ESERCIZIO S5 L5

SOCIAL ENGINEERING: EMAIL REDDITO DIGITALE UNDER 35

1. Idea dell'attacco

La tecnica che ho scelto è il **phishing** tramite **email istituzionale falsificata**, sfruttando il nome dell'**Unione Europea** e una tematica attuale e sensibile: **un presunto sussidio economico per i giovani sotto i 35 anni** chiamato *Reddito Digitale Europeo*.

L'attacco si basa sulla manipolazione della fiducia da parte delle istituzioni pubbliche e sull'**urgenza** di aderire a un'opportunità **esclusiva** e **temporanea.**

2. Scelgo il Target

- **Giovani tra i 18 e i 35 anni**, cittadini dell'Unione Europea, con interesse per:

  Opportunità di guadagno online;

  Programmi di sostegno economico;

  Forme di reddito passive

- In particolare: studenti universitari, giovani disoccupati o lavoratori precari, neolaureati.

Sono i soggetti potenzialmente più esposti perché sono spesso in cerca di opportunità, meno attenti a verificare le fonti ufficiali, e fortemente attratti da iniziative digitali e "semplici" da ottenere.

3. Canali utilizzati

- **Email** con finto dominio istituzionale simile a quello europeo (`info@europa-program.eu`)

- Supporto da una landing page che simula un portale europeo con dominio ingannevole dove registrarsi: https://europa-program.eu/reddito-digitale/registration

4. E-MAIL

Oggetto: NextGenerationEU: Contributo europeo fino a 1080€ per Under 35

Mittente:
Commissione Europea – NextGenerationEU <info@europa-program.eu>

Gentile cittadino,

Dal giorno 26/07/2025 è entrata in vigore l'iniziativa NextGenerationEU. Si tratta di un contributo mensile chiamato **Reddito Digitale Europeo**, riservato ai giovani tra i 18 e i 35 anni.

L'obiettivo è fornire un sostegno economico concreto ai giovani, favorendo la loro formazione e facilitando l'ingresso stabile e qualificato nel mercato del lavoro europeo.

Hai tempo fino al 3 agosto 2025 per inoltrare la tua domanda.

Clicca qui per accedere alla piattaforma di registrazione:
https://europa-program.eu/reddito-digitale/registration

Guida alla registrazione

Step 1: Inserisci i tuoi dati anagrafici

Step 2: Allega Fronte / Retro della tua carta d'identità

Step 3: Seleziona tra "studente"-"neolaureato"-"neodiplomato"-"disoccupato"

Step 4: Inserisci il tuo IBAN

Step 5: Inserisci la tua e-mail che sarà utilizzata per tutto il processo

Attenzione: Inserire una e-mail reale poichè il sistema invierà un *link di conferma.*

I fondi verranno erogati entro **10 giorni** dall'approvazione della candidatura.

L'adesione è gratuita, ma **i posti sono limitati**.

ATTENZIONE: ***la mancata presentazione entro il termine comporterà l'esclusione automatica.***

Cordiali saluti,
Commissione Europea – NextGenerationEU

---

5. Obiettivo dell'attacco

L'obiettivo principale è **ottenere dati sensibili** e **compromettere le credenziali** della vittima. In particolare:

- Dati anagrafici e identificativi (nome, cognome, data di nascita, codice fiscale)
- Documenti di identità caricati sulla piattaforma fasulla
- Credenziali email, password, IBAN o dati bancari

Con questi dati l'attaccante può:

- Avviare furti d'identità
- Creare account fittizi
- Accedere a servizi finanziari a nome della vittima

6. Perché è efficace

- **Autorità percepita**: il mittente fittizio è la Commissione Europea, che gode di altissima credibilità.

- **Tempismo**: l'email è inviata in un momento strategico (es. inizio mese o prima di ferie), quando molte persone sono economicamente vulnerabili.

- **Urgenza**: il termine di scadenza spinge l'utente ad agire impulsivamente senza riflettere.

- **Emozione**: fa leva su speranza e fiducia, con promessa di un aiuto economico concreto e immediato.

- **Realismo**: la struttura dell'email, la grafica del sito, il linguaggio istituzionale e il dominio simile a quello reale la rendono molto difficile da distinguere da una comunicazione legittima.

CONCLUSIONE

La mail utilizza diverse tecniche di manipolazione psicologica tipiche del phishing, sfruttando la **fiducia nell'istituzione** (Commissione Europea), **l'urgenza temporale** (scadenza ravvicinata) e **la promessa di un beneficio** concreto e desiderabile (contributo economico).

Ho cercato di comunicare con un tono **formale e dettagliato**, elementi che aumentano la credibilità e riducono i sospetti del destinatario. Inoltre, **la suddivisione in step** chiari guida l'utente lungo una procedura apparentemente semplice e legittima, facilitando l'adesione al messaggio.

Queste strategie non sono limitate a un solo tipo di phishing ma sono adattabili a molteplici contesti, dal settore finanziario alle iniziative sociali, bandi aziendali ed altro.

L'obiettivo comune è sempre quello di creare una combinazione efficace di pressione psicologica e rassicurazione, spingendo la vittima a **compiere azioni impulsive**, come cliccare su link malevoli o fornire dati sensibili.

Comprendere queste tecniche è fondamentale per riconoscere e difendersi da attacchi sempre più sofisticati, poichè il phishing si adatta a nuovi temi e scenari, sfruttando il **contesto sociale** e **culturale del momento**, come in questo caso il tema del denaro. Questa esercitazione come questo mi ha permesso di affinare la mia creatività,la mia capacità critica e di sviluppare contromisure efficaci e di riconoscimento rispetto ai tentativi di phishing che incontrerò in futuro.