REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere SICURI?

NIS2: governance e formazione

L’importanza della formazione: costruire una cultura del comportamento sicuro

Paola Girdinio – Docente UNIGE, Presidente START4.0

Nuovi obblighi del CDA secondo la NIS2 (D.lgs 138/2024 art.23)

Approvazione delle misure di cybersicurezza	Il CdA deve approvare le strategie e le misure tecniche e organizzative per la gestione della sicurezza informatica, garantendo la loro adeguatezza ai rischi specifici.
Supervisione diretta	Il CdA è responsabile della supervisione diretta e continua delle pratiche di cybersicurezza, assicurandosi che siano effettivamente implementate e aggiornate.
Formazione obbligatoria	I membri del CdA devono partecipare a programmi di formazione specifici per acquisire competenze adeguate nella gestione dei rischi cyber.
Formazione del personale	Il CdA deve garantire che l'organizzazione promuova una formazione continua e mirata per il personale aziendale, aumentando la sensibilità ai rischi informatici.
Responsabili delle violazioni	Il CdA è ritenuto responsabile delle violazioni relative al D.lgs 138/2024

Misure di gestione del rischio richieste

Politiche di gestione dei rischi	Analisi dei rischi e delle vulnerabilità con documentazione dettagliata
Sicurezza dell'informazione	Protezione sistematica dei dati e dei sistemi
Incident Response	Procedure di gestione degli incidenti di sicurezza con simulazioni periodiche
Continuità operativa	Piani di disaster recovery e business continuity testati regolarmente
Supply Chain Security	Valutazione e gestione dei rischi nella catena di approvvigionamento, con verifiche sui fornitori critici
Autenticazione multi-fattore	Implementazione di sistemi di autenticazione avanzati
Cifratura dei dati	Protezione dei dati sensibili con tecniche crittografiche

Possibili conseguenze per mancata conformità

Ispezioni ad audit	L'Autorità nazionale competente (ACN) può effettuare verifiche (ex post)
Obblighi di conformità	Diffide e imposizione di misure correttive in caso di non conformità
Sanzioni pecuniarie	Sanzioni proporzionate alla gravità della violazione

Per i membri del CDA:

Incapacità temporanea a svolgere funzioni dirigenziali
Art. 32(4) Direttiva NIS2 / Art. 38, comma 6, D.Lgs. 138/2024)

Rimozione temporanea dal ruolo
(Art. 32(4) Direttiva NIS2 / Art. 38, commi 5 e 6, D.Lgs. 138/2024)

Responsabilità legale diretta
(Art. 32(6) Direttiva NIS2 / Art. 38, comma 5, D.Lgs. 138/2024)

La formazione costituisce un cardine centrale dei processi di prevenzione e di mitigazione del rischio cyber nelle aziende.

Necessità di consapevolezza: Il top management deve essere consapevole dei rischi IT e della loro potenziale incidenza sulla sicurezza aziendale.

Ruolo strategico: la cybersecurity non è solo un problema tecnico, ma un aspetto strategico da gestire con attenzione.

Conformità normativa: la direttiva NIS2 richiede una maggiore responsabilità del top management nella gestione della cybersecurity.

Efficacia della formazione: i corsi di formazione devono essere mirati a migliorare la comprensione dei rischi, le capacità di valutazione e la risposta a incidenti.

Formazione continua: la cybersecurity è un campo in costante evoluzione, per cui la formazione deve essere continua per rimanere aggiornati.

Simulazioni di attacchi: le simulazioni di attacchi sono utili per testare la prontezza dell'organizzazione in caso di incidenti.

Ruolo del CISO: Il Chief Information Security Officer (CISO) deve lavorare a stretto contatto con il top management per assicurare una gestione efficace della sicurezza.

La formazione del Top Management

La sicurezza è una responsabilità condivisa: non può essere delegata solo all'IT. Ogni dirigente deve essere consapevole del proprio ruolo nella protezione dei dati e dei sistemi

La cultura della sicurezza va costruita: serve un approccio strutturato che includa comunicazioni chiare, formazione continua e coinvolgimento attivo dei leader

Formazione su misura per il top management: moduli specifici per i vertici, come la "Cybersecurity awareness per Top Management", sviluppato da START4.0, e simulazioni di crisi, per preparare i decisori a rispondere efficacemente agli attacchi

L'importanza della governance: è essenziale che i vertici comprendano le implicazioni normative e strategiche della sicurezza informatica

La formazione del Top Management

Per coloro che si occupano di infrastrutture critiche è necessario contestualizzare e rendere verticale la formazione perché il framework tecnico e normativo è stringente vista la criticità del settore di attività.

