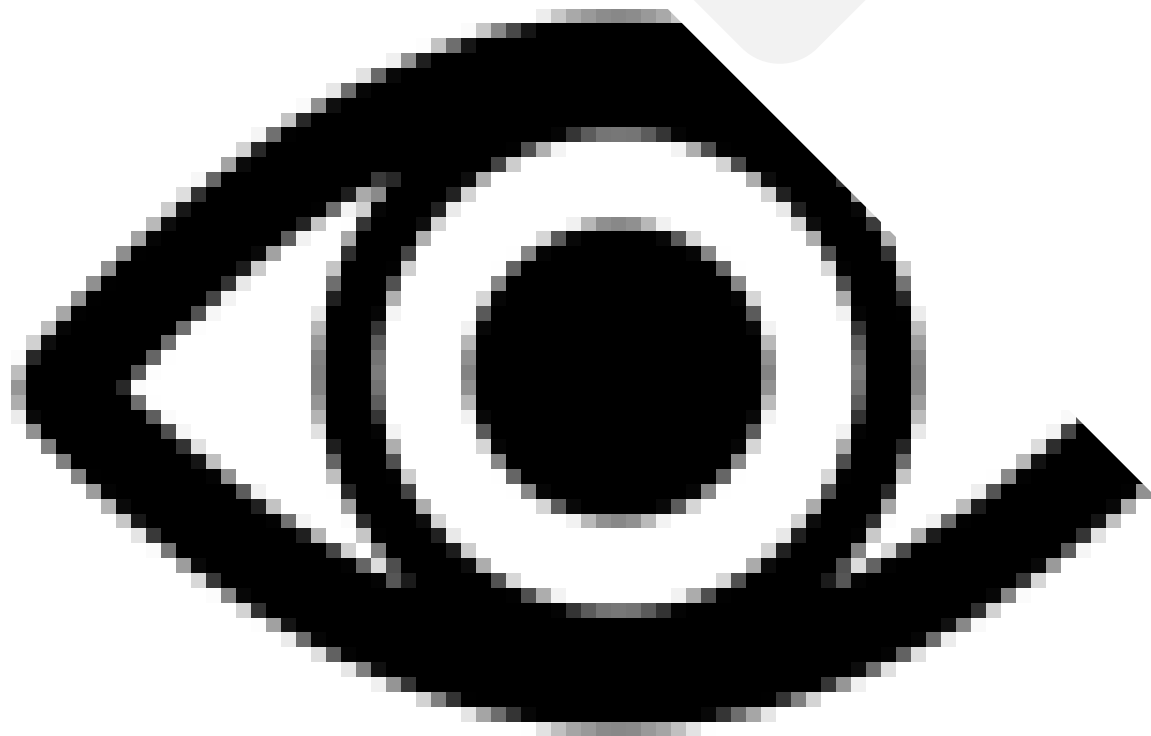




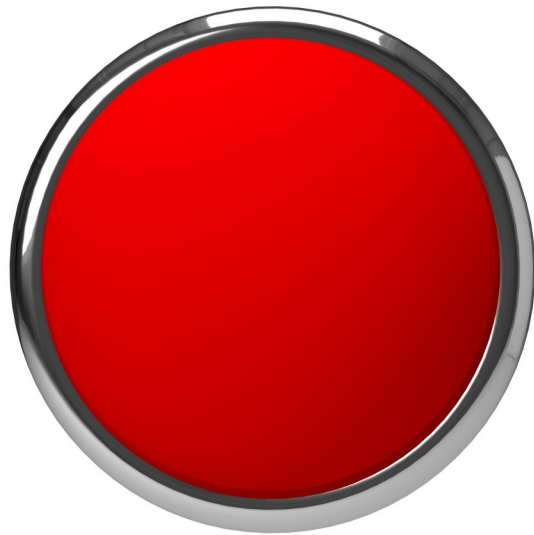
RICONOSCERE LA TRUFFA

 **ALTROCONSUMO**

SMS da banca che dice
«Abbiamo rilevato un'operazione anomala.
Clicca qui per bloccare il conto».

Il link porta a una pagina, dove viene chiesto
di inserire credenziali, PIN o codice OTP.

Di cosa si tratta? smishing + furto delle credenziali.



Campanello d'allarme:

- urgenza
- minaccia di blocco del conto
- richiesta di codici.

