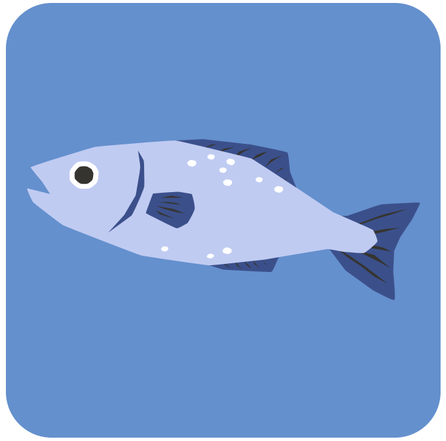
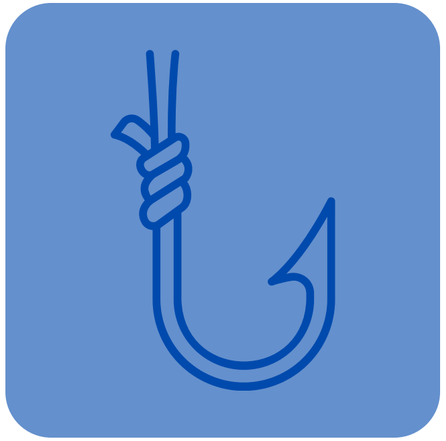
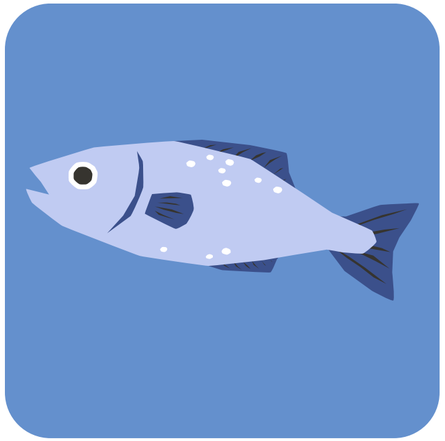
PHISHING

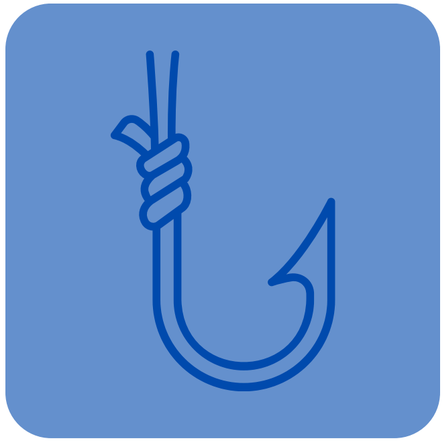




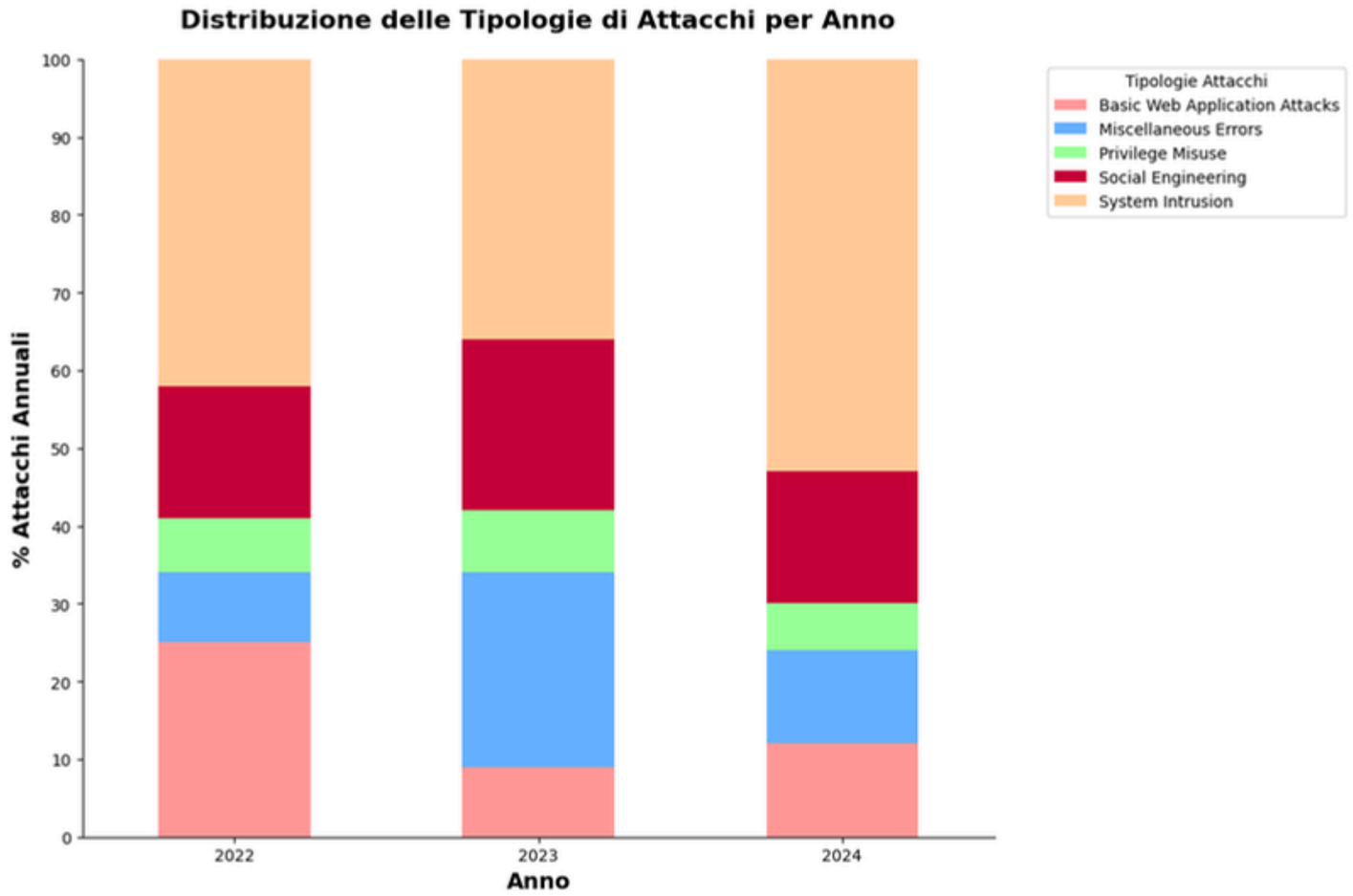
Edoardo Paradiso 63419A - Sara Zamboni 65980A

INCIDENCE OF ATTACKS





DISTRIBUZIONE DELLE TIPOLOGIE DI ATTACCHI PER ANNO



Con questo grafico a barre sovrapposte si mostra una panoramica generale sulle tipologie di attacco più frequenti; il colore più rilevante è quello associato alla categoria “Social Engineering”, quella che tratteremo più in dettaglio nelle prossime slide.

