Il fattore umano: costruire una cultura del comportamento sicuro

Paola Girdinio

Presidente START4.0

START4.0 – I nostri associati

Sondaggio State of the Phish 2024, ProofPoint

Il report State of The Phish 2024 ha interessato 7.500 lavoratori adulti e 1.050 professionisti dell'IT in 15 paesi.

Oltre 1 milione di attacchi viene lanciato con il framework di elusione dell'autenticazione a più fattori EvilProxy ogni mese

l'89% dei professionisti della sicurezza ritiene ancora che l'autenticazione a più fattori offra una protezione completa contro il takeover degli account.

Sondaggio State of the Phish 2024, ProofPoint

71% di utenti ha compiuto un’azione pericolosa

96% di loro l’ha fatto sapendo di correre un rischio

10 milioni di messaggi TOAD (Telephone-Oriented Attack Delivery) vengono inviati ogni mese

Microsoft continua ad essere il marchio più abusato, con, 68 milioni di messaggi dannosi associati al marchio o ai suoi prodotti

Sondaggio State of the Phish 2024, ProofPoint

85% dei professionisti della sicurezza ha affermato che la maggior parte dei collaboratori sa di essere responsabile della sicurezza, ma il 59% degli utenti non era sicuro o ha affermato di non esserne affatto responsabile

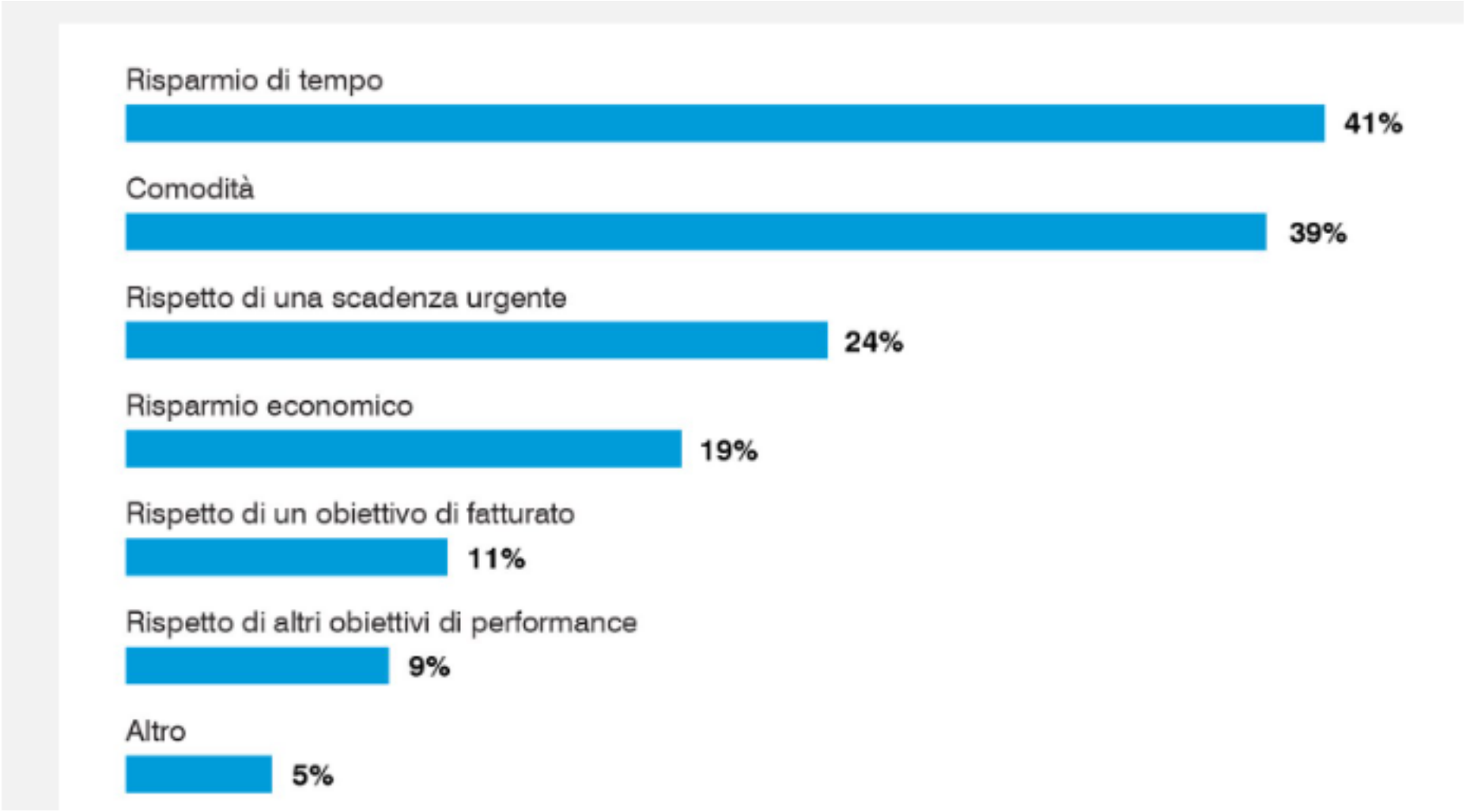
58% degli utenti che ha compiuto azioni pericolose ha assunto comportamenti che li avrebbero resi vulnerabili alle tattiche di social engineering comuni.

