

# TEST PHISHING

Andremo successivamente a testare previa autorizzazione del direttore la vulnerabilità al phishing dei dipendenti.

# Testing

Definiamo innanzitutto la mail mittente «fake», in questo caso essendo la legittima epicodesecurity@semoforti.com utilizzeremo:

- epicodesecurity@semforti.com (molto simile a quella legittima)

Definiamo successivamente la strategia da mettere in atto.

- Vogliamo che i nostri target vadano su un sito esca (epicodesecurty.it) dove loro inseriranno le credenziali di accesso al portale aziendale, possiamo usare come pretesto un possibile problema di sicurezza e indurli al reset password entro una data stabilita altrimenti non avranno accesso al portale aziendale.

# Testing

Creiamo la mail esca utilizzando font, loghi e template che di solito utilizza l'azienda e la inviamo a tutti i dipendenti target.

*Ciao nome_cognome,*

*Abbiamo avuto dei problemi di sicurezza nella nostra infrastruttura di rete ed è necessario che ogni dipendente provveda immediatamente al reset della password che è stata compromessa.*

*Cliccando qui (Inserimento link a pagina fake) potrai accedere al portale aziendale tramite le tue credenziali e cambiarle con delle nuove cliccando su «resetta la password».*

*Una volta eseguito questa azione la procedura è completata.*

*La procedura deve essere effettuata entro 7 giorni dalla ricezione della presente mail, altrimenti l'utenza sarà bloccata fino al reset della password.*

*La sicurezza di EpicodeSecurity è una priorità.*

*Ti ringraziamo per la comprensione*

*Nome_Cognome (Responsabile Team Security)*

*Team  Security*

*EpicodeSecurity*

Scaduto un tempo massimo andremo ad analizzare il test phishing che abbiamo effettuato e produrremo un report da consegnare al direttore per verificare il livello dei propri dipendenti nel contrastare il phishing

*Per il test di Phishing è stato utilizzato GoPhish*

# Sequenza temporale