CYBERTRIALS 2025

PROGRAMMA

16/04/2025

h. 17:30-19:00

SOCIAL ENGINEERING

29/04/2025

h. 17:30-19:00

WEB E NETWORK

06/05/2025

h. 17:30-19:00

CRYPTO

20/05/2025

h. 17:30-19:00

OSINT

Sonja Caramagno

Ilaria Matteucci

Sonia Montegiove

Veronica Roccato

Anna Vaccarelli

All’evento finale saranno ammesse le 100 partecipanti che, al termine del percorso formativo avranno conseguito il punteggio più alto.

12-15 giugno 2025
311 Verona
FINALI NAZIONALI

Per tutti è previsto vitto e alloggio in strutture della città. Gli spostamenti da e per il Campus dovranno essere organizzati in autonomia da tutte le partecipanti che saranno rimborsati successivamente a fronte ti una pezza giustificativa (biglietto, scontrino, ecc.)

Durante la prima giornata del campus le partecipanti saranno suddivise in 20 team.

PCTO

Le partecipanti che prenderanno parte alla finale di CyberTrials riceveranno un attestato per i crediti PCTO dipendente dall’effettiva partecipazione alle attività proposte durante l’evento finale per un totale massimo di 44 ore.

Le ore verranno conteggiate in questo modo:

- 4 ore per ogni argomento formativo (lezione frontale, training e challenge)
- 28 ore camp in presenza

Le partecipanti squalificate o che abbandonano il programma anticipatamente non riceveranno crediti PCTO.

Per maggiori informazioni sulla convenzione scrivere a pcto@cybersecnatlab.it.

Non siete sole! ;)

