

Propensione al Rischio - Risk appetite



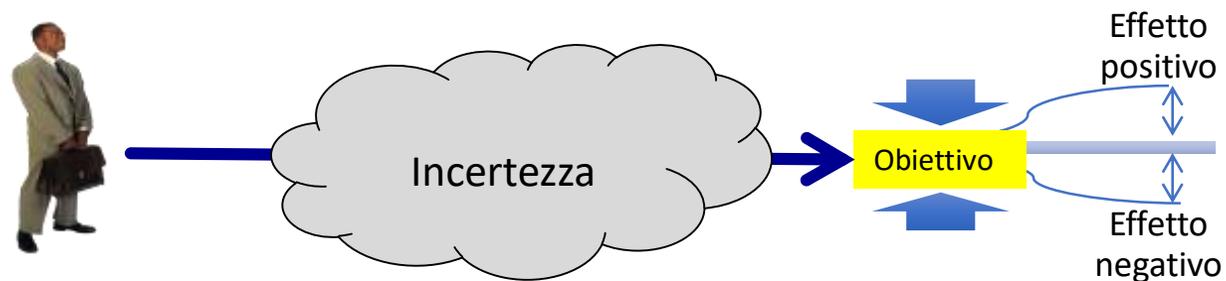
Pensiero basato sul RISCHIO – Risk based thinking



IL RISCHIO: Il concetto del rischio

Effetto dell'incertezza sugli **obiettivi**

(Source: ISO Guide 73 e ISO 31000)



Il Rischio è definito come

“*grado di esposizione dell'obiettivo all'incertezza*”

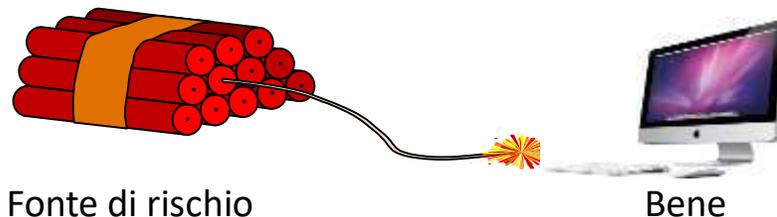
IL RISCHIO: Il concetto del rischio

Effetto dell'incertezza sugli obiettivi

(Source: ISO Guide 73 e ISO 31000)

In riferimento all'**incertezza** il Rischio dipende dai seguenti due elementi:

- **dall'incertezza**, intesa come **conoscenza** di un evento e delle relative condizioni di contorno che si manifesta nei confronti dell'obiettivo da soddisfare;
- **dall'esposizione dell'obiettivo all'incertezza**, intesa come conseguenza, impatto, danno, magnitudo.



$$\text{Entità di Rischio } R = f (P, D)$$

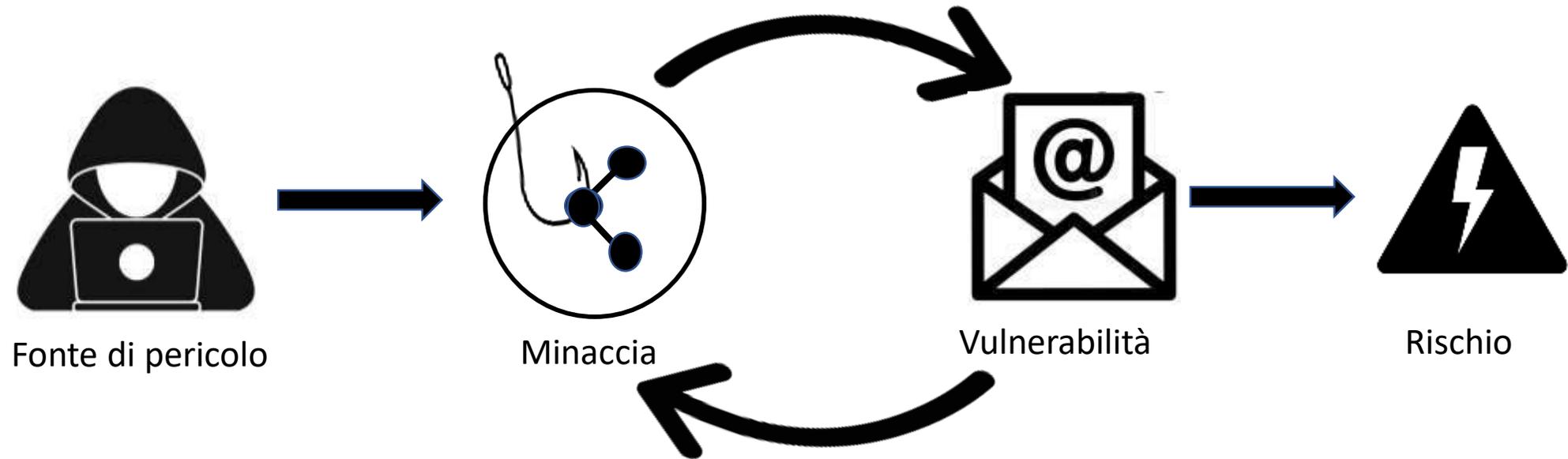
Ove:

P: è la **Probabilità** o la **Frequenza** dell'incidente in considerazione.