MOTIVO DI STUDIO E RILEVANZA

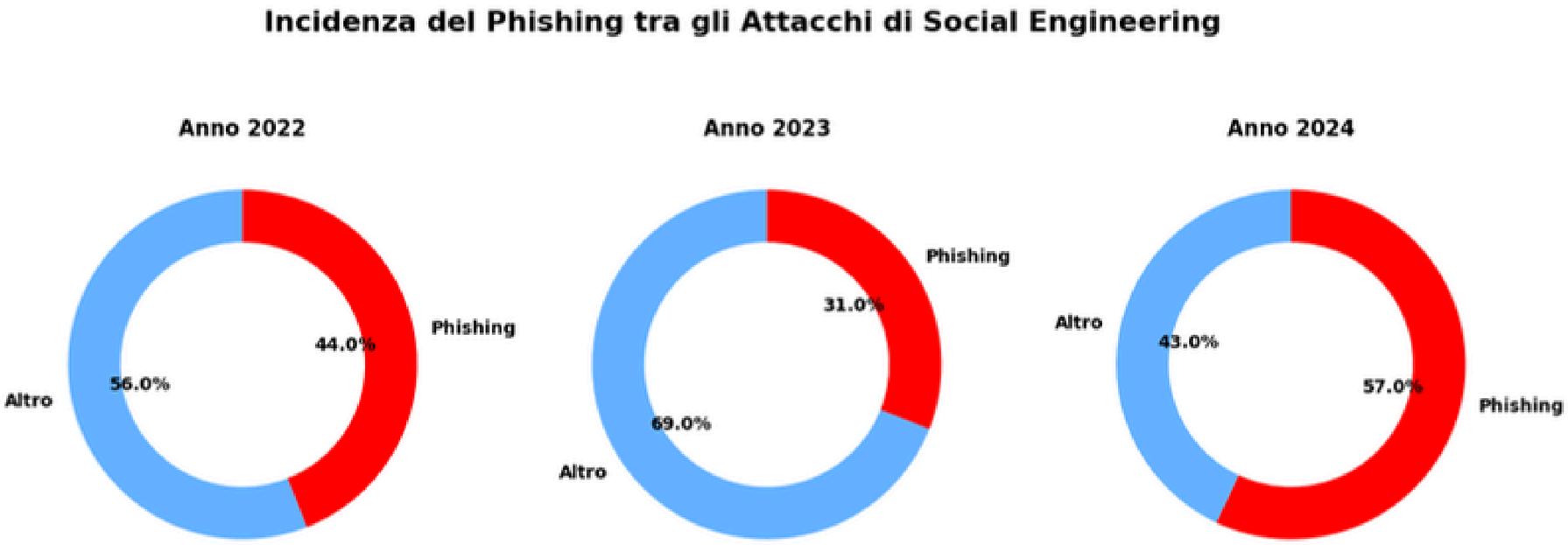
Una nuova campagna di phishing su finte truffe legate a multe per violazioni del codice della strada è oggi una minaccia per gli utenti, secondo quanto analizzato nell'ultimo bollettino del CSIRT Italia.

Una nuova campagna di **phishing** "*a tema 'Violazione codice della strada', per carpire le informazioni personali delle potenziali vittime, compresi gli estremi delle carte di credito*", è stata rilevata dal **CSIRT Italia**.

La campagna sfrutta la **posta elettronica** e informa la potenziale vittima "*del mancato pagamento di una sanzione amministrativa per eccesso di velocità*". Conseguentemente, la esorta "*a pagare tale sanzione, cliccando sul link presente all'interno del corpo del messaggio*".