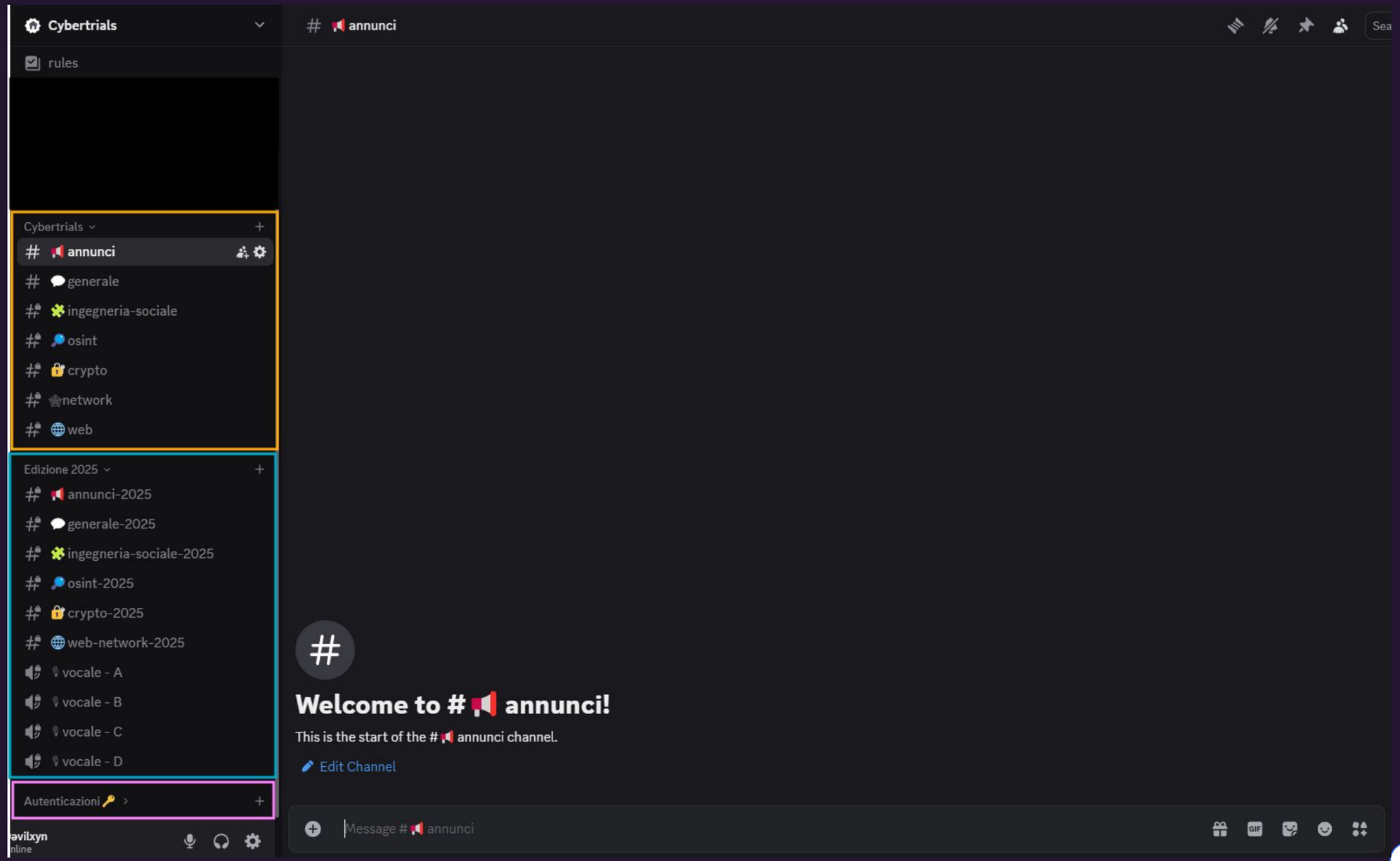
Sofia Bagnoli

Alice Mandaliti

Rebecca Todisco

Arianna Urciuoli

Il canale Discord



L'Arte dell'Inganno: Social Engineering

L'Arte dell'Inganno: Social Engineering

L'ingegneria sociale è la combinazione di tecniche sociologiche, psicologiche e di raccolta di informazioni utilizzate per manipolare le persone con l’obiettivo di:

1. Convincerle a rilasciare informazioni sensibili
2. Compiere azioni che non rispettino le normali misure di sicurezza
3. Farle agire in maniera tale da consentire l’accesso o l’uso non autorizzato di sistemi, reti, dati, autorizzazioni

L'Anello Debole: Il Fattore Umano

In ambito di ingegneria sociale, l'espressione "anello debole" si riferisce al **fattore umano** all'interno della catena di sicurezza informatica. Nonostante l'adozione di tecnologie avanzate come firewall, crittografia e sistemi di autenticazione multifattoriale, gli esseri umani rimangono il punto più vulnerabile.

Fiducia, fretta e ignoranza sono le vulnerabilità più sfruttate.

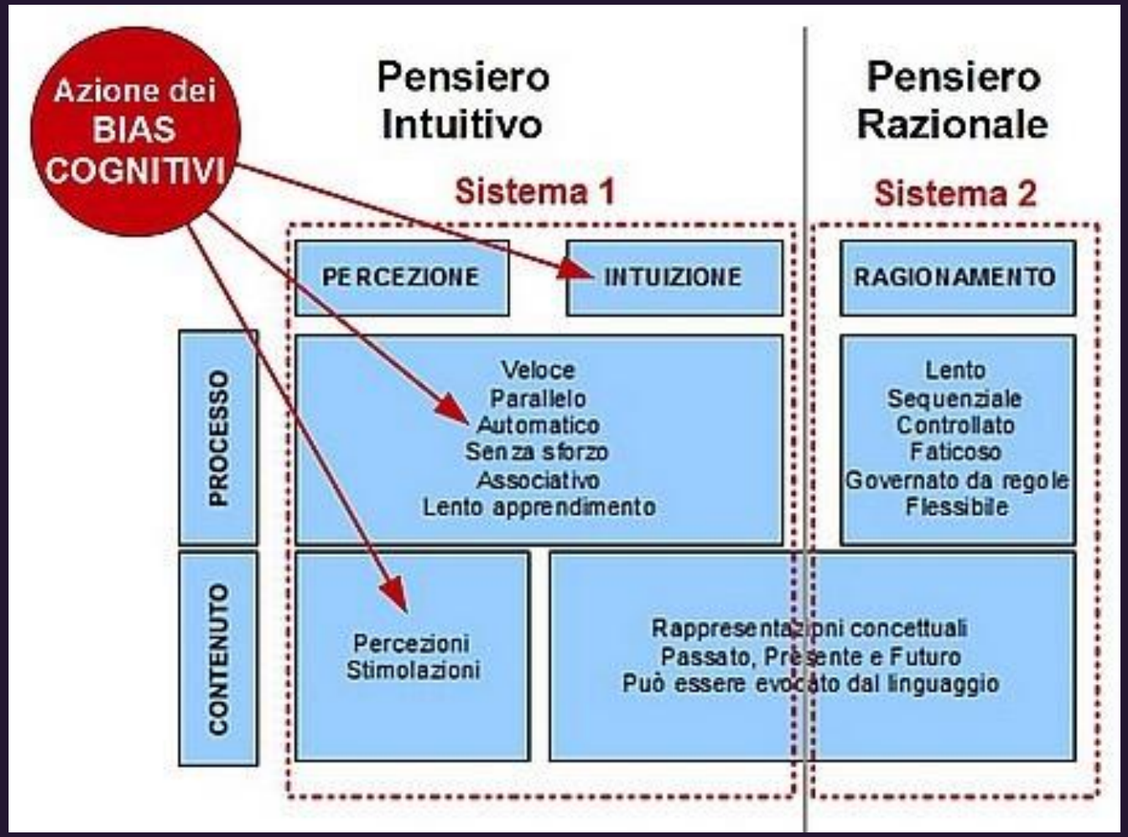
Teoria del doppio processo- Daniel Kahneman