69% delle aziende è stato infettato dal ransomware.

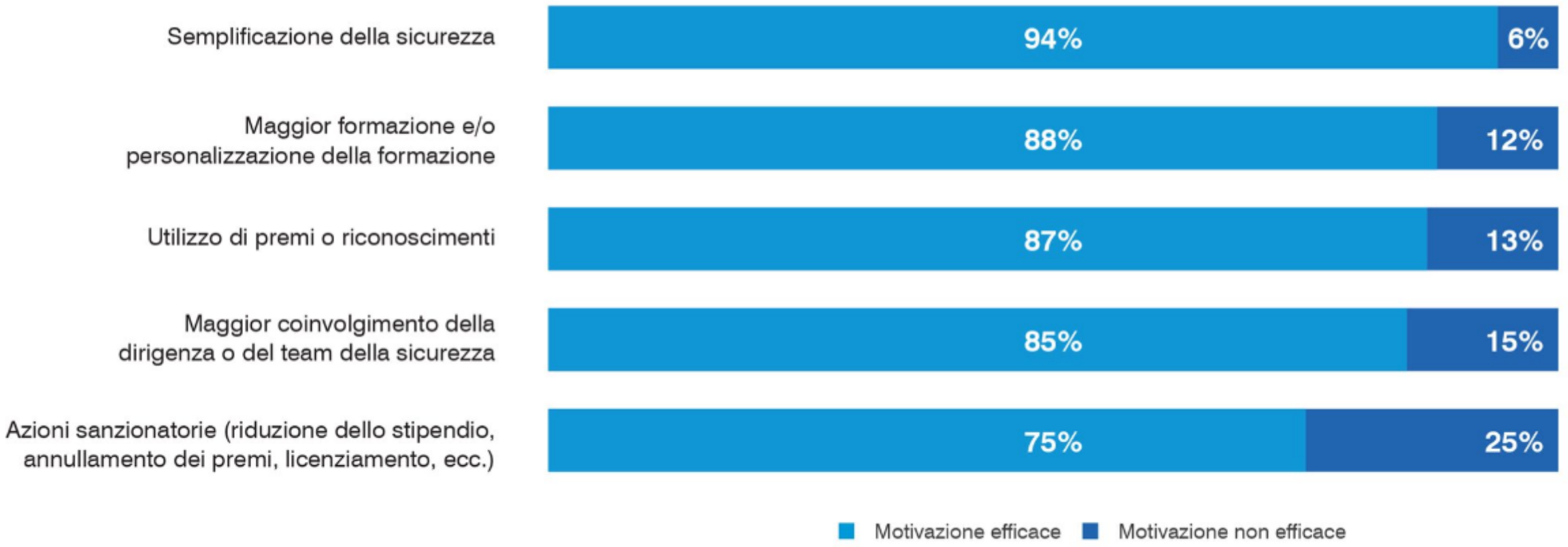
Comportamenti a rischio

Posizione	Comportamenti a rischio (secondo i responsabili della sicurezza)	Comportamenti a rischio (secondo gli utenti)
1	**Riutilizzo o condivisione delle password**	Utilizzo di dispositivi professionali per attività personali
2	Clic su un link o download di allegati provenienti da uno sconosciuto	**Riutilizzo o condivisione delle password**
3	Caricamento di dati sensibili su cloud di terze parti non approvato	Collegamento in un luogo pubblico senza utilizzare la VPN
4	Divulgazione di credenziali d'accesso a fonti non affidabili	Risposta a un messaggio (email o SMS) inviato da uno sconosciuto
5	**Accesso a siti web inappropriati**	**Accesso a siti web inappropriati**