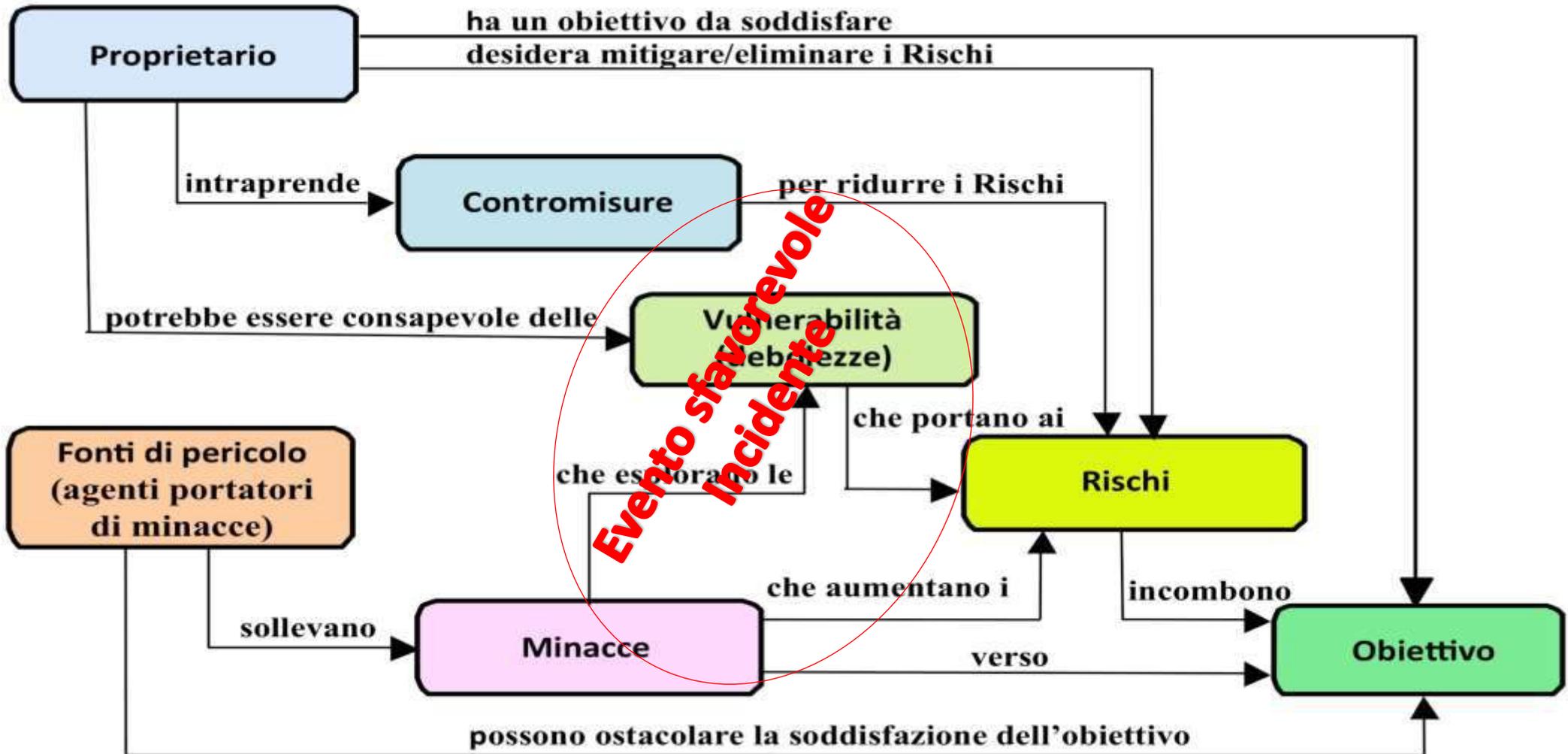
D: è il Magnitudo del danno, la massima **conseguenza/impatto** dell'incidente sull'**Obiettivo**.

f: è la funzione scelta per combinare **P** e **D** e dipende dal modello usato per l'analisi.

Come nasce un **RISCHIO**



IL RISCHIO: gli elementi coinvolti nel rischio



Entità di Rischio: $R = f(P, D)$



***Il valore di una formazione profusa
a tutti i livelli aziendali***

 **Telsy** | A TIM
ENTERPRISE
BRAND


UNOWEB[®]
COMMUNICATIONS

La comunicazione pietra angolare della società





Le attività di un individuo, nella sua interazione con il web, possono mettere a rischio la sua sicurezza, quella dell'organizzazione di cui fa parte e tutta la catena di fornitori (supply chain)



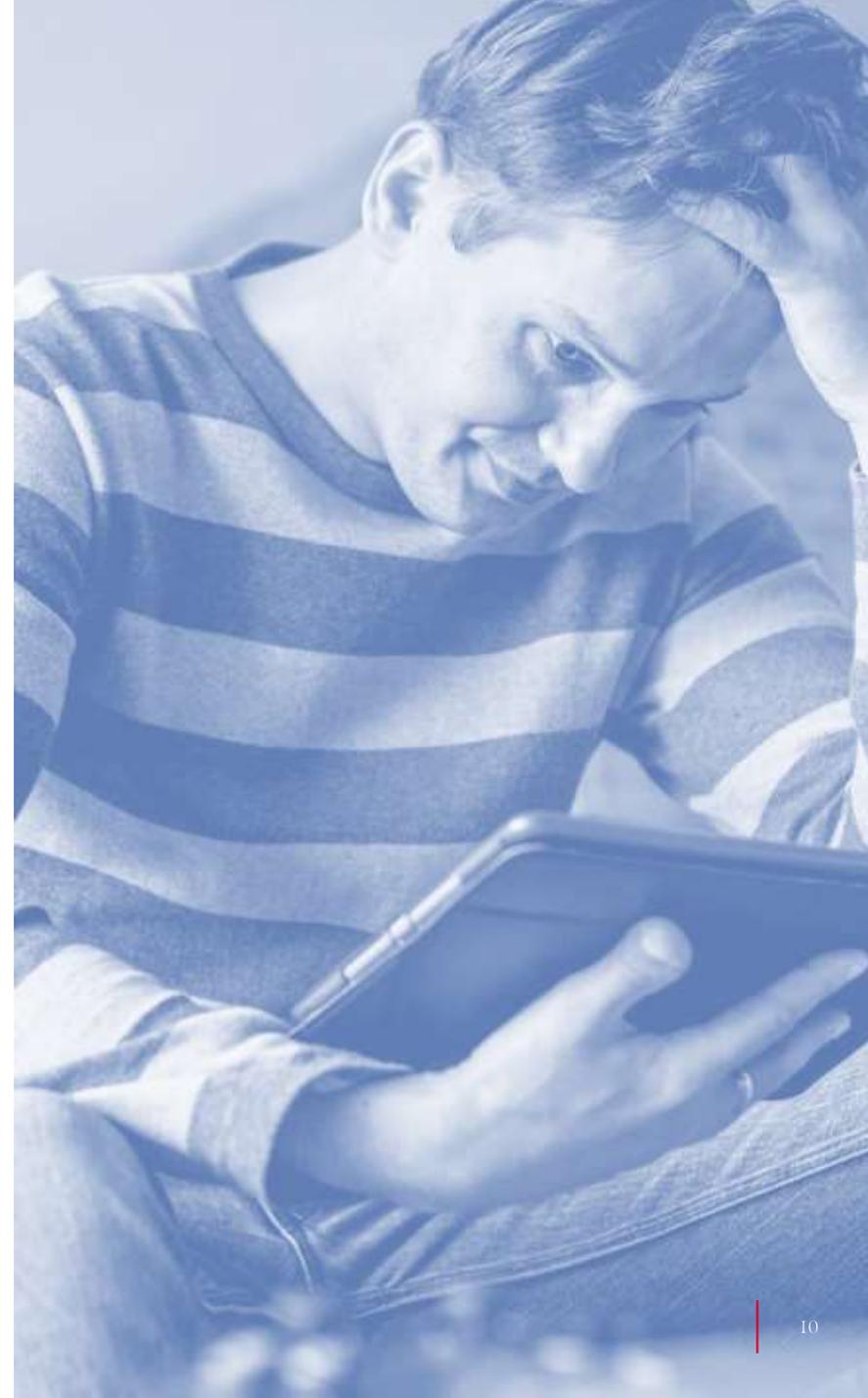


L'**anello debole** della
cybersecurity è legato al
comportamento umano

82%

degli incidenti causato da un
errore umano

*Verizon; 2022 Data Breach Investigations
Report; <https://www.verizon.com/business/resources/reports/dbir/>*