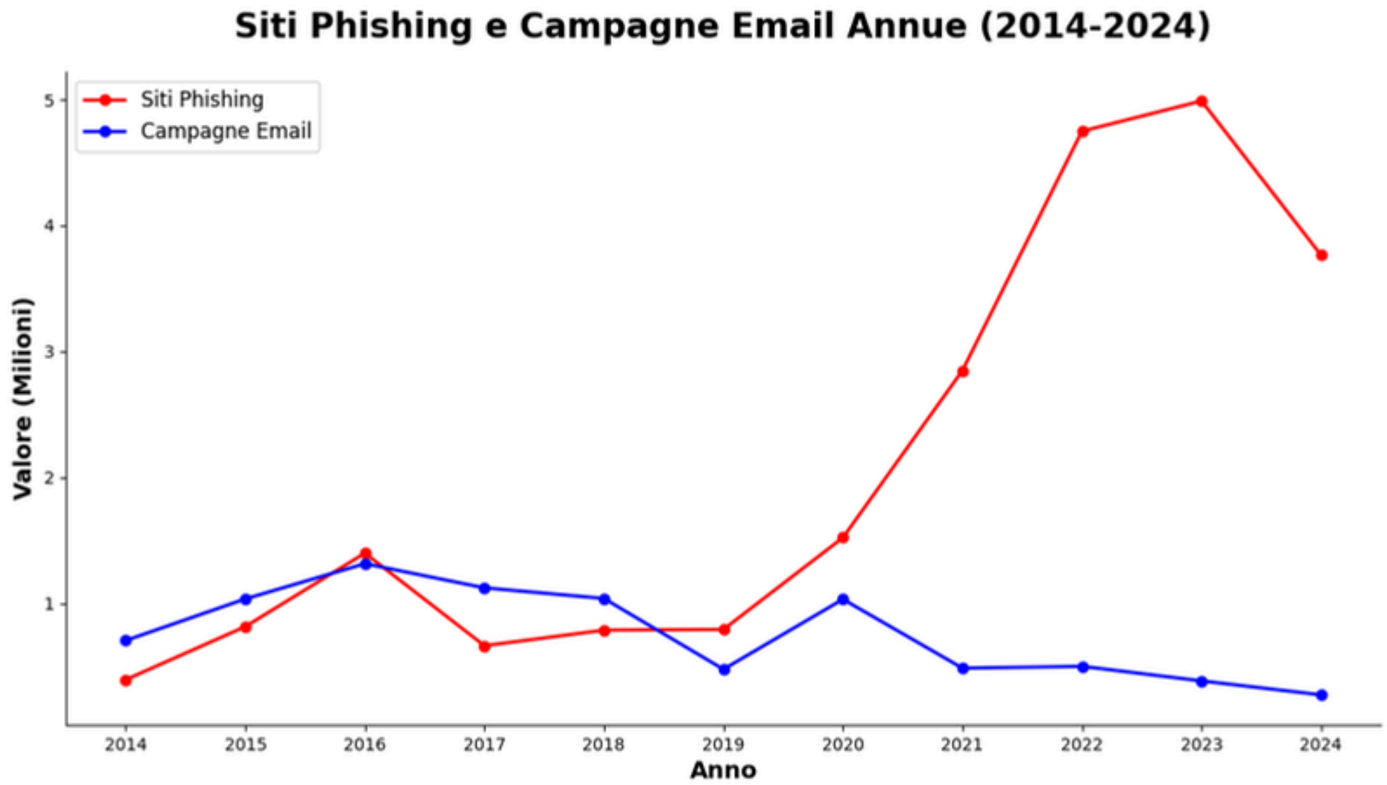
18 Novembre 2025

FREQUENZA TRIENNALE DEGLI ATTACCHI DI PHISHING



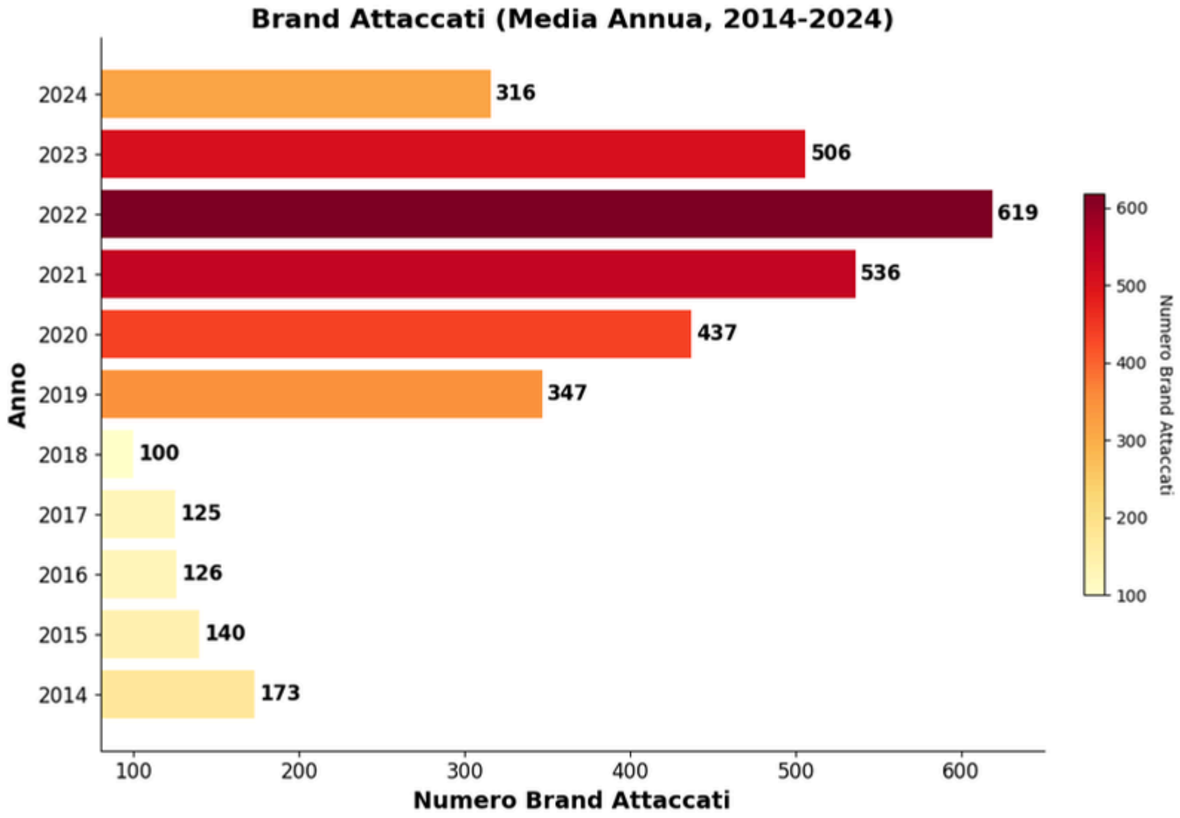
Con questo grafico a ciambella viene marcata la proporzione dominante del phishing rispetto ad altre forme di Social Engineering (Altro). Questo avviene per tre ragioni fondamentali: costo, scalabilità ed efficacia come vettore di ingresso.

SITI PHISHING E CAMPAGNE EMAIL ANNUE (2014 -2024)



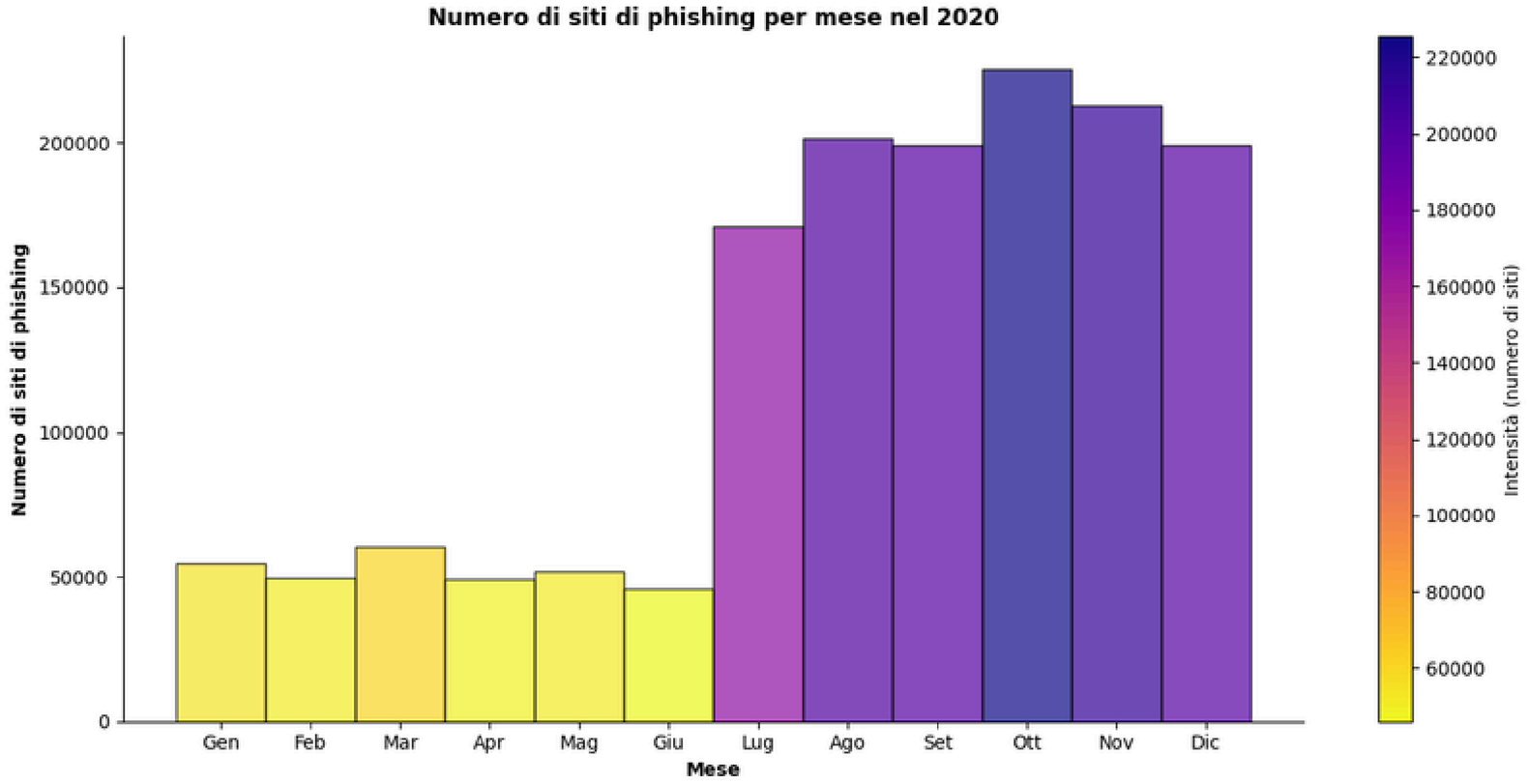
Nel grafico a linee si può osservare chiaramente il trend degli ultimi anni, relativo ai siti di phishing rilevati (destinazione dell'attacco) e il numero di campagne (vettore d'attacco).