Motivi per cui gli utenti compiono azioni pericolose



Cosa motiverebbe gli utenti ad anteporre la sicurezza



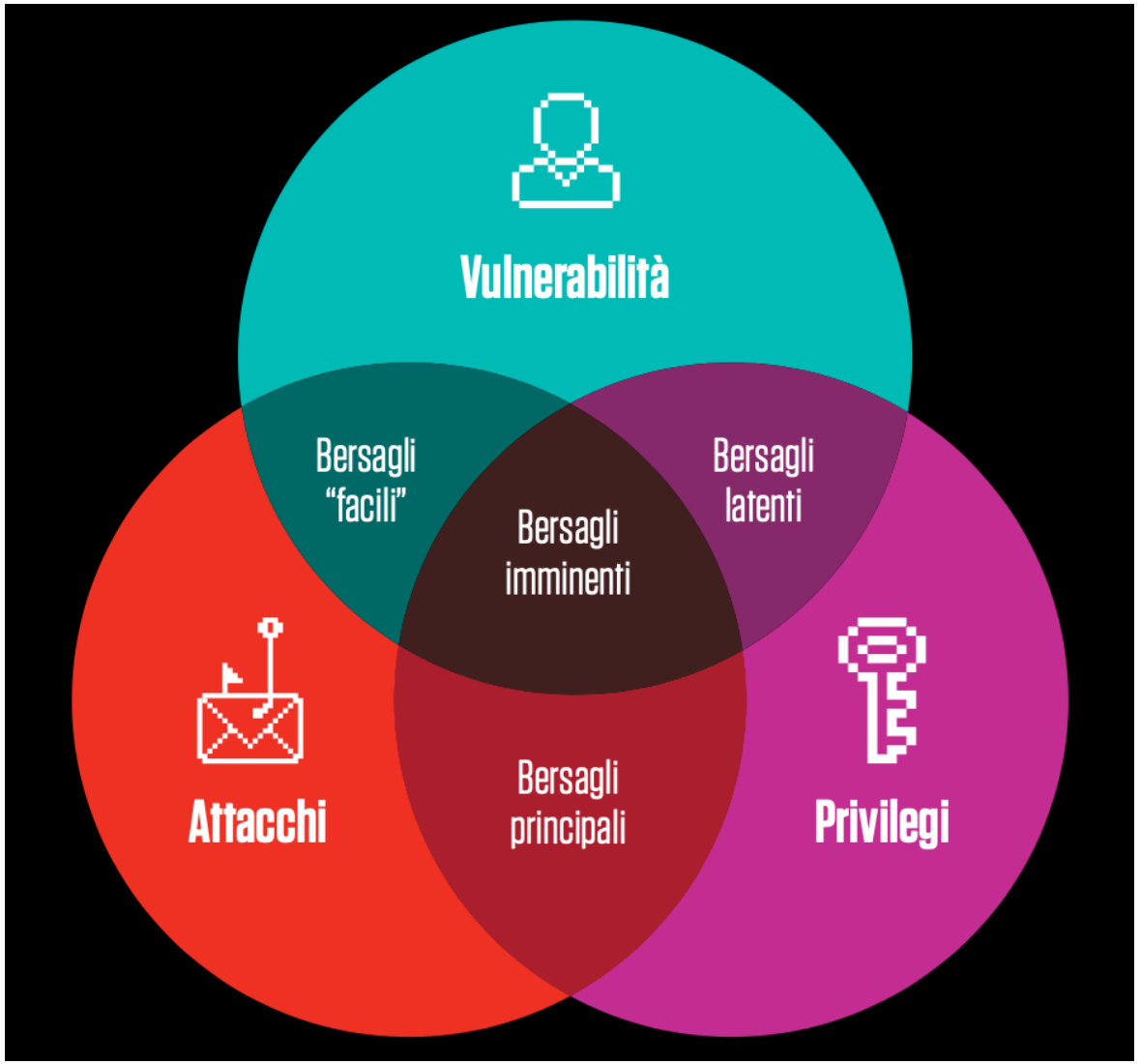
Cost of a Data Breach, IBM 2024

Il costo medio di una violazione dei dati in Italia ha raggiunto i 4,37 milioni di euro nel 2024, a fronte di violazioni sempre più dannose e di un aumento delle richieste ai team di sicurezza".

I costi delle violazioni rispetto al 2023 hanno subito un incremento del 23%, il più alto dai tempi anche postumi della situazione pandemica.

Il 74% degli attacchi andati a buon fine è dovuto al fattore umano (ENISA)

