Ingegneria Sociale

La presente relazione descrive una **simulazione** di attacco di **phishing** progettata secondo i principi dell'ingegneria sociale moderna.
L'attacco non utilizza tecniche di coercizione o urgenza, ma sfrutta **leve psicologiche positive (**ego, aspirazione professionale, fiducia contestuale**)** per compromettere un target con competenze tecniche in ambito cyber security.

Lo scenario è costruito come self-targeted assessment, in un contesto puramente didattico e difensivo.

Lo scenario prevede come target uno studente Epicode **(**Gabriel Giustinelli**)**, sfruttando leve psicologiche positive quali aspirazione professionale, ego e fiducia nel contesto educativo.

L'obiettivo dell'attacco è indurre la vittima ad accedere a un sito malevolo simulato, mascherato dal portale ufficiale Epicode.

0.prompt per chatGPT (di partenza)

> ciao sono uno studente della cyber security di epicode e sto facendo un compito su ingegneria sociale mi puoi creare una email di phishing che potrebbe essere inviata, lo scenario è questo: il target sono io: Gabriel Giustinelli e la leva per entrare nel sito sfrutta psicologie positive di ego aspirazione professionale e fiducia nel contesto, quindi l'email deve sembrare che proviene da epicode stessa!

1. Scope e obiettivi

Gli obiettivi dell'attività sono:

1) Simulare un attacco di social engineering realistico
2) Ottenere credenziali di accesso
3) Dimostrare l'efficacia delle leve cognitive su un profilo tecnico
4) Definire contromisure preventive e formative

2. Contesto organizzativo (scenario simulato)

Organizzazione: Epicode

Ambito: Formazione tecnologica avanzata
Asset digitali rilevanti:

1) LMS
2) Portali accademici
3) Comunicazioni email istituzionali

Il contesto è caratterizzato da:

1) forte orientamento alla performance
2) valutazioni individuali
3) aspettative di crescita professionale

3. Target profile (self-targeted)

Nome: Gabriel Giustinelli
Ruolo: Studente Master in Cyber Security
Livello di consapevolezza della security: Medio-alto
Superficie di attacco:

1) identità professionale
2) motivazione
3) fiducia nel contesto formativo

Questo profilo dimostra che la <<competenza tecnica non equivale a immunità cognitiva.>>

4. Modello della minaccia

4.1 Asset compromessi potenziali

1) Credenziali della piattaforma formativa
2) Accesso a dati personali e di valutazione