BRAND ATTACCATI (MEDIA ANNUA, 2014-2024)



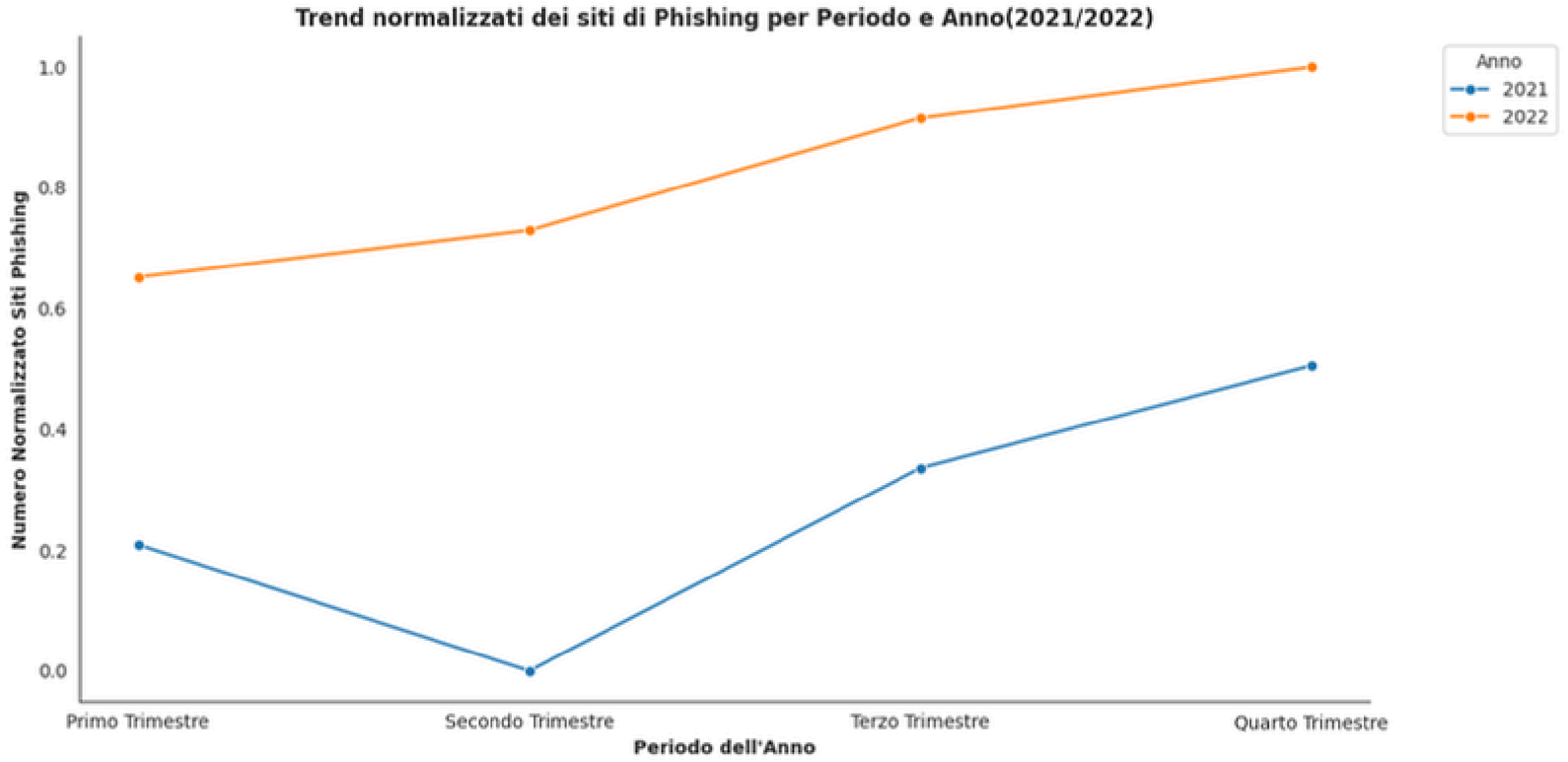
Con questo grafico a barre si osserva un chiaro trend di crescita del numero di brand presi di mira, con un picco nel 2022. La successiva e improvvisa flessione nel 2023 è dovuta principalmente al blocco delle registrazioni di domini gratuiti da parte del provider Freenom, il quale aveva costituito l'infrastruttura a basso costo per migliaia di siti di phishing.

LA SITUAZIONE DELL'ANNATA "COVID"



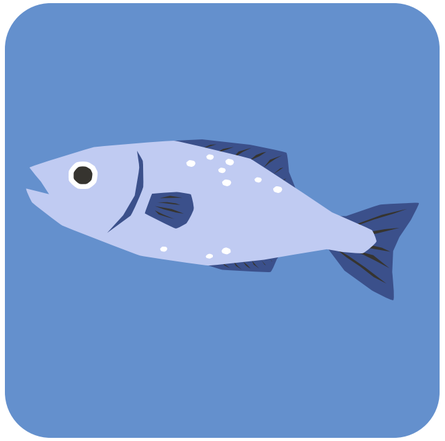
Il grafico a barre soprastante mostra un incremento notevole dei siti di phishing solo a partire da luglio 2020, in ritardo rispetto all'inizio della pandemia. Questo ritardo si spiega con la necessità dei criminali di adattare le loro "catene di approvvigionamento", identificando i temi pandemici più efficaci (es. e-commerce, autorità sanitarie) e i brand giusti da impersonare per massimizzare la riuscita degli attacchi.