OGNI PERSONA È UNICA



Una nuova metodica formativa

La consapevolezza dei rischi in ambito Cybersecurity è la prima forma di prevenzione in grado di ridurre l'esposizione al rischio.

Le iniziative atte ad instaurare una nuova consapevolezza dei rischi e delle vulnerabilità nell'ambito della sicurezza prevedono una metodica formativa finalizzata ad indurre nei partecipanti il cambiamento del comportamento.

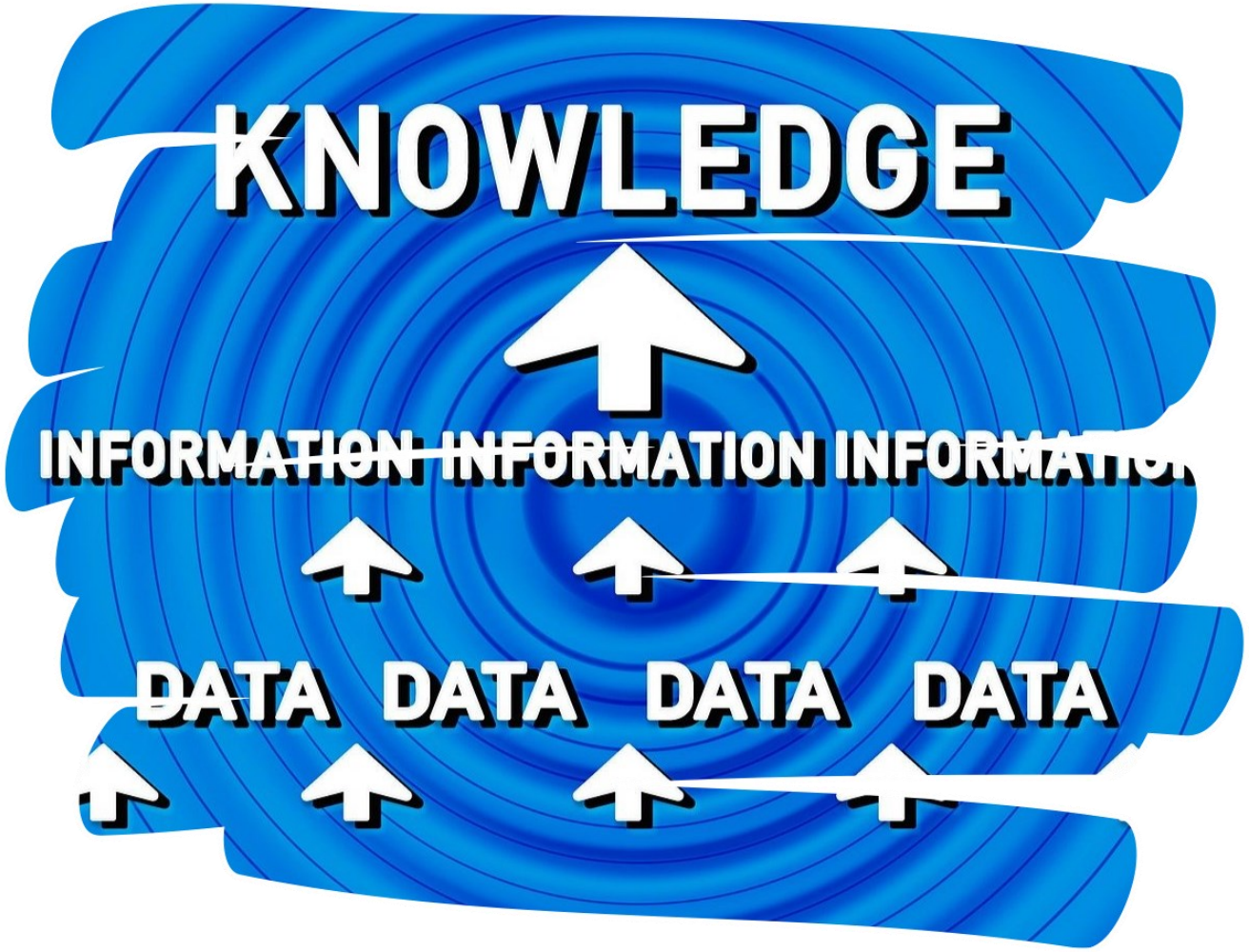
L'introduzione di sistemi di protezione non è sufficiente a prevenire e mettere al sicuro l'azienda da attacchi informatici