- **CER** (Critical Entities Resilience Directive); **Direttiva Macchine**

Deve essere specialistica e approfondita la formazione e l'aggiornamento continuo di IT Manager e CISO (Chief Information Security Officer) su tecnologie e strumenti di analisi e protezione in continua evoluzione che molto spesso richiedono la conoscenza complementare di diverse tecnologie abilitanti.

- Es: convergenza dei mondi OT e IT

La formazione del Top Management

Il Top Management deve saper impostare e gestire il processo relativo alla sicurezza aziendale mettendo le **risorse opportune** e stabilendo un **budget correttamente dimensionato.**

Il CDA deve comprendere a fondo il quadro normativo al fine di avere contezza sulle importanti **responsabilità che i membri di ogni CdA** hanno **in caso di violazione** della sicurezza aziendale e in caso di **non adeguamento alle normative,**

spesso non è noto che i membri del CdA hanno la responsabilità del piano di continuità aziendale in seguito ad un attacco.

Fondamentale coordinamento con CdA e Top Managment per realizzare approccio sistemico

Questo permette **di tenere sotto controllo il perimetro aziendale** per **capire le vulnerabilità** e la loro evoluzione nel tempo, **impostando** gli **strumenti e le corrette misure di protezione.**

La tecnologia non basta, necessari **processi aziendali** in cui definire misure di protezione, a seguito di un attacco, tramite **piani di business continuity** e di **disaster recovery.**

E tutti gli altri?