SMS:

«Il tuo pacco non può essere consegnato. Paga 2,99 € per modificare la consegna».

Il link conduce a un sito di Poste, DHL, UPS o altro corriere e chiede i dati della carta.

Di cosa si tratta? smishing + furto delle credenziali.



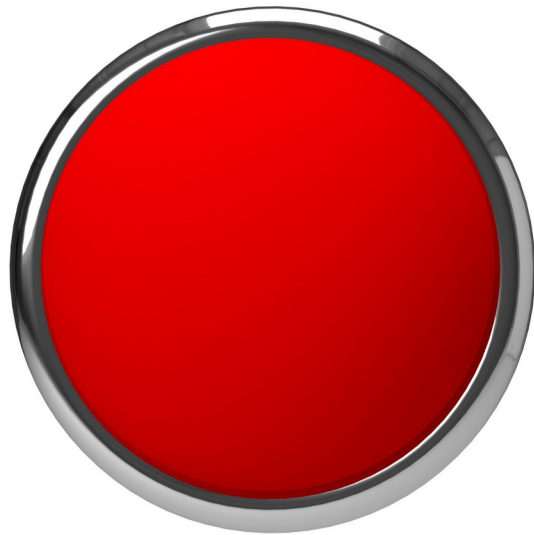
Campanello d'allarme:

- link ricevuto via SMS
- richiesta di pagamento per una consegna non verificata.

Messaggio WhatsApp dal figlio o dalla
figlia:

«Ho cambiato numero, ho bisogno
urgentemente di 800 € per pagare una
cosa. Puoi farmi un bonifico?».

Che meccanismo? Si sfrutta la fiducia e la pressione emotiva per impedire alla vittima di



Campanello d'allarme:

- richiesta economica urgente
- nuovo numero
- impossibilità di parlare normalmente.

Compare sui social una pubblicità con un personaggio famoso o un presunto esperto che promette guadagni elevati investendo poche centinaia di euro.

Dopo aver lasciato i propri contatti, si viene chiamati da un “consulente” che invita a versare altro denaro.

Che meccanismo? Deepfake con AI. Falsa opportunità di investimento + pressione del falso



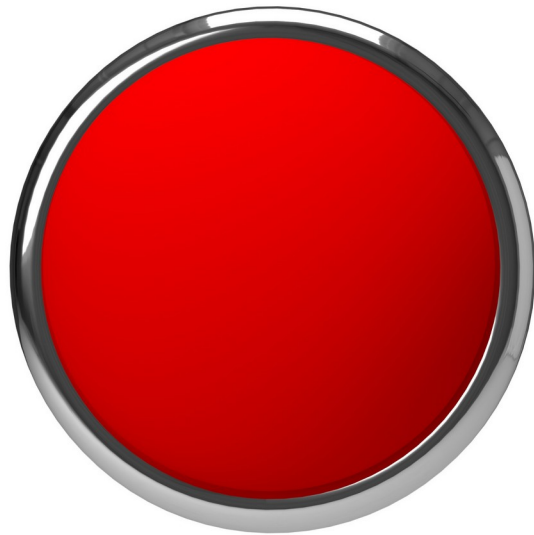
Campanello d'allarme:

- guadagni garantiti
- rendimenti molto elevati
- richiesta di versare rapidamente altro denaro.

Mentre si naviga compare una finestra:
«ATTENZIONE! Il tuo dispositivo è stato
infettato. Chiama immediatamente
questo numero».

Un finto operatore Microsoft, Apple o di
un altro servizio convince la persona a
installare un programma per
“controllare” il computer.

Che meccanismo? Si ottiene accesso remoto al dispositivo o alle informazioni personali



Campanello d'allarme:

- messaggio allarmistico
- richiesta di telefonare a un numero
- installare un software.

Si riceve un messaggio WhatsApp o Telegram: «Stiamo cercando persone per mettere like ai prodotti online.

Puoi guadagnare 100-200 € al giorno». Dopo alcune piccole attività, viene chiesto di versare una somma per “sbloccare” incarichi più remunerativi.

Che meccanismo? Si costruisce fiducia con piccoli guadagni iniziali e poi si chiede denaro alla vittima.



Campanello d'allarme:

- promessa di guadagni elevati per attività semplicissime
- richiesta di anticipare denaro.