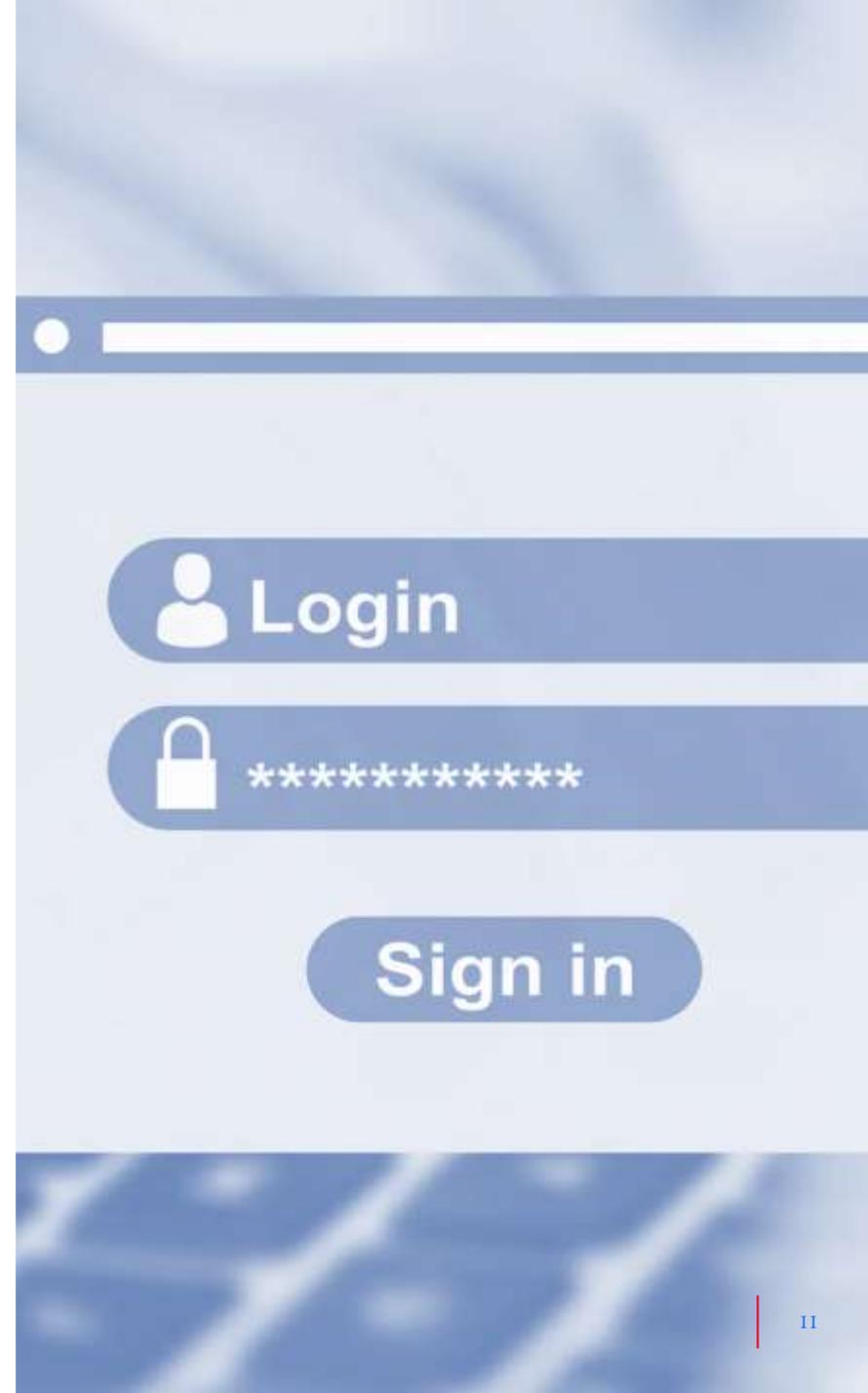




Gli errori più ricorrenti

Il **57%**
genera password deboli
e le conserva in modo improprio

Gartner; 2022; IG_766511_When_Security_Awareness



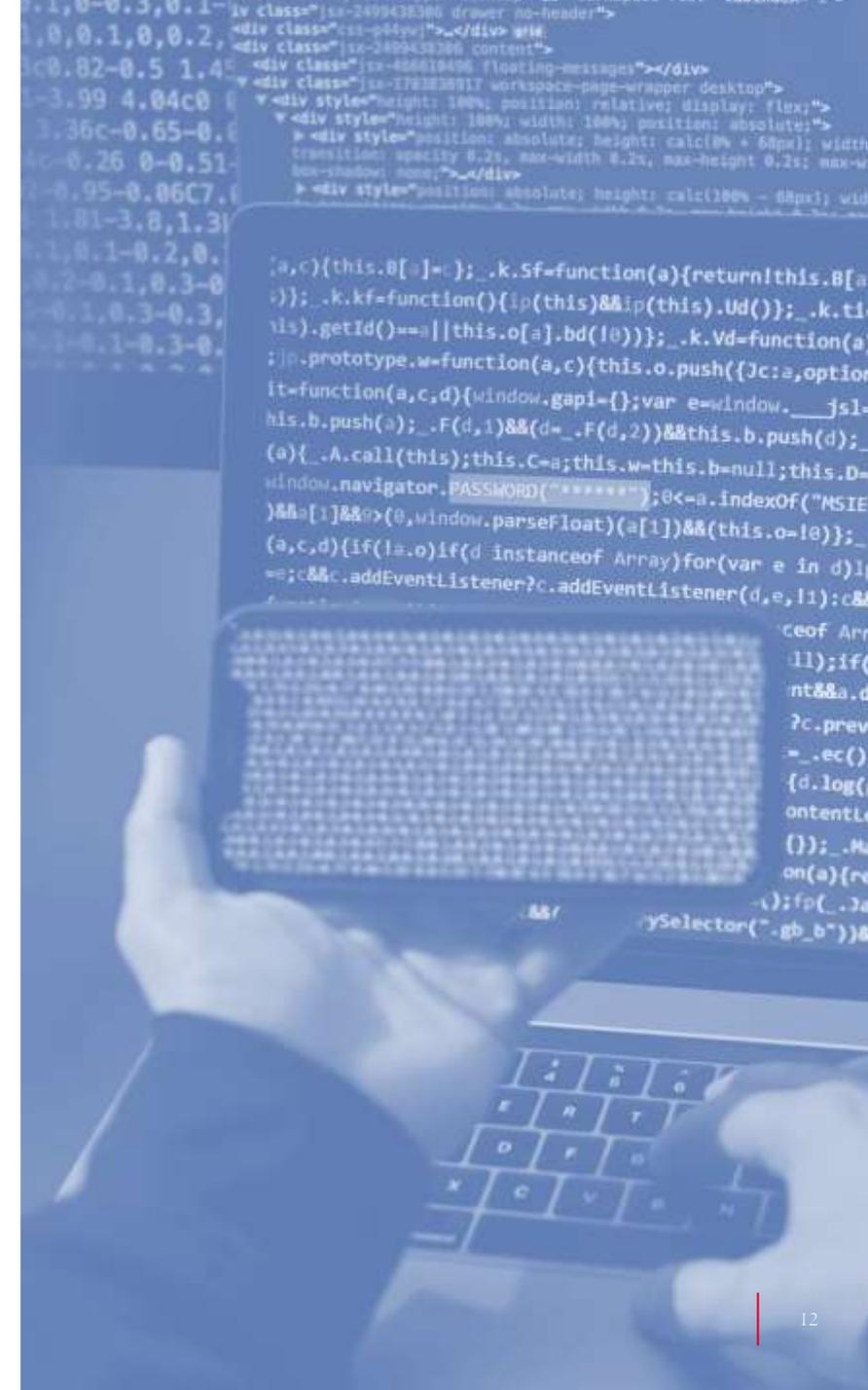


Gli errori più ricorrenti

Il **35%**

condivide informazioni sensibili
(es. internet oversharing sui social media)