FORMAZIONE SPECIALISTICA

FORMAZIONE CYBER

PIATTAFORME

LA TECNOLOGIA NON BASTA → PROGETTO FORMATIVO

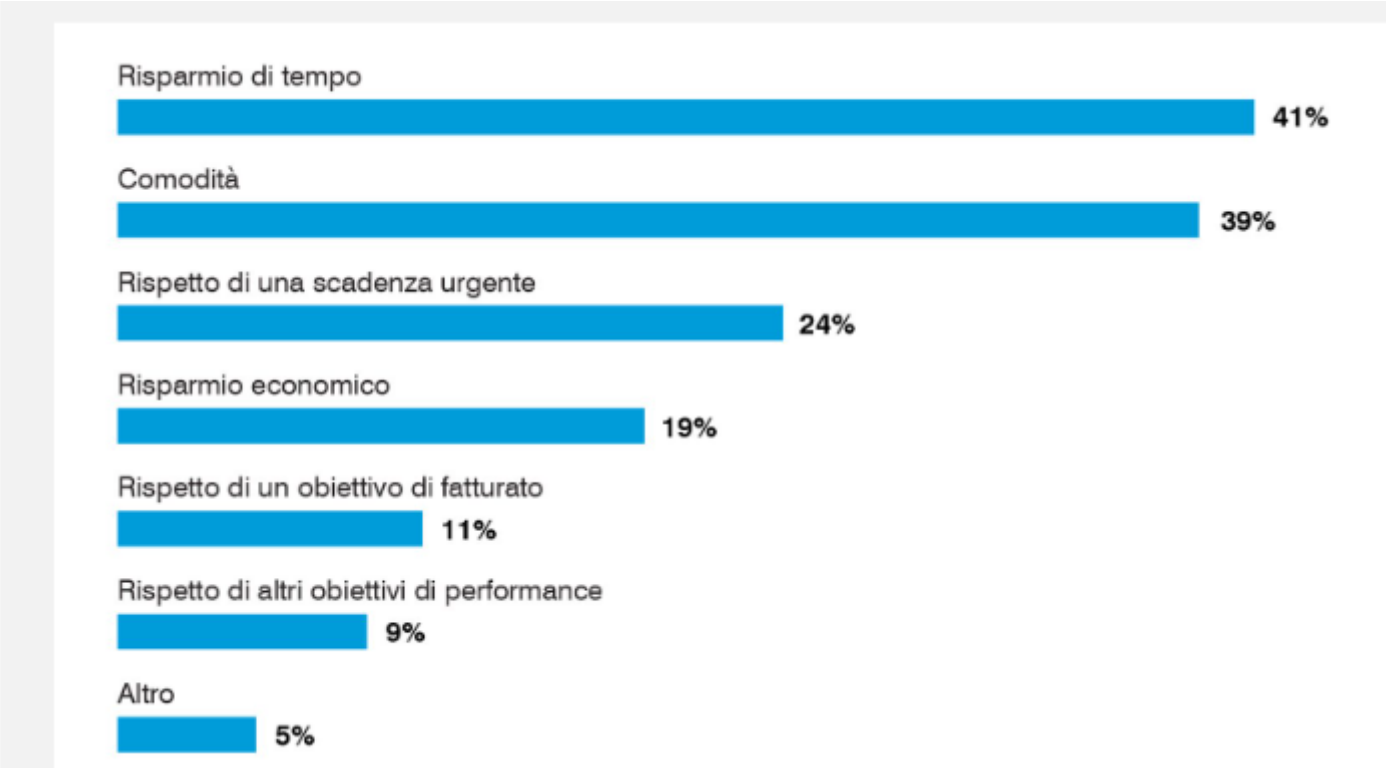
Cost of a Data Breach, IBM 2024

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.

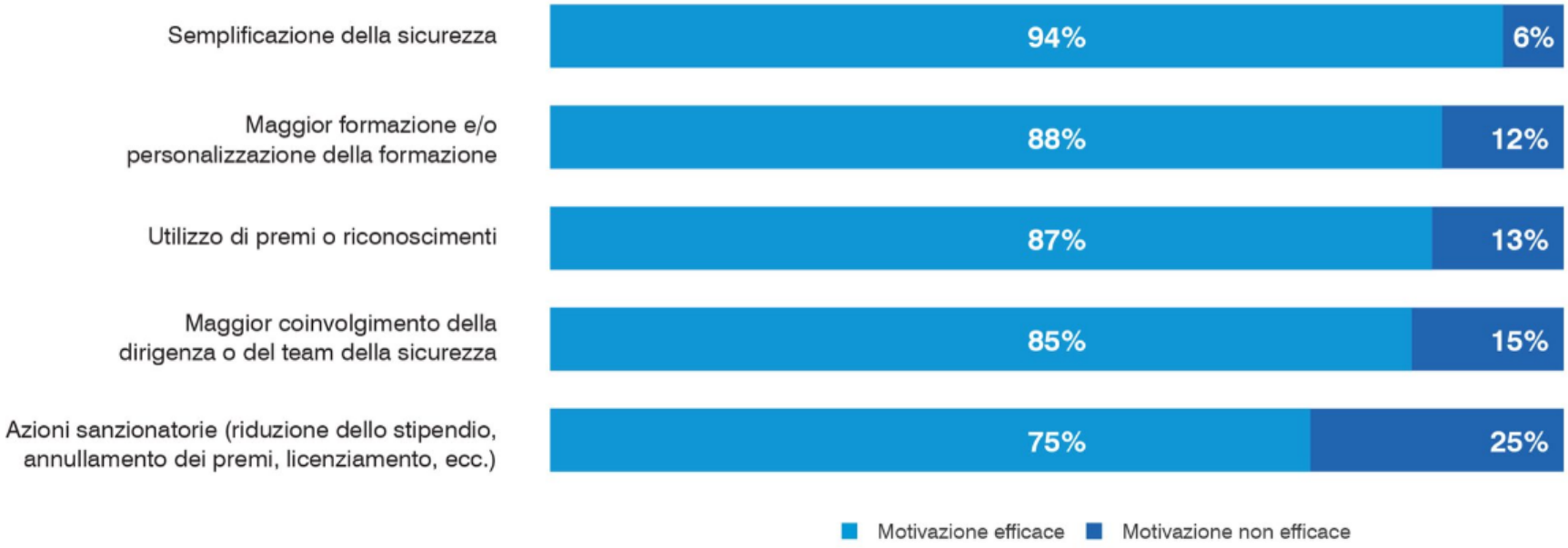
Il 74% degli attacchi andati a buon fine è dovuto al fattore umano (ENISA)