Il processo decisionale è influenzato dall'interazione di due sistemi

SISTEMA 1 (INTUITIVO)
Opera in modo automatico, è veloce, non richiede sforzo cogitivo, è sempre al lavoro e attivo

SISTEMA 2 (ANALITICO)
Si attiva di fronte ad attività mentali impegnative, è lento, richiede maggiore sforzo cognitivo, la capacità di mantenerlo attivo si esaurisce facilmente

Solitamentte il nostro cervello utilizza il sistema 1 in quanto meno dispendioso di energie.



Cosa Sono i Bias Cognitivi?

Scorciatoie Mentali

I bias cognitivi sono "filtri", pregiudizi che il nostro cervello usa per semplificare le decisioni.

Vulnerabilità Prevedibili

I truffatori conoscono questi meccanismi e li sfruttano per manipolarci.

Bias Cognitivi Chiave nella Social Engineering

Principio di Autorità

Tendenza a obbedire a figure autoritarie

Riprova Sociale

Imitare il comportamento degli altri

Scarsità

Paura di perdere opportunità limitate

Simpatia

Aiutiamo più facilmente chi ci piace

Principio dell'Autorità

Impersonificazione IT

Attaccanti che fingono di essere tecnici informatici per ottenere accesso a sistemi protetti.

Falsi Manager

Il 92% delle persone obbedisce a ordini provenienti da figure autoritarie senza verificare.

Autorità Istituzionali

L'impersonificazione di forze dell'ordine genera immediata fiducia nelle vittime.

ESEMPIO:

Marco riceve una telefonata da una donna che si presenta come “Dott.ssa Bianchi dell’Agenzia delle Entrate”. La sua voce è ferma, professionale. Gli dice che ci sono delle incongruenze fiscali e che, per risolverle rapidamente evitando un’ispezione, deve inviare subito alcuni documenti riservati via email.

Meccanismo: L’attaccante sfrutta il rispetto (o la paura) verso figure autoritarie per spingere all’azione, saltando il pensiero critico.

Principio della Simpatia

Complimenti

Lusinghe per abbassare le difese della vittima.

Interessi Comuni

Finta condivisione di passioni per creare connessione emotiva.

Somiglianze

Evidenziare similitudini per generare un senso di appartenenza.

Le ricerche dimostrano che una richiesta viene accettata nel 65% dei casi quando esiste un rapporto di simpatia tra le persone.

ESEMPIO:

Giulia riceve un messaggio su LinkedIn da Luca, che ha interessi simili ai suoi e un profilo amichevole. Iniziano a chattare. Dopo giorni di conversazioni piacevoli, Luca le chiede un piccolo favore: può inoltrare una mail a un collega, “tanto è solo una presentazione”?

Meccanismo: L’attaccante costruisce una relazione positiva e simpatica per abbassare le difese della vittima.

Principio della Scarsità

78%

Attacchi Phishing

Utilizzano tattiche di scarsità secondo il Rapporto Clusit 2023.