Gartner; 2022; IG_766511_When_Security_Awareness



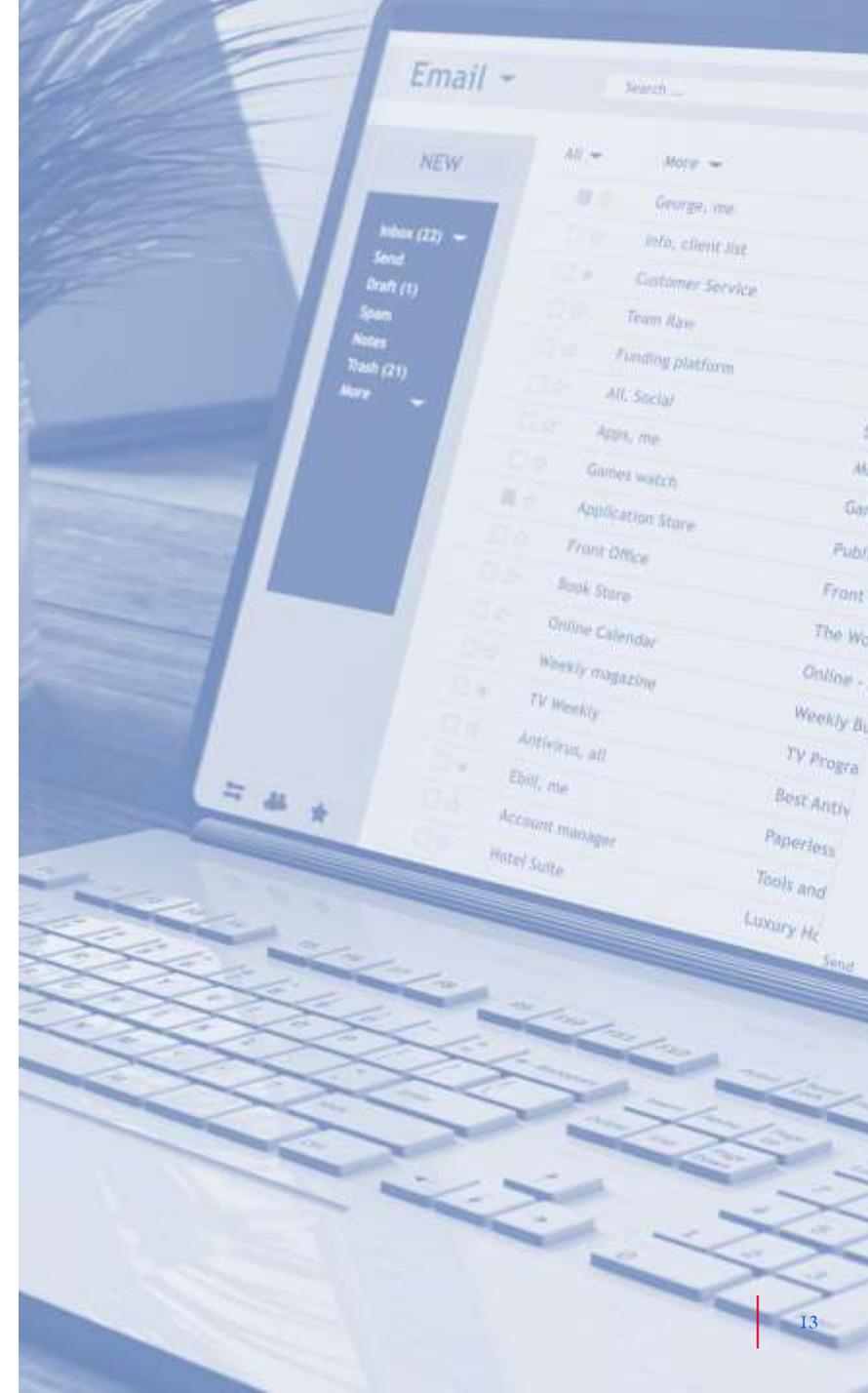


Gli errori più ricorrenti

Il **36%**

degli impiegati **apre e-mail**
da **utenti** o **fonti sconosciute**

Gartner; 2022; IG_766511_When_Security_Awareness





***La formazione tradizionale ha
mostrato chiari limiti di
efficacia***



La piattaforma

Al fine di migliorare la qualità della formazione, è più efficace l'uso di una **piattaforma modulare ed interattiva** che aiuta a sviluppare una chiara consapevolezza del rischio cyber.

Il fine è **migliorare la postura digitale degli utenti** per ridurre la componente di vulnerabilità legata all'errore umano.