Per questo è fondamentale promuovere una cultura aziendale legata ai concetti di cybersecurity.

È dimostrato che attraverso una costante azione di Training & Awareness unita ad attacchi simulati è possibile di ridurre i rischi di phishing e le infezioni malware fino al 90%.

Formazione centrale nella NIS2 e DORA.

Dall’esperienza sul campo alla metodica formativa



La strada che porta alla conoscenza è una strada che passa per dei buoni incontri…

Da dove siamo partiti?

2020

FORMAZIONE CYBER

FORMAZIONE SPECIALISTICA

PIATTAFORME

LA TECNOLOGIA NON BASTA → PROGETTO FORMATIVO

Behaviour-based Cybersecurity Training

+ aspetti cognitivo-comportamentali

- aspetti legati alle competenze

Il feedback dell'utente è il vero scopo finale da raggiungere

l'attivazione è l'elemento utile e benefico alla salvaguardia della realtà in cui è inserito

l'effetto dei rinforzi positivi porta ad interiorizzare il comportamento desiderato assicurandone l'attivazione in modo stabile e duraturo nel tempo

I primi fruitori del nostro servizio

iren
luce gas e servizi

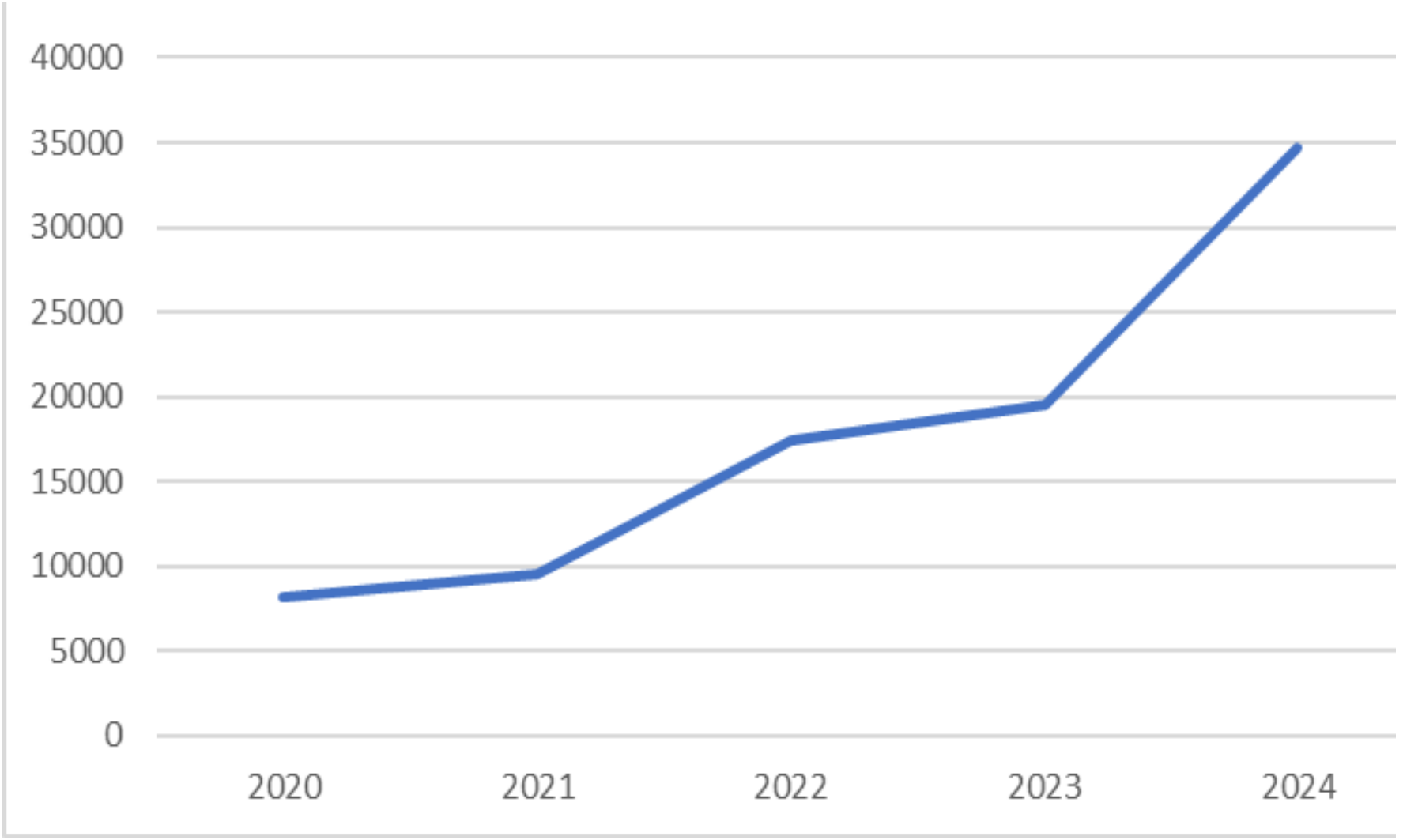
COMUNE DI GENOVA

ITA AIRWAYS

Autorità di Sistema Portuale
del Mar Ligure Orientale
Porti di La Spezia e
Marina di Carrara

PORTS of GENOA
VADO LIGURE ▪ SAVONA ▪ PRA' ▪ GENOVA

I nostri numeri

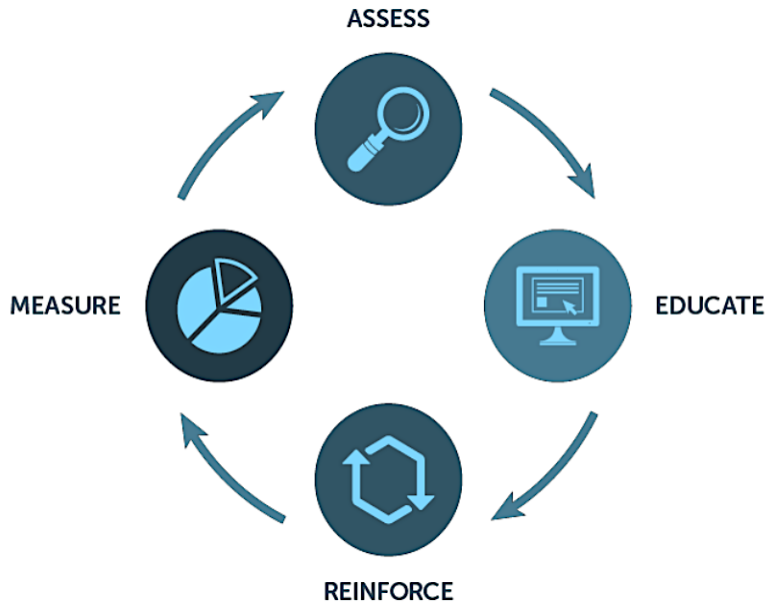


- Il progetto si compone di 3 macro fasi che seguono il ciclo: valutare, istruire, rinforzare, misurare