Motivi per cui gli utenti compiono azioni pericolose



Sondaggio State of the Phish 2024, ProofPoint

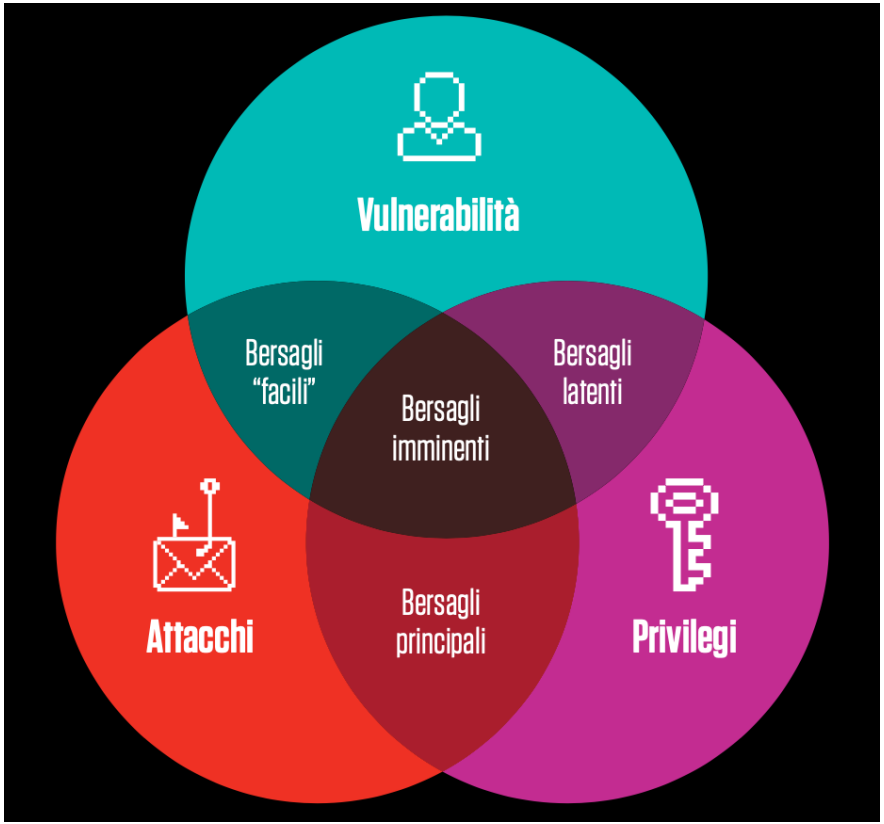
Cosa motiverebbe gli utenti ad anteporre la sicurezza



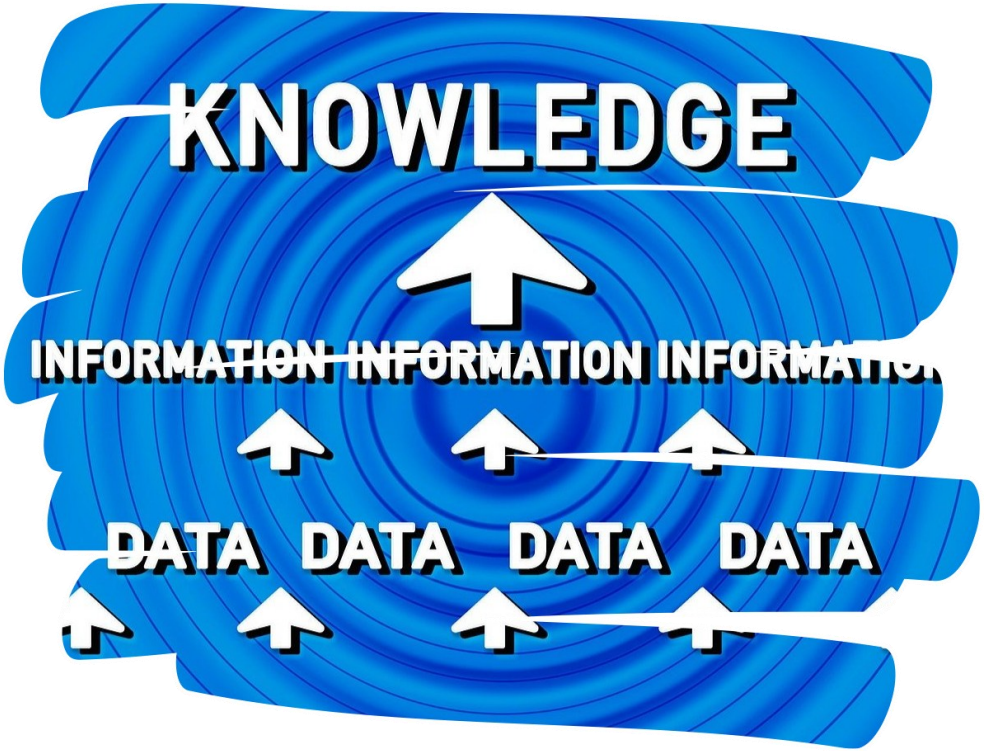
Sondaggio State of the Phish 2024, ProofPoint