Dati in Italia



Reportistica integrata



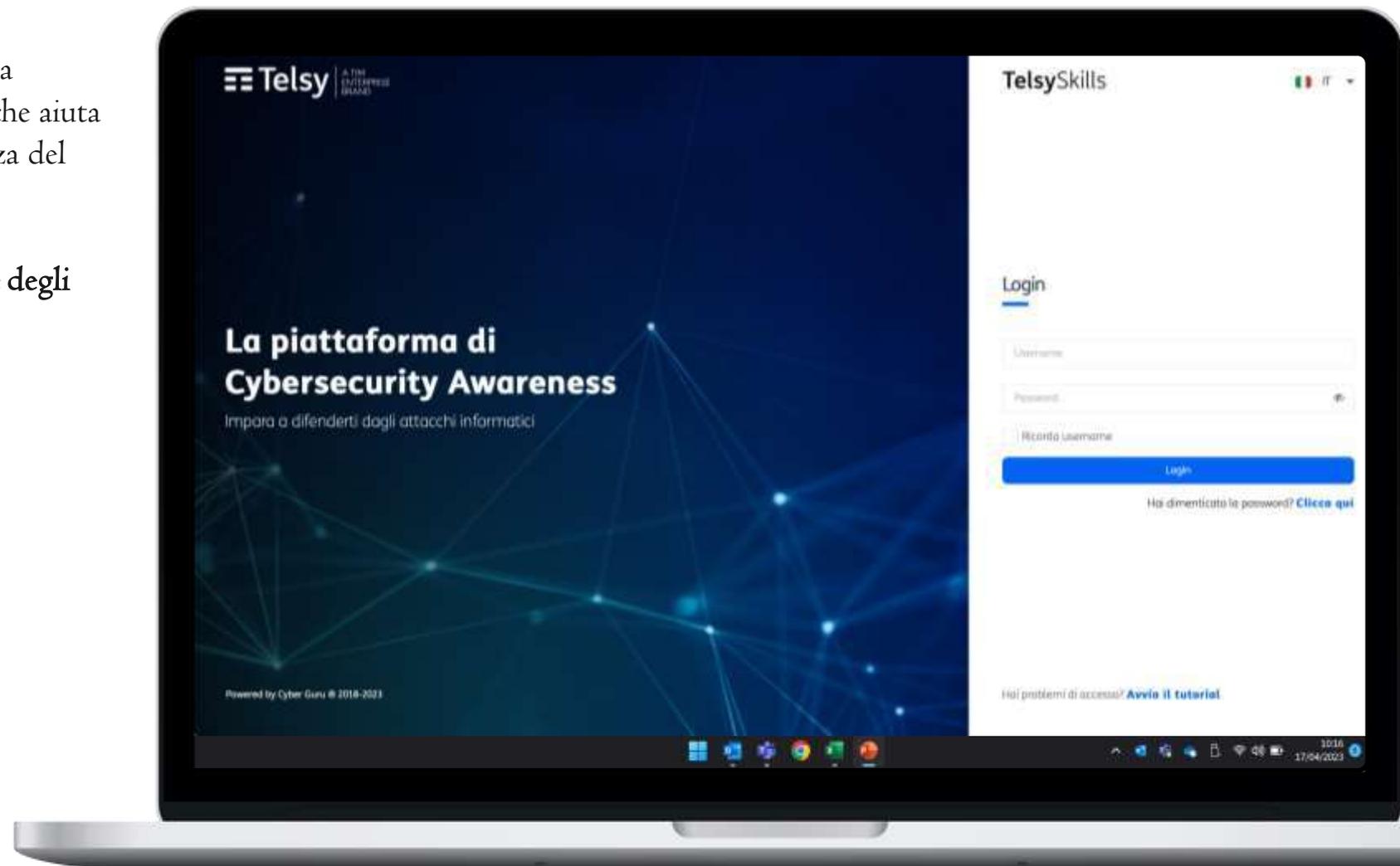
Multilingua e multidevice



Help Desk dedicato



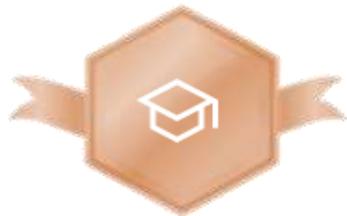
In cloud con impatto zero



I Contenuti

La piattaforma dovrà consentire la fruizione di **moduli di e-learning interattivi**, vedere **micro video** e gestire campagne di **addestramento anti-phishing**.

La stessa può essere navigata per accedere a **contenuti extra** come le **ultime news**, l'**enciclopedia cyber** ed **ulteriori pillole video esclusive**.



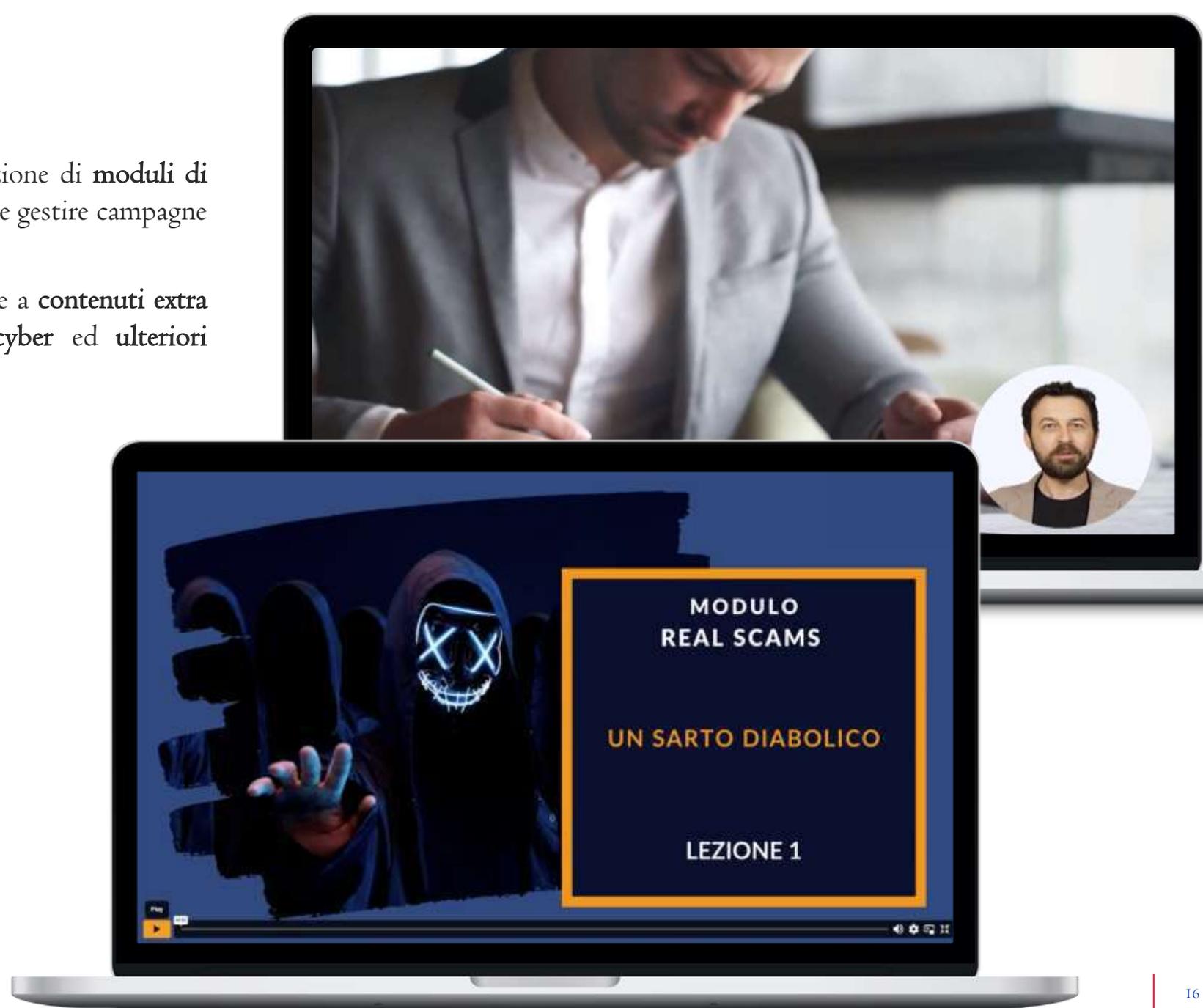
Awareness

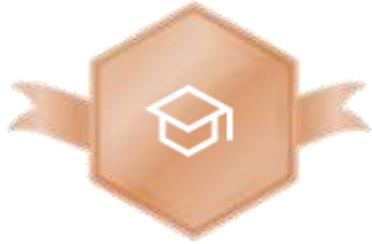


Channel



Phishing





Awareness

Un percorso di apprendimento
dinamico, stimolante ed interattivo
per rendere i dipendenti più
consapevoli nell'utilizzo degli
strumenti web