24h

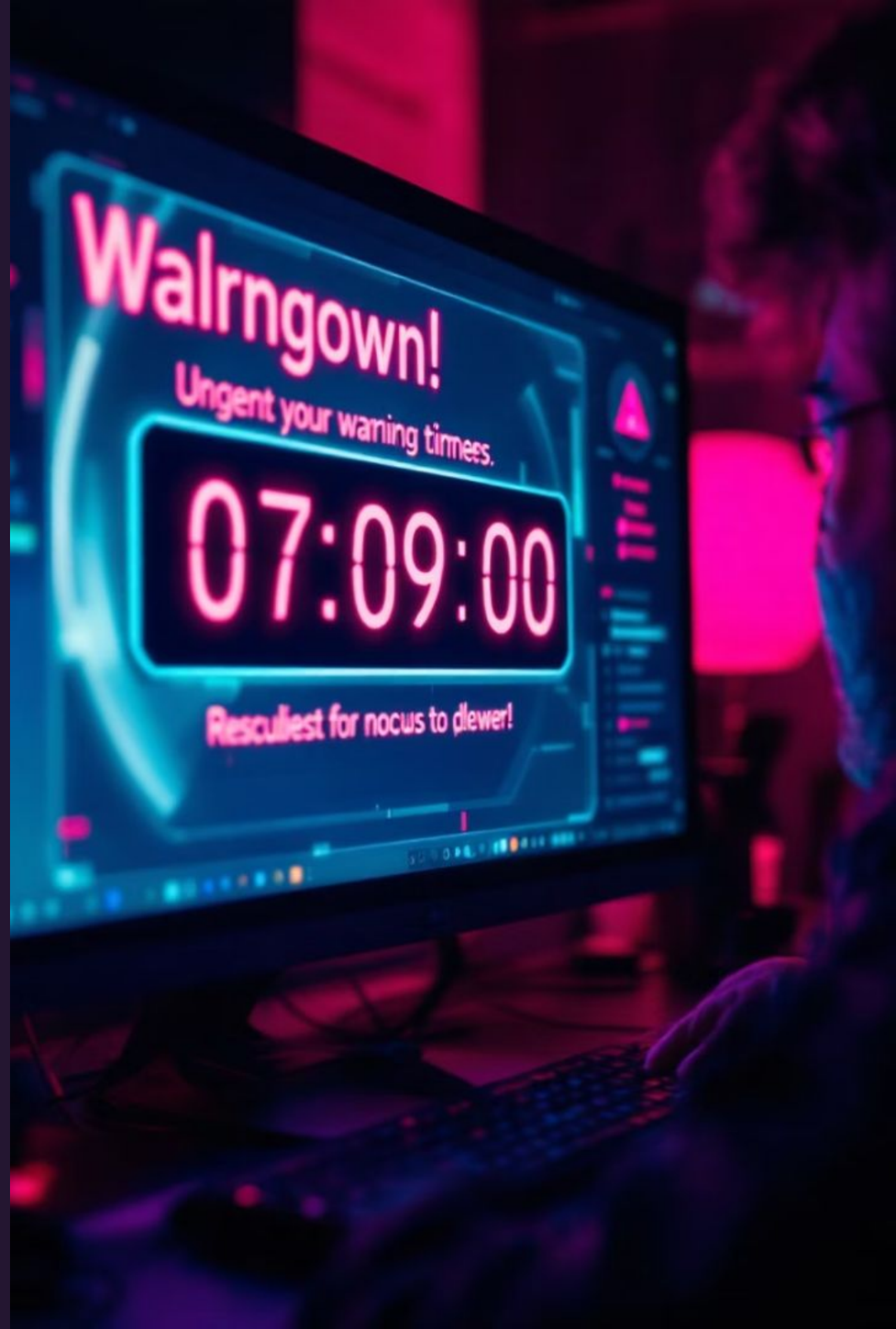
Tempo Limitato

Scadenze brevi per forzare decisioni affrettate.

3X

Efficacia

Maggiore probabilità di successo rispetto ad attacchi senza urgenza.



ESEMPIO:

Un popup appare su un sito apparentemente legittimo: “Solo per oggi – VPN gratuita per i primi 50 utenti. Clicca subito per scaricarla!”

Meccanismo: La percezione di una risorsa rara o un’opportunità limitata spinge all’azione rapida, senza controlli.

Principio della Riprova Sociale

Le persone tendono a seguire il comportamento della maggioranza. Questo principio viene utilizzato nel 60% delle truffe online secondo la Polizia Postale.

Recensioni false e testimonianze inventate creano una falsa percezione di popolarità e affidabilità.