Analisi approfondita del rischio legato al fattore umano

OGNI PERSONA È UNICA



Dall’esperienza sul campo alla metodica formativa



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

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 per 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

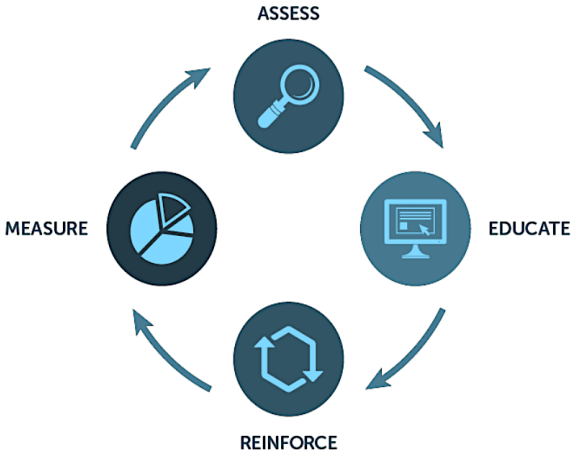
Macrofasi

- 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.

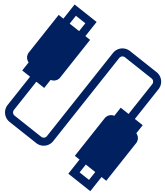
Bisogna prevedere un'evoluzione delle campagne di attacchi simulati sulla base dell'avanzamento delle attività.

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**

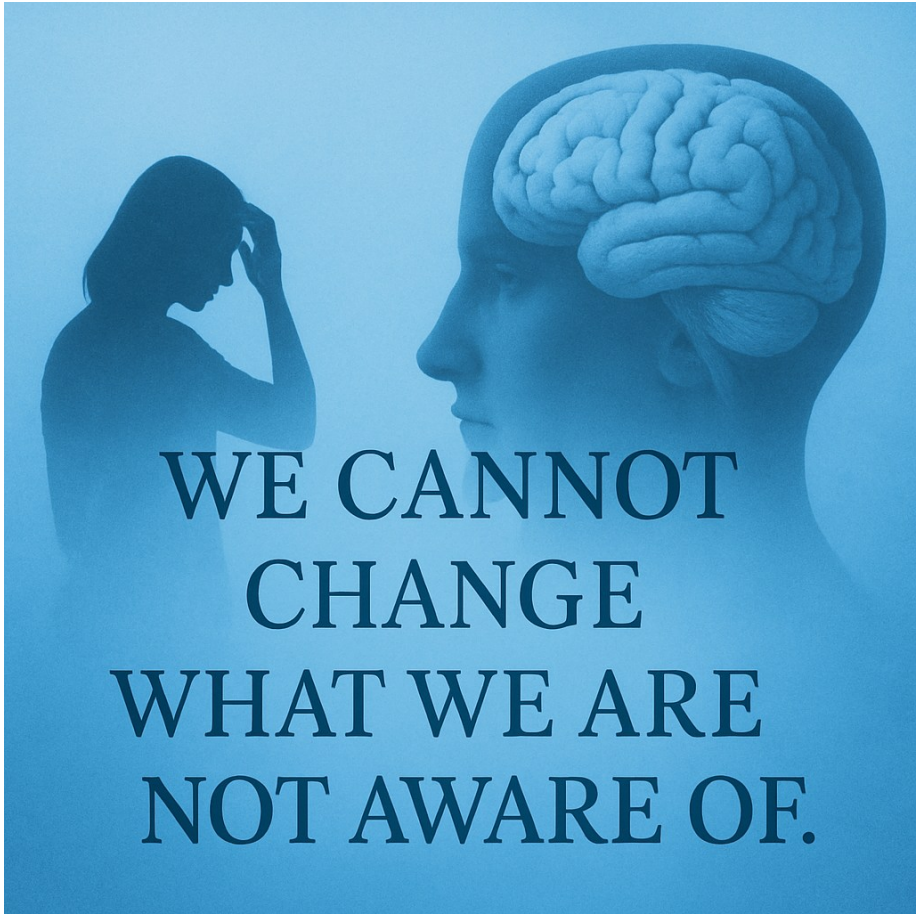


Le campagne USB sono costituite da chiavette USB contenenti file eseguibili che si collegano alla piattaforma e segnalano che è stato aperto un file non sicuro.

Erogazione moduli formativi

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

Avvia



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

SHERYL SANDBERG