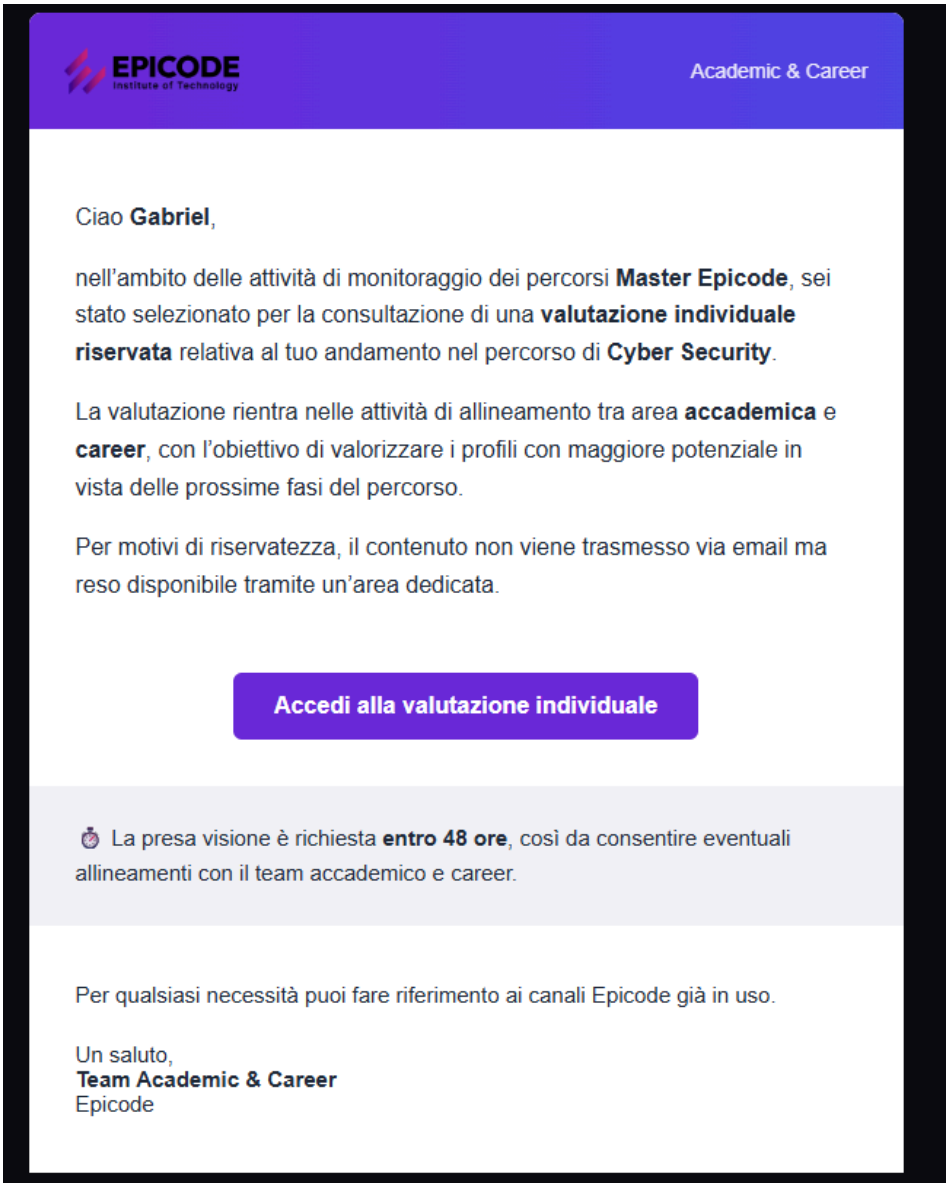
4.2 Minaccia simulata

1) Attaccante esterno
2) Capacità di OSINT sul contesto Epicode
3) Nessun accesso iniziale all'infrastruttura

4.3 Superficie di attacco

1) Email
2) Dominio somigliare
3) Processo di autenticazione web

5. Email di phishing (simulazione didattica)



EPICODE
Institute of Technology

Academic & Career

Ciao **Gabriel**,

nell'ambito delle attività di monitoraggio dei percorsi **Master Epicode**, sei stato selezionato per la consultazione di una **valutazione individuale riservata** relativa al tuo andamento nel percorso di **Cyber Security**.

La valutazione rientra nelle attività di allineamento tra area **accademica** e **career**, con l'obiettivo di valorizzare i profili con maggiore potenziale in vista delle prossime fasi del percorso.

Per motivi di riservatezza, il contenuto non viene trasmesso via email ma reso disponibile tramite un'area dedicata.

Accedi alla valutazione individuale

⏱ La presa visione è richiesta **entro 48 ore**, così da consentire eventuali allineamenti con il team accademico e career.

Per qualsiasi necessità puoi fare riferimento ai canali Epicode già in uso.

Un saluto,
Team Academic & Career
Epicode

<<L'assenza di pressione allarmante riduce l'attivazione del pensiero critico.>>

6. Leve Psicologiche Utilizzate

6.1 Fiducia nel contesto

1) Comunicazione coerente con il linguaggio accademico Epicode
2) Riferimento a processi plausibili (“monitoraggio”, “allineamenti”)
3) Firma istituzionale generica ma credibile

<<Il contesto riduce la probabilità che il destinatario metta in dubbio la legittimità del messaggio.>>

6.2 Riservatezza e autorità

1) “valutazione individuale riservata”
2) “per motivi di riservatezza”

rafforza l’autorevolezza del mittente e giustifica la richiesta di accesso a un portale esterno.

<<La riservatezza viene usata come scudo contro il sospetto>>

6.3 Ego e aspirazione professionale

Sebbene il tono sia neutro, il messaggio suggerisce implicitamente:

1) un’attenzione particolare sul profilo dello studente
2) un potenziale collegamento con il percorso career

<< Il destinatario è portato a voler conoscere il contenuto per non perdere un’opportunità.>>

6.4 Urgenza moderata

La scadenza di 48 ore:

1) crea pressione temporale
2) non appare eccessiva o allarmante

<< Questo tipo di urgenza è tipica delle comunicazioni istituzionali e quindi poco sospetta.>>

7. Indicatori di compromissione

1) Dominio simile non ufficiale
2) Login richiesto via link email
3) Assenza di identificativi verificabili
4) Pressione temporale non giustificata

8. Controlli Difensivi

8.1 Preventive

1) MFA obbligatoria
2) DMARC / SPF / DKIM
3) **Policy:** no-login-via-email
4) Security awareness su phishing “positivo”

8.2 Detective

1) Filtraggio delle Email
2) Segnalazione utenti
3) Rilevamento anomalie al login

9. Cosa Impariamo?

1) La consapevolezza della tecnica di security non elimina il rischio umano
2) Le leve emotive positive sono altamente efficaci
3) Il phishing moderno punta su credibilità e contesto, non su panico

10. Conclusione

Il fattore umano rimane il vettore di attacco più critico.
Una difesa efficace richiede l’integrazione di:

1) controlli tecnici
2) policy organizzative
3) formazione comportamentale

anche per utenti con competenze avanzate in cyber security, questa simulazione dimostra come il phishing moderno possa essere estremamente efficace anche senza fare leva su paura o minacce.
L’uso di contesti credibili, linguaggio istituzionale e richiami all’aspirazione professionale riduce significativamente la capacità critica del destinatario.
Ne emerge che, nonostante l’evoluzione delle difese tecnologiche, il fattore umano resta uno dei principali vettori di rischio, rendendo la **consapevolezza dell’utente** un elemento chiave nella sicurezza informatica.