ESEMPIO:

In un gruppo Slack aziendale, appare un messaggio da “IT Helpdesk”: “Stiamo aggiornando i sistemi, *tutti* stanno completando questa verifica a due fattori. Fallo anche tu cliccando qui.” Il messaggio è pieno di risposte di altri utenti (in realtà fake): “Fatto”, “Tutto ok!”.

Meccanismo: L’attaccante crea un’illusione di consenso per far credere alla vittima che l’azione sia normale e sicura.

Altri Principi Psicologici dell'Ingegneria Sociale

Impegno

Desiderio di essere coerenti con impegni precedenti.

Ignoranza

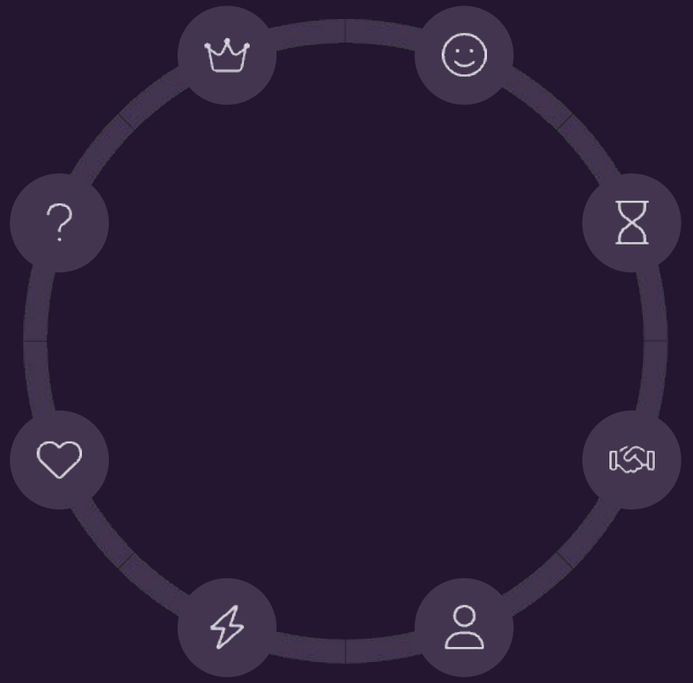
Sfruttamento della mancanza di conoscenza.

Fiducia

Tendenza a fidarsi senza verificare.

Paura

Reazioni impulsive generate dalla paura o ansia.



Principio dell'Impegno e Coerenza

Piccolo impegno iniziale

Richiesta di un'azione semplice e apparentemente innocua.

Escalation graduale

Aumento progressivo delle richieste basato su impegni precedenti.

Richiesta sensibile finale

Accesso a informazioni o sistemi protetti.

ESEMPIO:

Fabio partecipa a un finto sondaggio sulla sicurezza informatica. Dopo aver risposto a domande come “Proteggi sempre la tua password?” con “Sì”, riceve una richiesta: “Perfetto! Per rafforzare la tua sicurezza, scarica questa estensione raccomandata.”

Meccanismo: Dopo essersi impegnati su un’idea, le persone tendono a voler essere coerenti con essa, anche se li porta su una strada pericolosa.

La Fiducia come Arma

Definizione

Manipolazione basata sulla credulità e sulla fiducia altrui.

Come Funziona

L'attaccante si presenta come una figura affidabile. Ad esempio, un tecnico o un'autorità.

Statistica

Il 70% degli attacchi di social engineering inizia con la fiducia.

È essenziale verificare sempre l'identità di chi richiede informazioni sensibili.

Indurre la Paura per il Controllo

Definizione

Sfruttare la paura per forzare decisioni rapide e irrazionali.

Come Funziona

Minacce di conseguenze gravi, come la perdita di dati o sanzioni.

Esempio

Email che minaccia di bloccare l'account se non si aggiornano subito i dati.

La paura bypassa il pensiero critico, aumentando la vulnerabilità.

Mantenere la calma è fondamentale.

Sfruttare l'Ignoranza Informatica

Definizione

Sfruttare la mancanza di conoscenza sulla sicurezza informatica.

Come Funziona

L'attaccante usa termini tecnici per confondere e manipolare.

Esempio

Email che avvisa di una "vulnerabilità critica" e richiede download urgente di un software infetto.