Apprendimento **cognitivo**



Formazione **continua** e **pluriennale**:
36 moduli in 3 anni



Micro-lezioni video con attori coach



Gamification individuale e aziendale



Multidevice e **multilingua**
(anche da smartphone o tablet)

Awareness (2 di 2)

Primo anno

- Phishing
- Password
- Social
- Privacy & GDPR
- Mobile Device & APP
- Fake News
- USB Device
- Malware
- Email Security
- Web Browsing
- Critical Scenarios
- Social Engineering

Secondo anno

- Clean Desk
- Smart working
- Social collaboration e video conferencing
- Smishing & Vishing
- Spear Phishing
- Sneaky Phishing
- IoT Device
- Bluetooth & WIFI
- Information Classification
- Data Protection
- Personal Identifiable information
- Social Engineering 2

Terzo anno

- Privacy
- Social & Cyberbullying
- Legal Aspect
- Real SCAM I
- Real SCAM 2
- Malware 2
- E-commerce
- Holiday & Business trip
- Cyber Hygiene
- Backup & restore
- Best practice
- Social Engineering 3

Singola
annualità

12 Moduli

La piattaforma sblocca **un modulo al mese** nel corso dell'annualità. Può essere prevista una diversa calendarizzazione.

36 lezioni

Ogni modulo è composto da **3 lezioni video** della durata di 5-7 minuti ciascuna (fruibile anche per mezzo della lettura del relativo pdf)

36 test di apprendimento

Dopo ogni lezione è presente **un test di apprendimento**

4 test di consolidamento

Ogni 3 moduli l'utente sarà sottoposto ad **un test di consolidamento**



Attestato

Al completamento dei moduli di ogni annualità, l'utente potrà scaricare il proprio **attestato**



Channel (I di 2)



Channel

Serie di brevi video
sui rischi cyber con uno
storytelling innovativo,
coinvolgente ed immersivo



Apprendimento **induttivo**



Formazione continua e pluriennale:
36 video in 3 anni



Episodi video tipo Stagioni TV con contenuti
speciali e sempre aggiornati



Multidevice e multilingua
(anche da smartphone o tablet)

Channel (2 di 2)

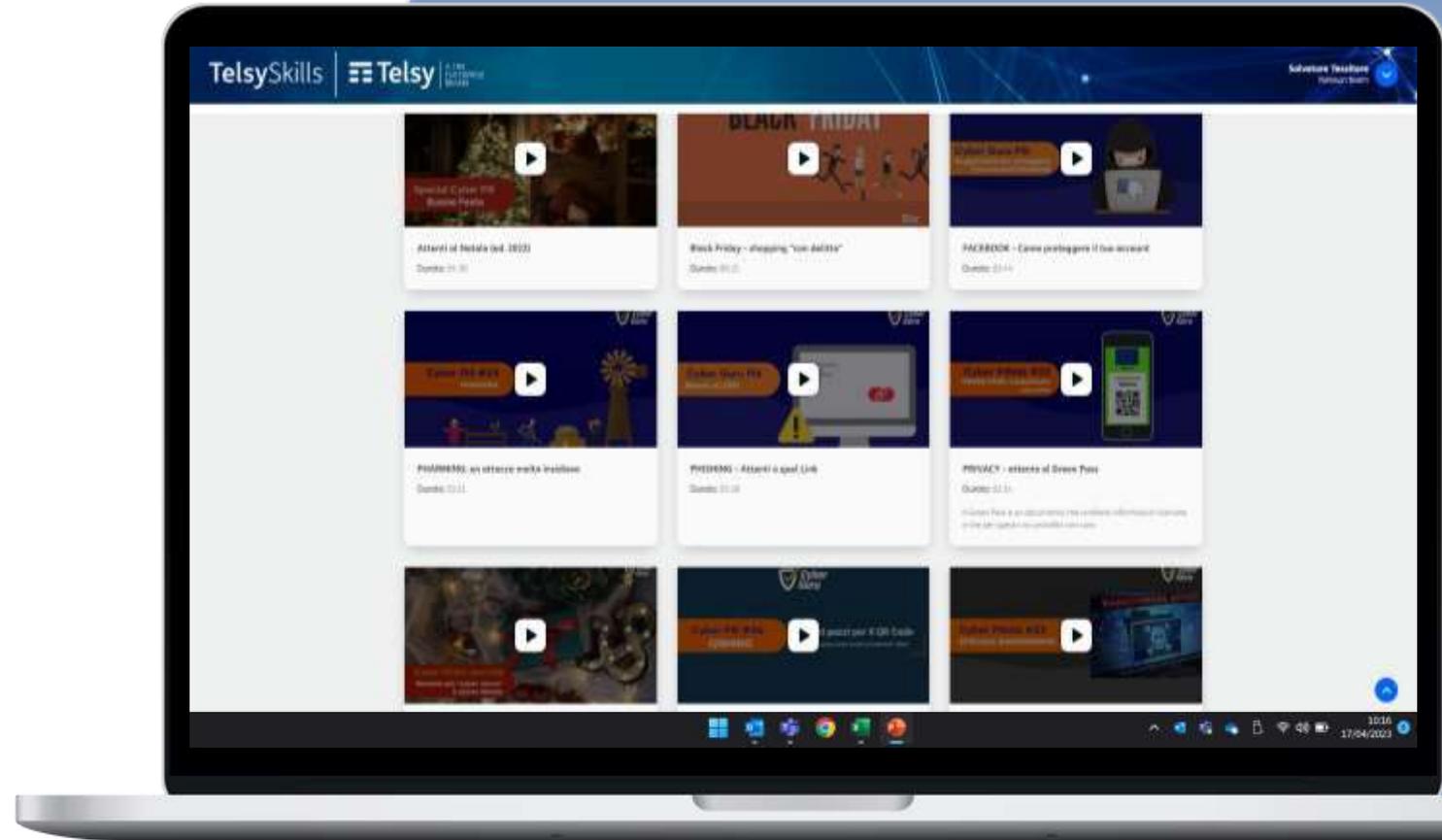
Prima Serie

- 1° episodio - Dal paradiso all'inferno in un click
- 2° episodio - La tempesta perfetta
- 3° episodio - E' solo un gioco!
- 4° episodio - Per un "pugno" di canzoni
- 5° episodio - Impigliata nella rete
- 6° episodio - Il peggiore affare di sempre
- 7° episodio - Le vie dei truffatori sono infinite
- 8° episodio - Impara a leggere!
- 9° episodio - L'insostenibile leggerezza del conto in banca
- 10° episodio - In troppi vogliono essere nei vostri panni
- 11° episodio - La tecnica del cocodrillo
- 12° episodio - Rimborso fatale

Seconda Serie

- 13° episodio - Tutti pazzi per gli sconti
- 14° episodio - Una pesca fruttuosa
- 15° episodio - Se telefonando
- 16° episodio - Parcheggi "pericolosi"
- 17° episodio - Provare, ma senza dimenticare
- 18° episodio - Copia con troppa conoscenza
- 19° episodio - Foto ricordo...da dimenticare
- 20° episodio - Galeotta fu l'e-mail
- 21° episodio - Oltre le apparenze
- 22° episodio - Una donazione "sbagliata"
- 23° episodio - Post Pericolosi
- 24° episodio - Una vacanza molto "costosa"