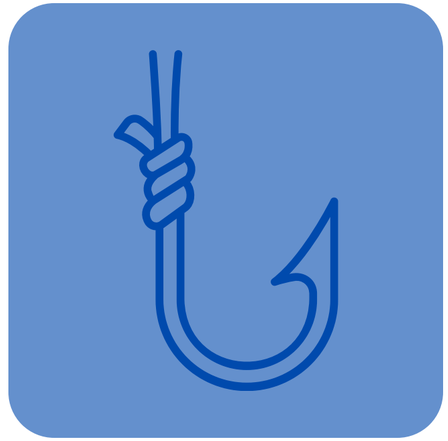
TREND DEI SITI DI PHISHING PER PERIODO E ANNO (2021/2022)



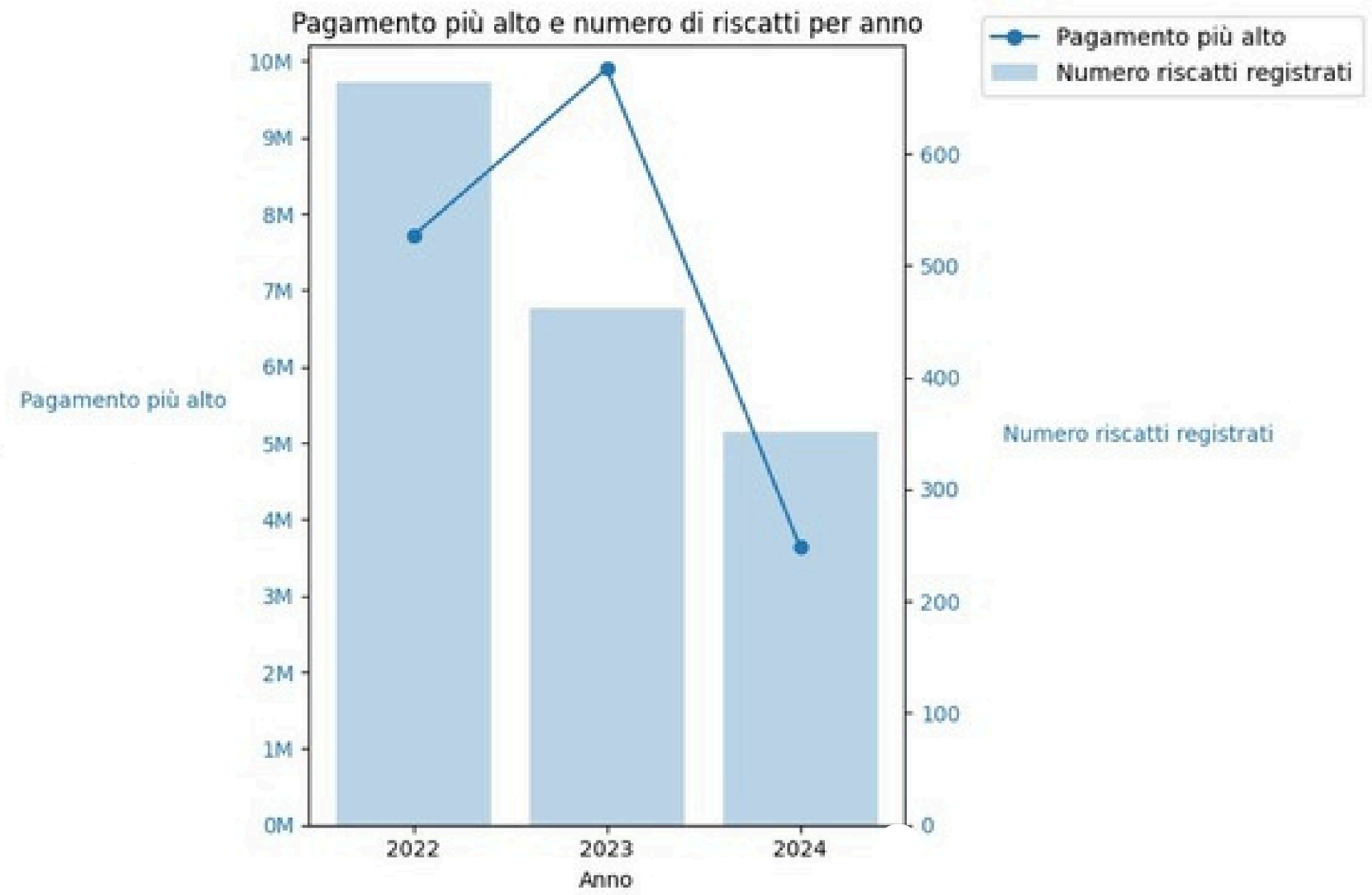
Questo grafico a linee mostra un andamento stagionale marcatamente simile tra il 2021 e il 2022 (presi come esempio), con una crescita significativa nel Terzo e Quarto Trimestre. Tale aumento è guidato principalmente da fattori economici e psicologici come la stagione dello shopping e delle festività (aumento delle transazioni) e la chiusura dell'anno fiscale (impersonificazione di agenzie governative).

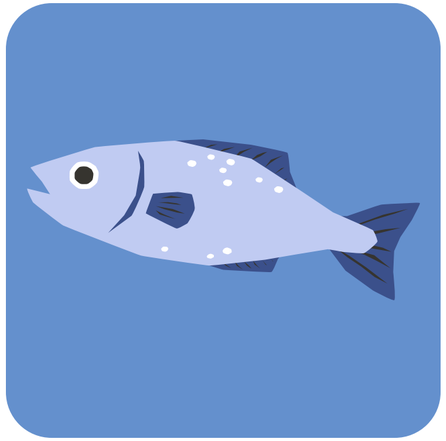
COMPANY LOSSES



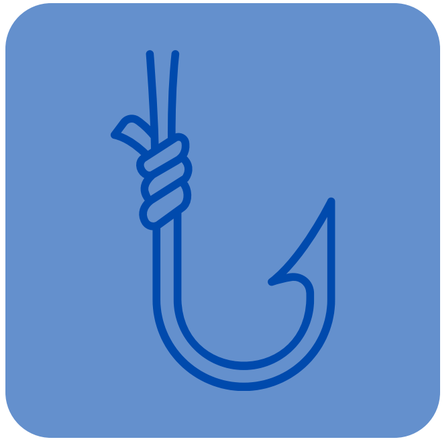


PAGAMENTI PIU' ALTI E RISCATTI PER ANNO (2022 -2024)