Vettori di attacco di Social Engineering

Varie tipologie di pesca

Phishing, spear phishing, whaling, vishing e smishing,

Attacchi fisici

Baiting, dumpster diving, piggubacking o shoulder surfing, physical acess

Bufale

Hoaxing, fake news, fake software

Spacciarsi per altri

Impersonation,do ut des, quid pro quo

Vettori di Attacco: Phishing

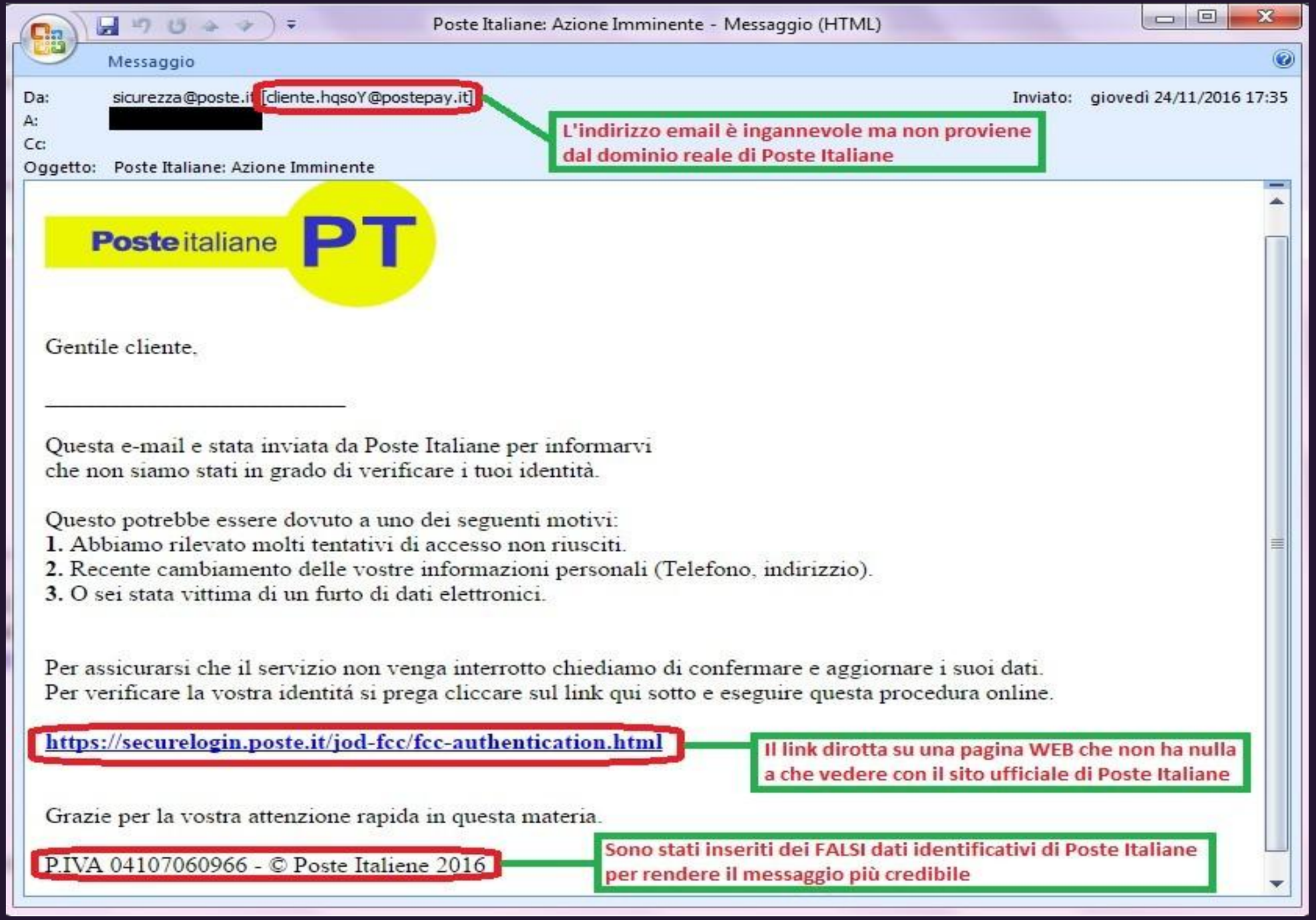
Truffa via internet in cui l’aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali o aprire allegati che contengono malware

Come riconoscerlo?