☀ *Terza Serie disponibile entro Q4 2023*



Phishing (I di 2)



Phishing

Addestramento con campagne che simulano attacchi mirati di phishing e smishing



Apprendimento **esperienziale**



Programma di **attacco simulato** con **ricalibrazione della difficoltà** degli attacchi simulati **tramite AI**



Personalizzazione della **tipologia** di campagne e della **frequenza** di invio



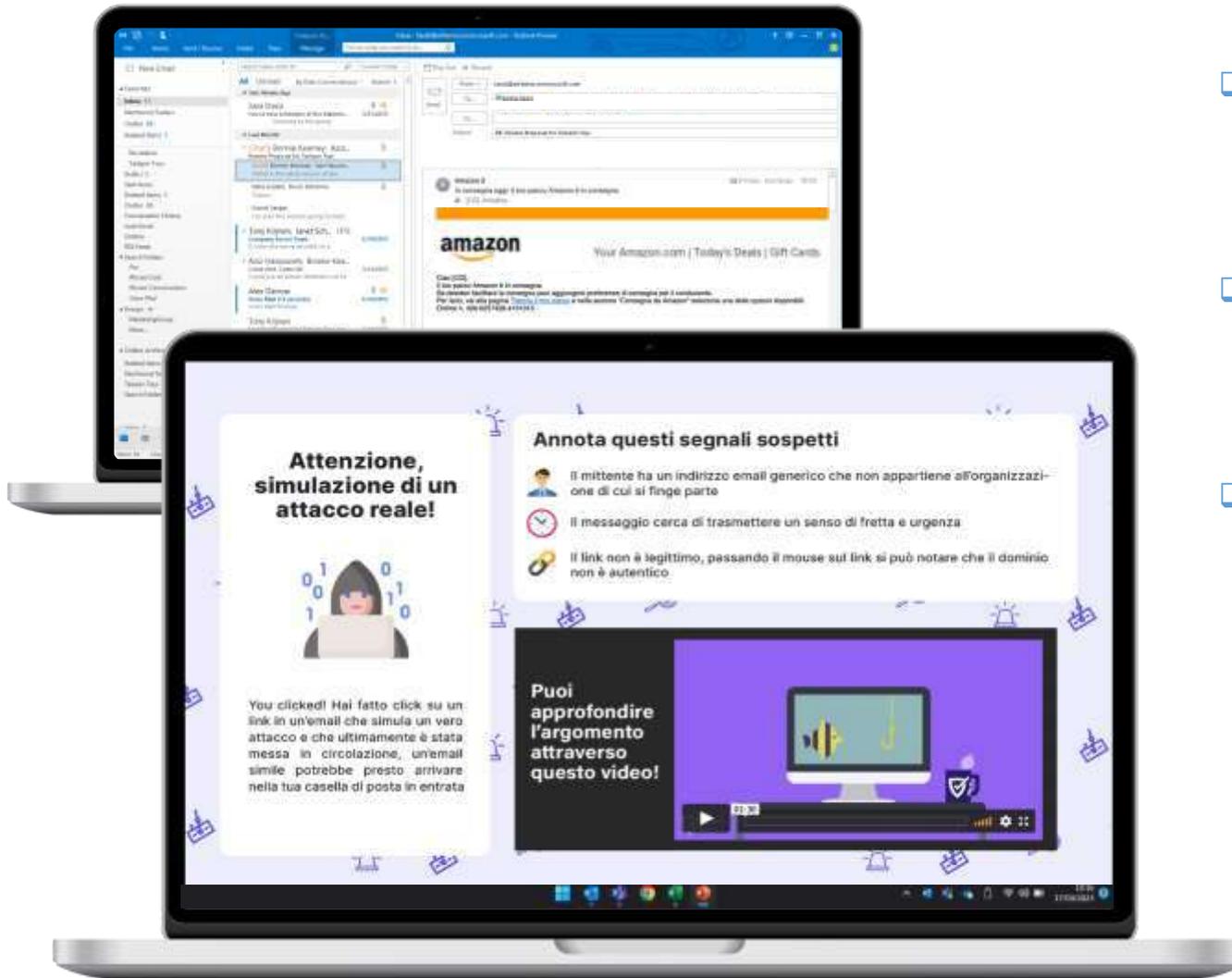
Reportistica con analisi di numerosi indicatori di rischio ed efficacia



Garanzia di **efficacia** e aumento della **resilienza** dei dipendenti

Help Desk

Phishing (2 di 2)