1. **Assessment**: valuta la consapevolezza degli utenti identificando i rischi all'interno dell'organizzazione e gli utenti a rischio e misurando l'efficacia della formazione. Libreria di 400 domande. L'auto-enrollment assegna automaticamente la formazione agli utenti in base ai risultati.

2. **Campagne di phishing e USB attack**: attacchi simulati con momenti formativi finali. Campagne personalizzabili con libreria di modelli predefiniti e sempre aggiornati. Funzione di auto-enrollment per assegnare la formazione a coloro che cadono vittima dell'attacco simulato.

3. **Formazione**: scegliendo tra più di 80 moduli di formazione interattivi, è possibile educare i dipendenti sulle minacce relative alla cibersicurezza sul posto di lavoro e nella vita privata. I moduli, da 5 a 15 minuti, vengono assegnati al singolo dipendente in funzione delle due fasi precedenti.



Campagne di assessment

Le campagne di assessment sono momenti di **verifica** e di **formazione**.

STRATEGIA DELLE CAMPAGNE:

Le campagne di assessment evolvono seguendo una strategia formativa ben definita e dipendente dall'avanzamento delle attività formative nel loro complesso e dai risultati delle periodiche simulazioni di attacco.

Vengono selezionati i migliori quesiti sulla base dei risultati delle attività globali del piano formativo andando ad evidenziare le maggiori criticità aziendali per poter impostare le contromisure grazie ad azioni formative mirate.

Campagne di phishing

Tra gli **obiettivi** del progetto di **Cybersecurity Awareness** ci sono:

- Preparare le persone a **identificare, gestire e segnalare ogni anomalia** che potrebbe essere sintomo di un attacco
- **Cambiare il comportamento delle persone** nei riguardi di richieste sospette

Questi obiettivi vengono raggiunti attraverso **campagne di phishing**.

STRATEGIA DELLE CAMPAGNE: è prevista una strategia in termini di forma e di contenuti.

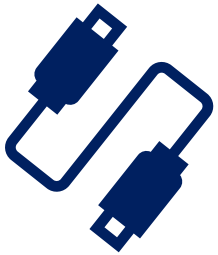
Bisogna prevedere un'evoluzione delle campagne di attacchi simulati sulla base dell'avanzamento delle attività.

Vengono scelti e la personalizzati i migliori layout per la struttura della campagna di attacchi simulati, la definizione delle tempistiche e l'analisi dei risultati in rapporto ai risultati globali del percorso formativo.

Campagne USB

Tra gli **obiettivi** di queste campagne ci sono:

- **Preparare le persone a identificare, gestire e segnalare dispositivi presenti in azienda che potrebbe essere veicolo di un attacco**
- **Cambiare il comportamento delle persone nei riguardi di dispositivi sospetti**



Le campagne USB sono costituite da chiavette USB contenenti file eseguibili che si collegano alla piattaforma e segnalano che è stato aperto un file non sicuro.

Erogazione moduli formativi

Scopri come i ladri possono infiltrarsi nel tuo computer e nella tua azienda se fai clic su un link pericoloso.

Avvia

La nostra piattaforma

- Creata reportistica che analizza dati multipiattaforma
- Analisi congiunta dei dati creati da phishing, formazione e assessment
- Miglior supporto all'adeguamento del piano formativo personalizzato

WE CANNOT CHANGE WHAT WE ARE NOT AWARE OF, AND ONCE WE ARE AWARE, WE CANNOT HELP BUT CHANGE

SHERYL SANDBERG