Mittente sconosciuto o sospetto, errori ortografici nel testo, viene richiesto con URGENZA di fornre dati personali

Cosa succede se accedo?

Probabilmente finirò su una landing page (pagina pensata per ingannare l’utente) dove verrò spinto a rivelare info preziose



Vettori di Attacco: Spear Phishing

Forma mirata di phishing, orientata a colpire una vittima accuratamente selezionata

Come riconoscerlo?

La mail che riceviamo contiene il nome di un collega o un amico, si riferisce alle attività che svolgiamo, al nostro compleanno

Vettori di Attacco: Vishing e smishing

Vishing

Forma mirata di phishing, che viene fatta tramite chiamate da fake call center che ci chiedono dati

Smishing

Forma mirata di phishing, che viene fatta tramite messaggi che simulano per contenuto e utente quelli di un operatore della tua Banca

Vettori di Attacco: Impersonation, Do ut des, Quid Pro Quo

Do ut des

L’attaccante offre alla vittima un regalo, un compenso o un benefit

Quid pro quo

L'attaccante offre alla vittima un servizio in cambio delle credenziali d’accesso

SI BASANO SUL PRINCIPIO DI RECIPROCITÀ

Vettori di Attacco fisico: Baiting

1

L'Esca

Utilizza un'esca di solito fisica per catturare l'interesse della vittima.

2

Esempi Pratici

Chiavette USB "trovate", download gratuiti di software costosi. Oppure l’attaccante crea un dispositivo USB che quando viene collegato a un computer simula una serie di comandi in grado di installare nel computerun programma malevolo (payload)

Vettori di attaco fisici: Piggybanking o shoulder surfing

Capacità di un attaccante di ottenere l’accesso illecito a un’area o un’informazione riservata seguendo a breve distanza qualcuno che invece la possiede

Vettori di attaco fisici: Piggybanking o shoulder surfing

Capacità di un attaccante di ottenere l’accesso illecito a un’area o un’informazione riservata seguendo a breve distanza qualcuno che invece la possiede

Come Riconoscere un Attacco di Social Engineering

Individuare i Segnali d'Allarme

Urgenza sospetta, errori grammaticali, dettagli incongruenti.

Pensare Criticamente

Verificare l'identità del richiedente attraverso canali ufficiali.

Mantenere lo Scetticismo

Le offerte troppo belle nascondono sempre insidie.

DEEPFAKE

Il *deepfake* (parola coniata nel 2017) è una tecnica per la sintesi dell'immagine umana fondata sull'intelligenza artificiale, usata per combinare e sovrapporre immagini e video esistenti con video o immagini originali

Gli utenti online possono utilizzare i deepfake per:

diffondere informazioni false;

- Rovinare la fiducia nelle figure pubbliche;
- manipolare le conversazioni sulla politica e su altre questioni importanti.

Your wooclap poll will be displayed here

1

Install the **Chrome** or **Firefox extension**

2

Make sure you are in **presentation mode**

wooclap

🧪 CASO STUDIO 1: L'Email del Responsabile HR

Scenario:

Sara, impiegata in un'azienda da pochi mesi, riceve un’email con oggetto:
📩 *"URGENTE: Aggiornamento dati per il pagamento dello stipendio!"*

Il mittente è “Alessandra Rizzi – Ufficio HR” e l’indirizzo sembra autentico. Il messaggio dice:

> *“Ciao Sara,*
> *abbiamo aggiornato il nostro sistema pagamenti. Ti chiedo gentilmente di inserire i tuoi dati bancari cliccando su questo link. È fondamentale farlo* ***entro oggi alle 17:00*** *per non ritardare l’accredito del tuo stipendio.*
> *Grazie per la collaborazione,*
> *Alessandra - Responsabile HR”*

Il link porta a una pagina che **sembra identica** a quella interna del gestionale aziendale.