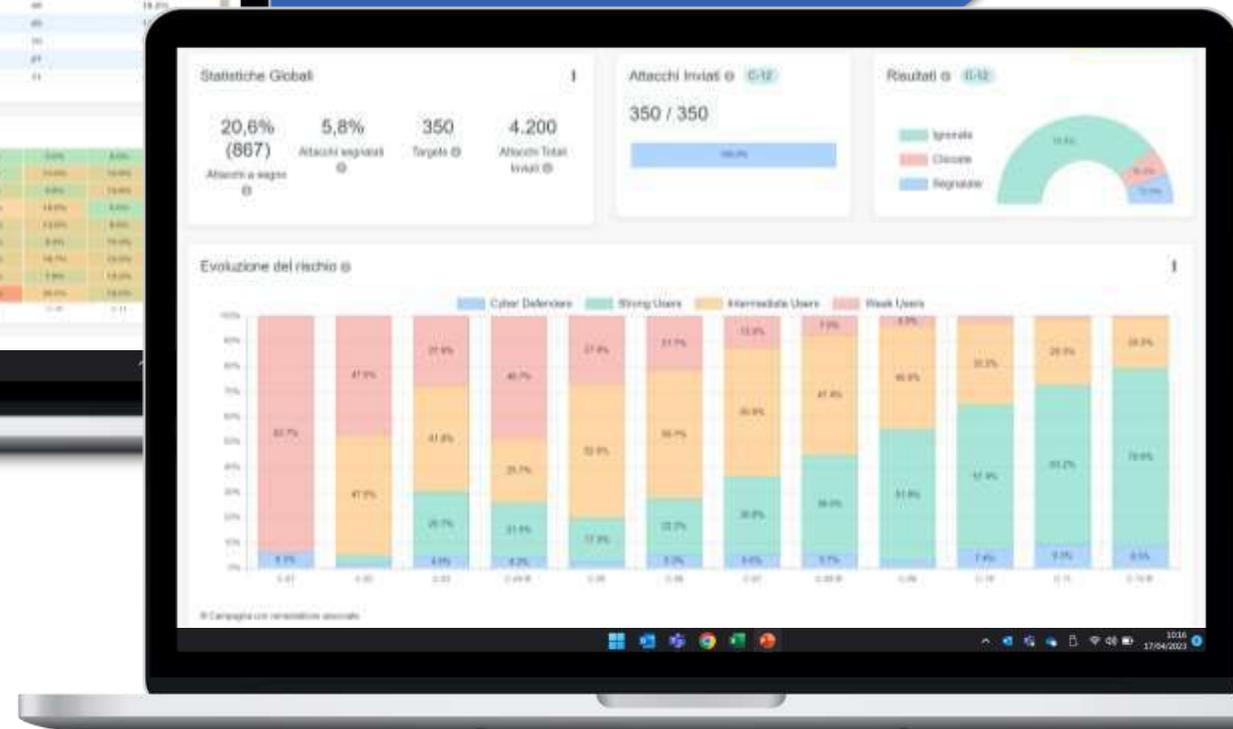
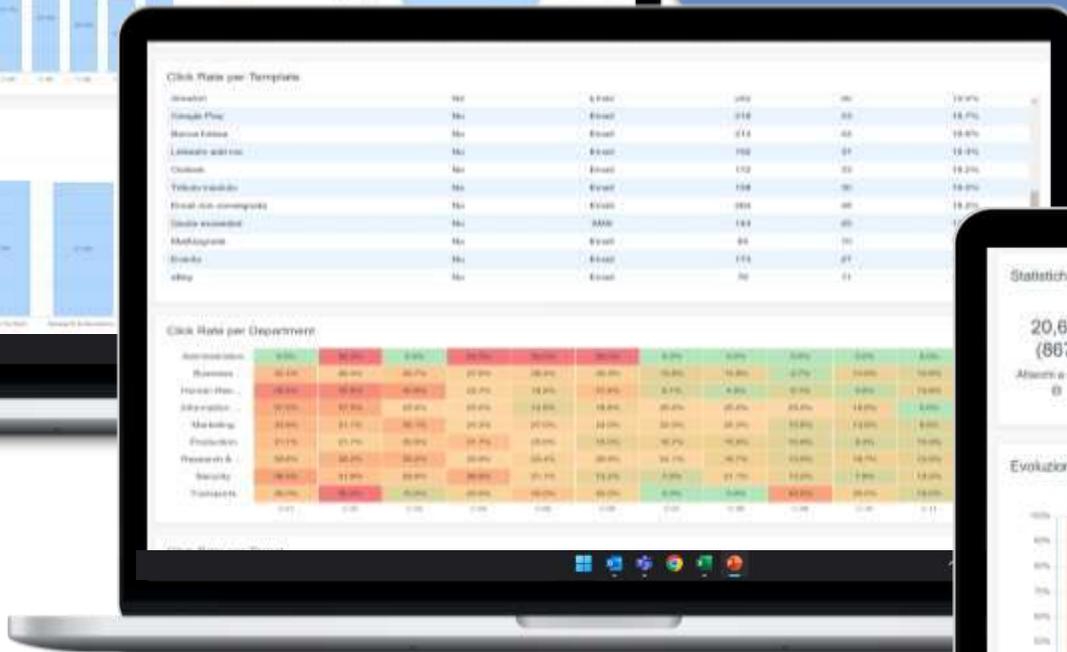
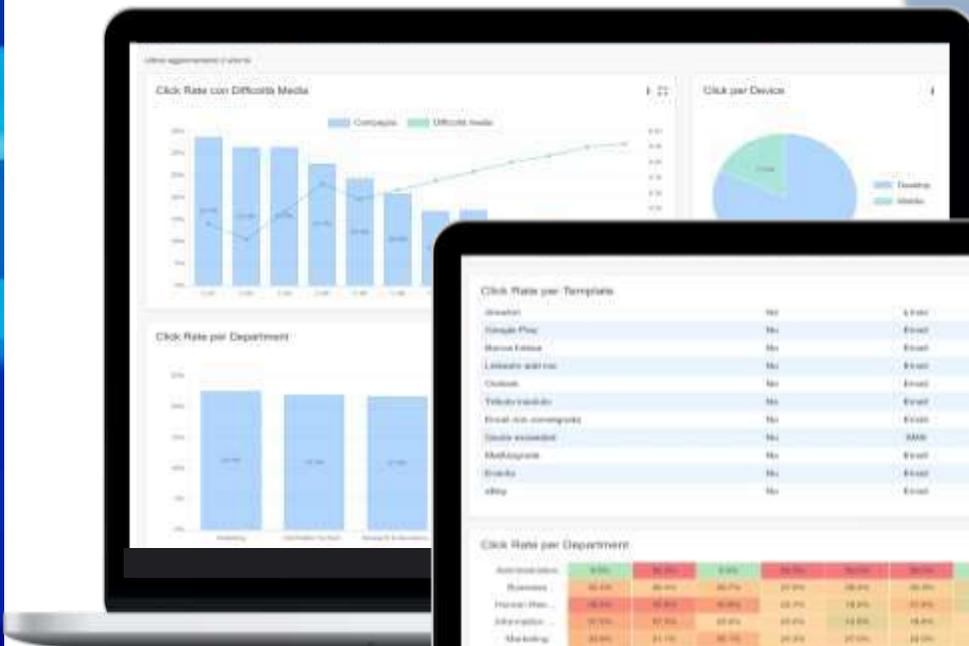


- ❑ Ogni campagna potrà avere un **diverso orario di invio e template differenziati** per evitare il passaparola
- ❑ La durata standard della singola campagna è stimata in **4 settimane**. Dopo le prime 3 campagne il motore di **AI studia il comportamento** in base alle risposte del singolo destinatario per calibrare il livello di difficoltà degli invii successivi
- ❑ La piattaforma può evidenziare attraverso una dashboard **l'andamento delle campagne**, la risposta degli utenti e numerose altre metriche utili per verificare l'efficacia del percorso e la resilienza dei dipendenti
- ❑ Sulla base di quanto emerge dalle statistiche, si può decidere di **avviare campagne mirate** su un determinato cluster





Reportistica dedicata



Help Desk





Help Desk dedicato

a

Assistenza nella configurazione iniziale per l'avvio e la calendarizzazione del programma di formazione e di addestramento

b

Assistenza continua per ridurre l'impatto lato Cliente (da parte della funzione Risorse Umane, IT o Sicurezza)

c

Aggiornamenti periodici per analizzare l'andamento del programma di formazione, analizzare la reportistica e decidere ulteriori interventi nelle aree più deboli



La piattaforma di riferimento, potrà essere completa di security awareness per agevolare il riconoscimento degli attacchi cyber e meglio comprendere come potersi difendere.



Servizio in **cloud** ad **impatto zero** per le funzioni HR, IT o Security



Reportistica per monitorare l'efficacia della formazione



Multilingua e **multidevice** (anche da smartphone o tablet)



Help Desk dedicato



Dati in Italia

Grazie

Fabio Luigi Ghioldi

CEO UNIWEB

Fabio.ghioldi@uniweb.it

Mauro De Maria

TELSY
Technical Marketing & Innovation
Manager

mauro.demaria@telsy.it

 **Telsy** | A TIM
ENTERPRISE
BRAND

 **UNIWEB**®
COMMUNICATIONS

info@uniweb.it
www.uniweb.it