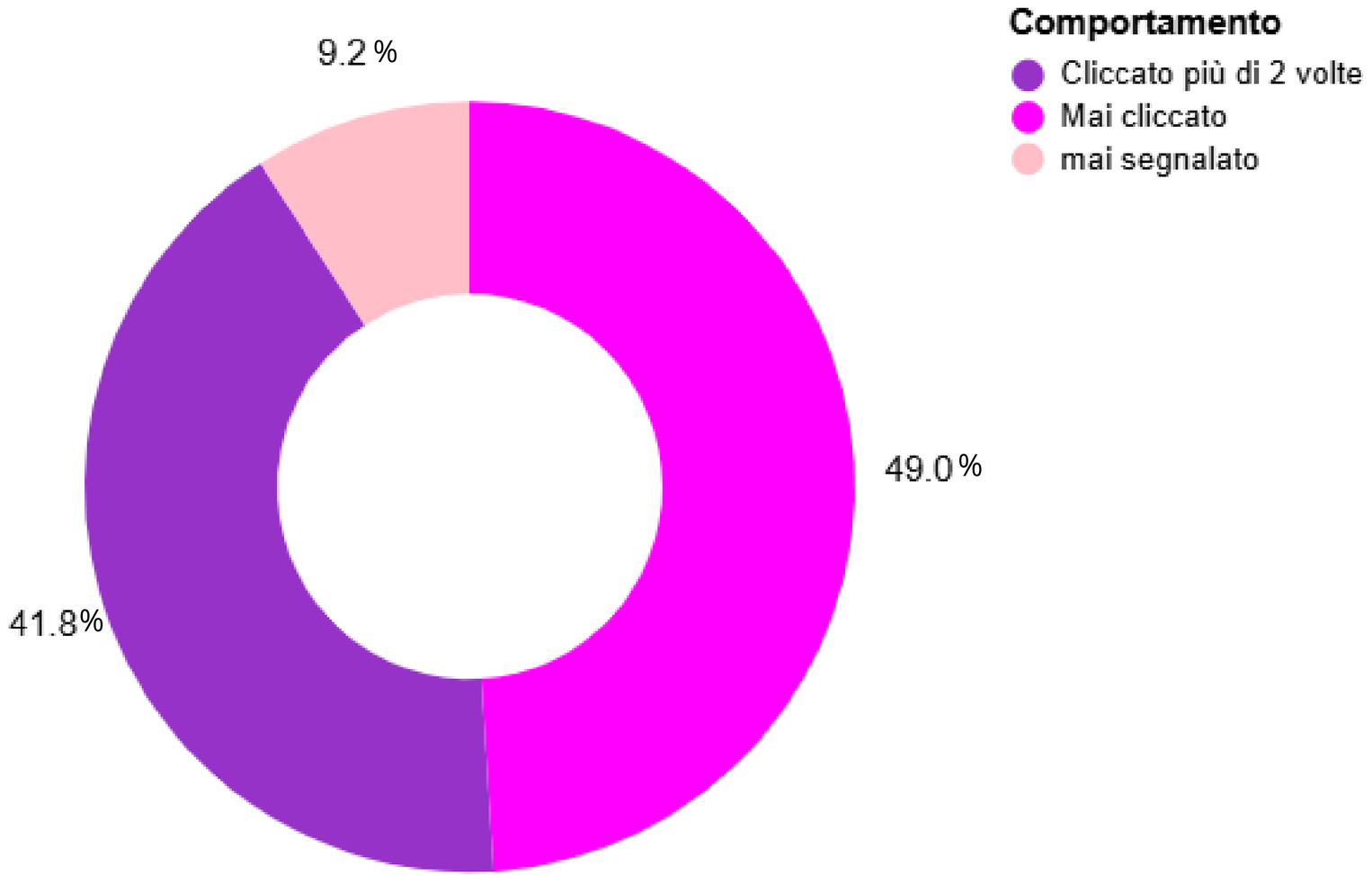


VICTIM DATA



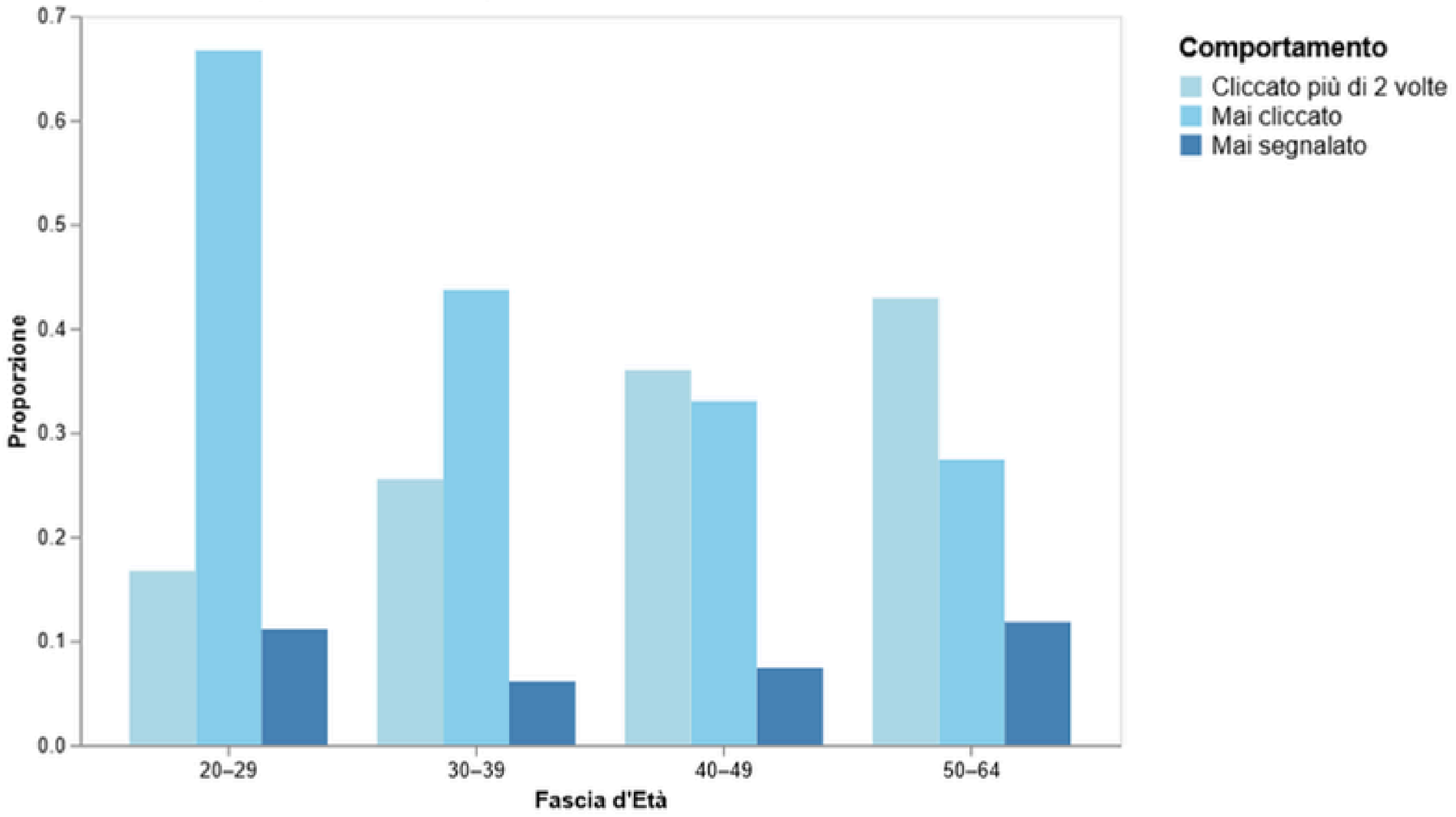
L’anello debole della catena

DISTRIBUZIONE RELATIVA DEI COMPORTAMENTI DI PHISHING (UOMINI E DONNE COMBINATI)