Your wooclap poll will be displayed here

Install the **Chrome** or **Firefox extension**

Make sure you are in **presentation mode**

wooclap

`flag{Th3r3_4r3_us3ful_1nf0_h3re}`

🧪 CASO STUDIO 2: Il Tecnico IT Misterioso

Scenario:

Giulia lavora in un coworking e una mattina riceve una chiamata sul numero interno da un uomo che dice:

> *“Buongiorno, sono Marco del reparto IT centrale. Stiamo aggiornando i protocolli di sicurezza. Abbiamo notato accessi sospetti dal tuo account e dobbiamo intervenire. Mi puoi fornire la tua password per confermare l’identità? Se non procediamo subito, l’account verrà sospeso per sicurezza.”*

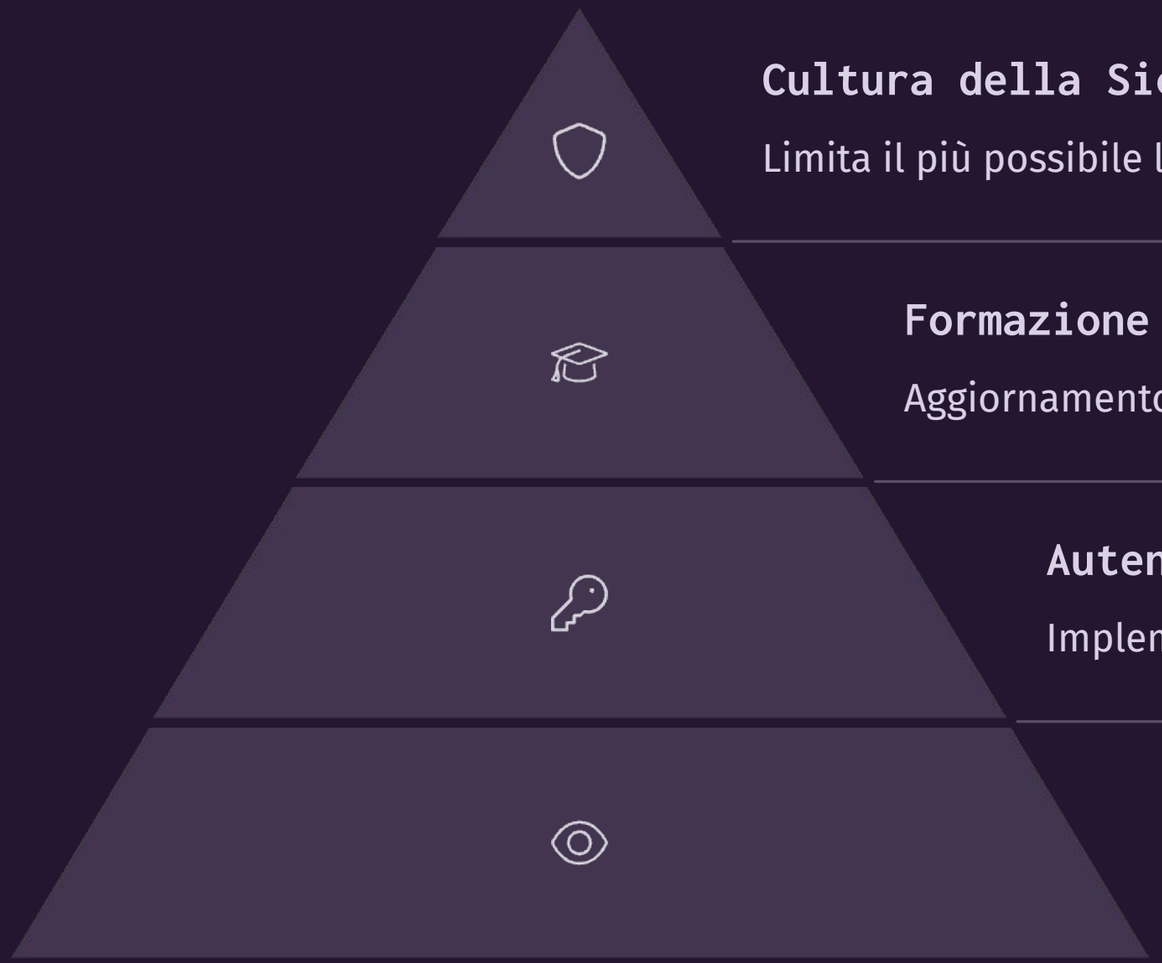
Your wooclap poll will be displayed here

Install the **Chrome** or
Firefox extension

Make sure you are in
presentation mode

wooclap

CYBER HYGENE



Cultura della Sicurezza

Limita il più possibile la divulgazione via web delle tue informazioni

Formazione Continua

Aggiornamento costante sulle nuove tecniche di attacco.

Autenticazione Forte

Implementare sistemi a più fattori e verifiche aggiuntive.

Verifica Sistematica

Controllare sempre l'identità di chi richiede informazioni.