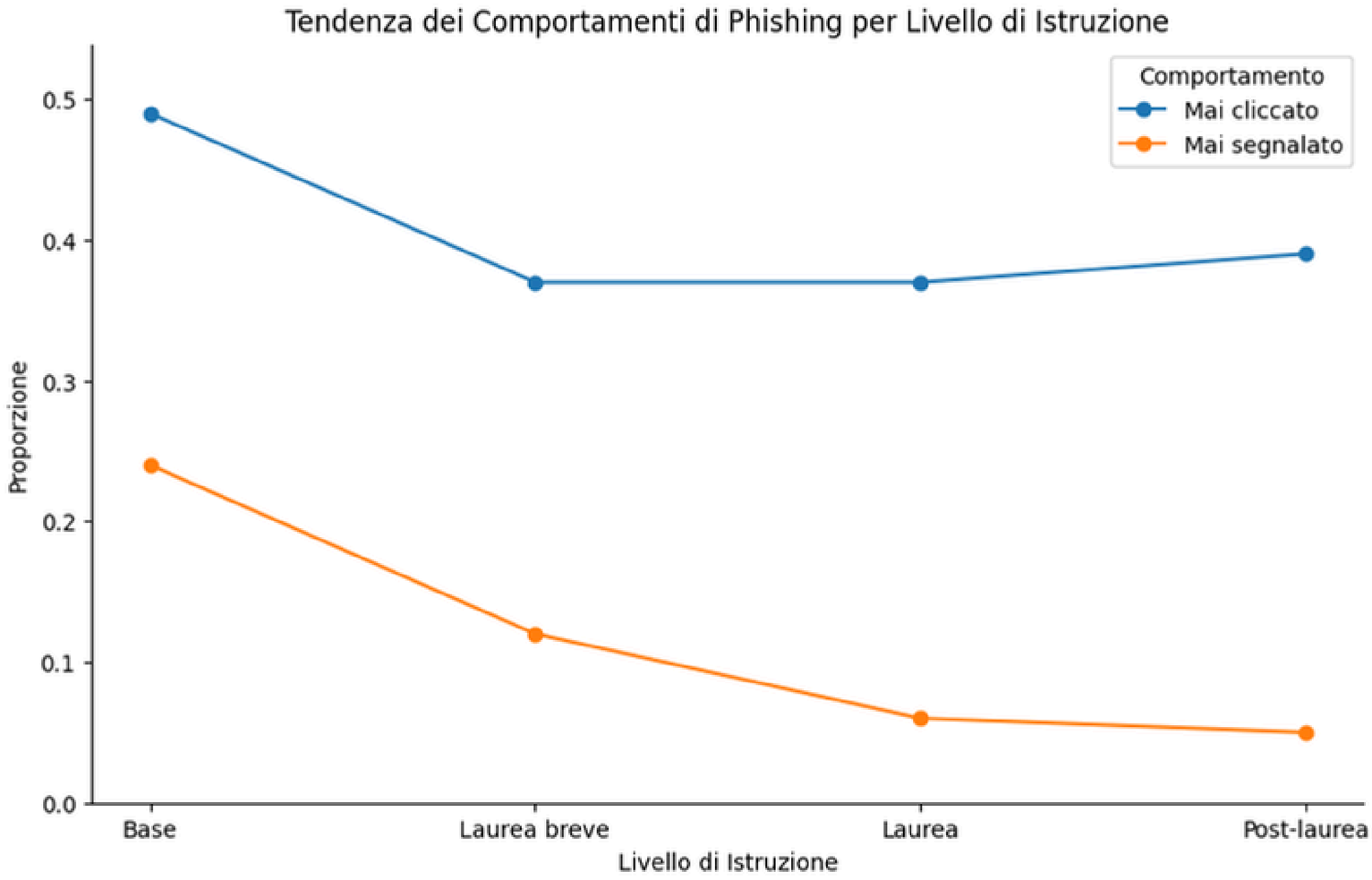
Attualmente circa la metà del campione mostra comportamenti rischiosi (clic multipli o mancata segnalazione)
campagne di sensibilizzazione,simulazioni di phishing e la semplificazione dei canali di segnalazione potrebbero migliorare il trend comportamentale

CORRELAZIONE NUMERO DI CLICK E FASCIA D'ETA'



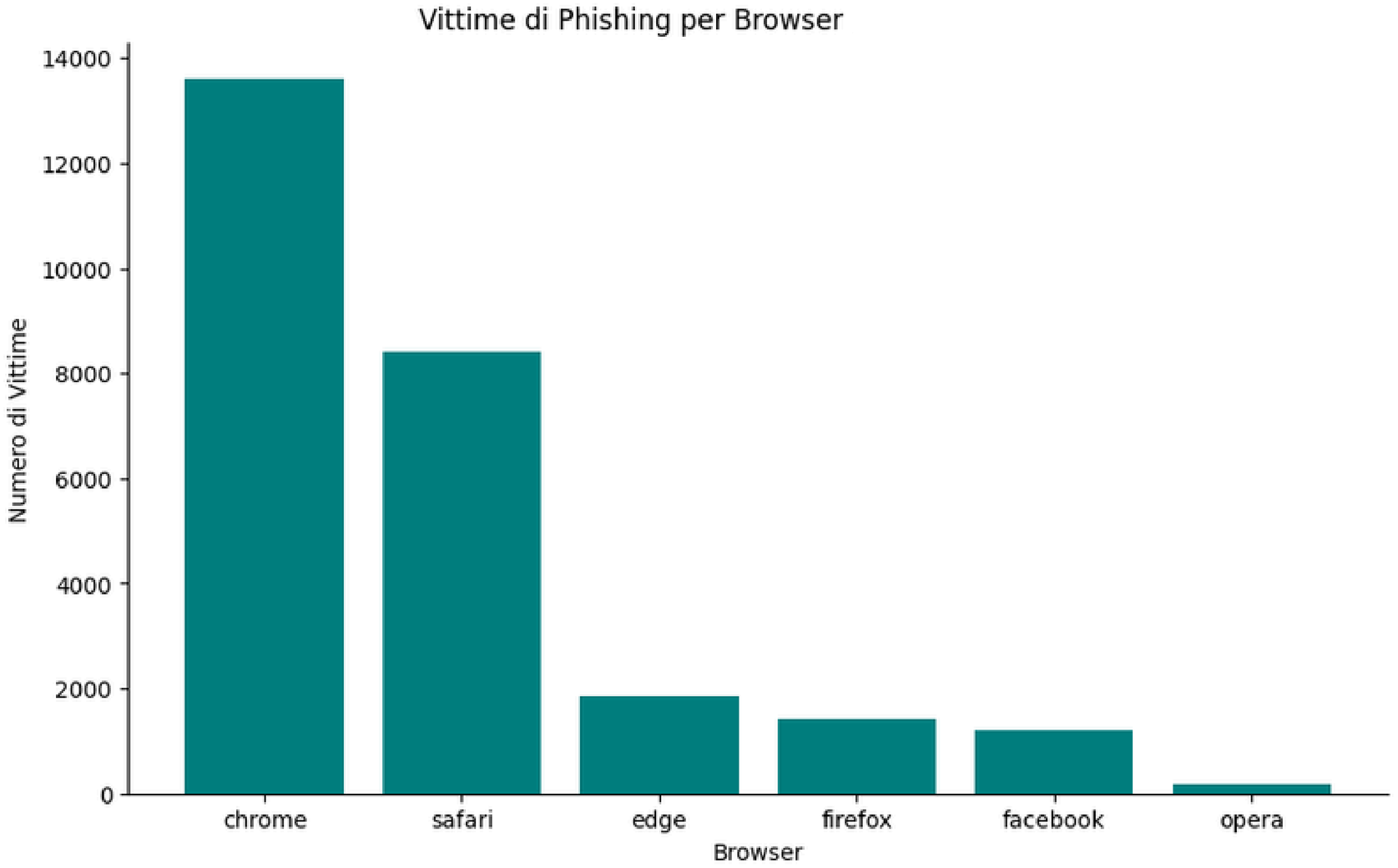
E' presente una forte relazione tra età e rischio di vittimizzazione: più sale l'età più aumentano i click ripetuti e diminuisce il tasto di "mai cliccato".

TENDENZA DEI COMPORTAMENTI DI PHISHING PER LIVELLO DI ISTRUZIONE



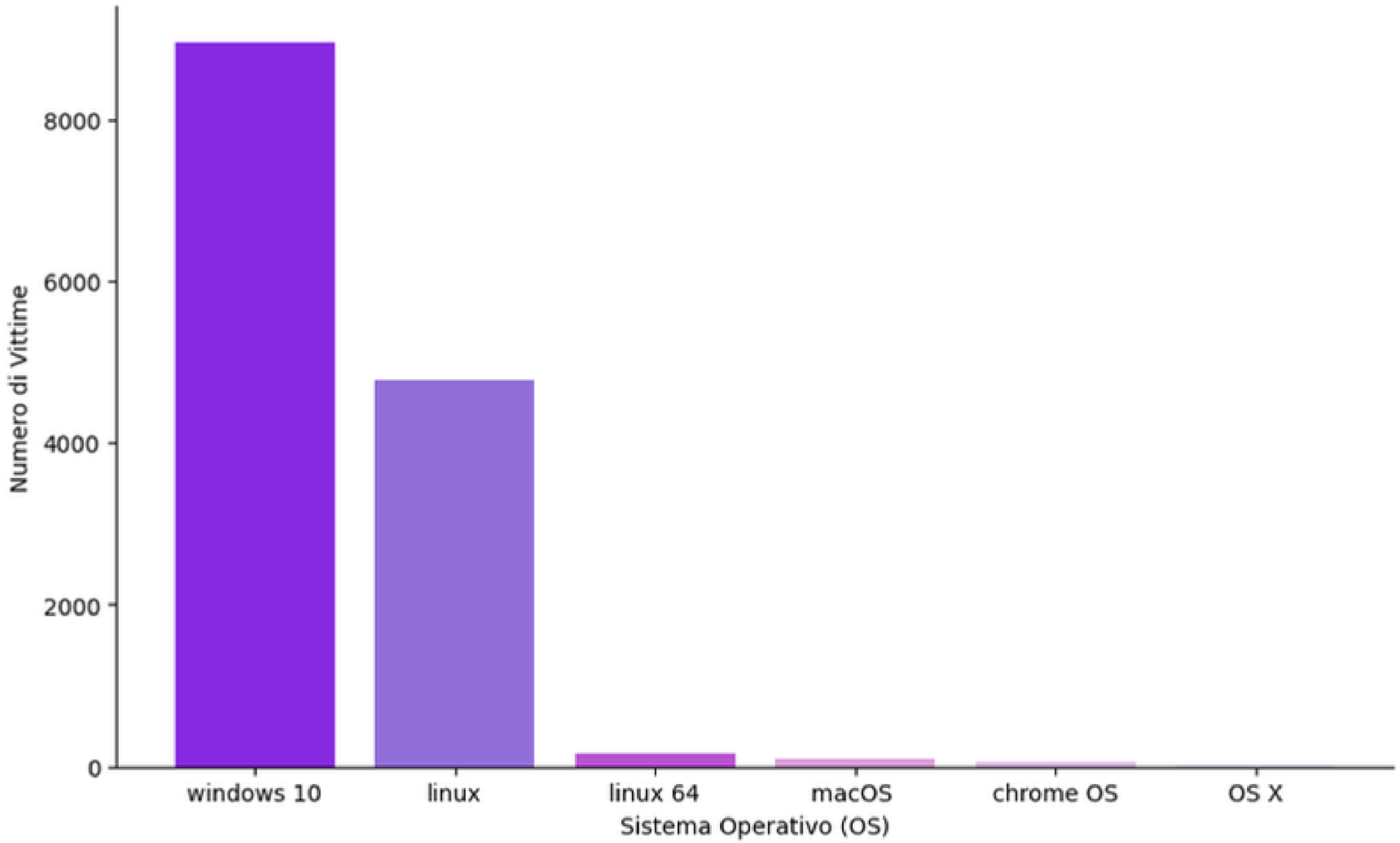
All'aumentare del livello di istruzione diminuisce nettamente la quota di chi non segnala mai il phishing, ma la tendenza a cliccare non sparisce, quindi anche i più istruiti restano vulnerabili agli attacchi

VITTIME DI PHISHING PER BROWSER



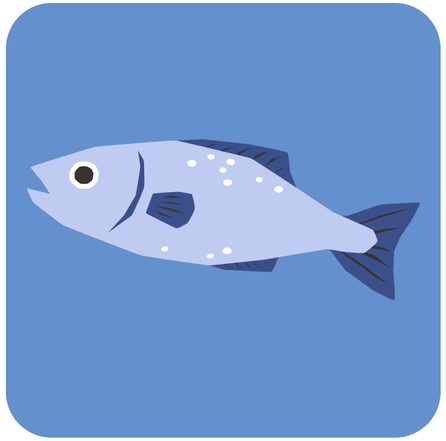
la sicurezza dipende soprattutto dal comportamento dell'utente e dai meccanismi di protezione dell'organizzazione, non solo dal browser scelto

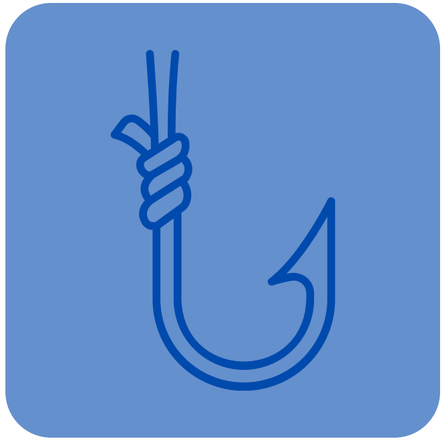
VITTIME DI PHISHING PER SISTEMA OPERATIVO



Il phishing si conferma quindi un problema trasversale, legato prima di tutto ai comportamenti degli utenti e solo in secondo piano alla piattaforma utilizzata

GRAZIE PER L'ATTENZIONE





Edoardo Paradiso 63419A - Sara Zamboni 65980A