

UNA PROSPETTIVA SISTEMICA AL PROBLEMA DELLO HUMAN FIREWALL (HFP): L'APPROCCIO AWAKE

Università Cattolica del Sacro Cuore (UCSC)

Sedi di Milano, Brescia, Piacenza-Cremona e Roma

Scheda di sintesi del progetto (max 2000 caratteri spazi inclusi)

L'Università Cattolica ha sviluppato un approccio sistemico per rendere il Personale Tecnico Amministrativo (PTA) protagonista nella gestione dei rischi di sicurezza informatica, passando da un approccio in cui i PTA subivano passivamente le misure di sicurezza, ad un approccio in cui i PTA (un vero e proprio Human Firewall) sono diventati un attore primario nel difendere i servizi e la sicurezza informatica dei colleghi, dei docenti e degli studenti. Come parte dell'approccio, la **gamification** ha avuto un ruolo importante in quanto stimola in maniera molto efficace sia l'aspetto pratico che l'aspetto didattico.

Il progetto è iniziato con la creazione di una comunità di "Ambasciatori della Sicurezza" (oggi circa il 13% dei PTA), un gruppo di volontari formati e certificati per estendere la portata del team di sicurezza.

Per raggiungere una popolazione più ampia, è stata inoltre attivata una piattaforma di cyber security awareness che offre un percorso formativo triennale per migliorare la consapevolezza e la conoscenza dei fondamenti della cyber security ed ha permesso, tramite campagne di ethical phishing, di individuare criticità specifiche in alcuni cluster di utenti.

Eventi esperienziali come simulazioni di cyber-incident, workshop non convenzionali, escape room fisiche e virtuali hanno aumentato l'engagement e la partecipazione alla formazione, dimostrando l'efficacia del coinvolgimento emotivo nel migliorare la postura di sicurezza.

In sintesi, l'approccio che abbiamo chiamato "**Aw.A.K.E.**" si basa su quattro pilastri: Awareness, Ability, Knowledge and Emotional Engagement. Il progetto prevede, con la collaborazione dei PTA e in particolare degli ambasciatori, di estendere progressivamente le iniziative a studenti e ricercatori, potenziare la comunicazione e focalizzarsi su gruppi critici. Importante sottolineare che sia le piattaforme che le metodologie sono riutilizzabili, adattabili e diffondibili a tutta la comunità universitaria.

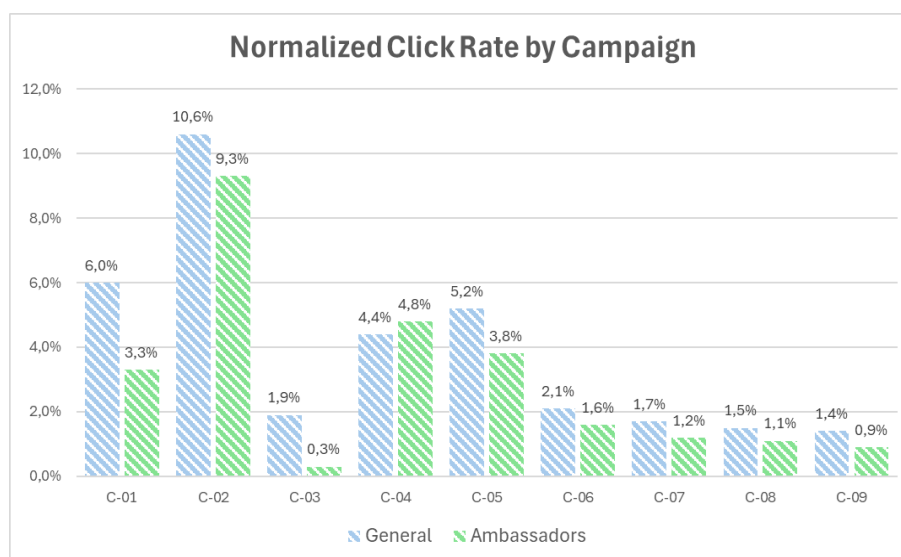
Relazione del progetto (max 8000 caratteri spazi inclusi)

Il concetto di **Human Firewall (HF)** è usato per descrivere le persone che seguono le migliori pratiche per prevenire o segnalare violazioni di dati e attività sospette. Il suo valore è evidente: alcuni studi riportano che l'elemento umano è coinvolto in una percentuale che varia dal 74% al 95% di tutte le violazioni di cyber-sicurezza.

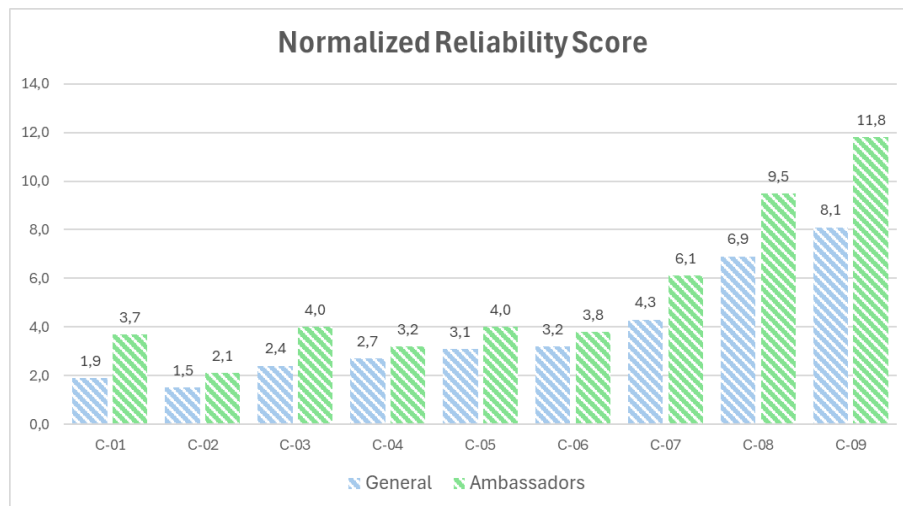
Human Firewall problem è un termine che rappresenta l'insieme di problemi e sfide che comporta creare uno **HF**. Per considerarsi affidabile, uno **HF** deve avere una efficacia elevata, una capacità di riconoscere le minacce e di reagire di conseguenza molto superiore alla media. L'idea di partenza è stata quella di rendere il Personale Tecnico Amministrativo (PTA) protagonista nella gestione dei rischi di sicurezza informatica, passando da un approccio in cui i PTA subivano passivamente le misure di sicurezza, ad un approccio in cui i PTA (un vero e proprio Human Firewall) sono diventati un attore primario nel difendere i servizi e la sicurezza informatica dei colleghi, dei docenti e degli studenti.

Ecco le azioni intraprese per abilitare la nostra vision:

- la creazione, nel 2022, della comunità degli **"Ambasciatori della Sicurezza" (AdS)**, formando e certificando circa il 13% dei PTA, distribuito in tutti i livelli organizzativi e in tutti i campus; l'efficacia è dimostrata dalle statistiche sul phishing etico, dove performano meglio degli altri cluster di utenti e aiutano gli altri utenti ad orientarsi.



- un **approccio più "industrializzato"** e sostenibile alla formazione sulla sicurezza informatica per raggiungere una popolazione più ampia, attivando nel 2023 una piattaforma di CyberSecurity Awareness che fornisce diverse funzionalità tra le quali:
 - un percorso formativo triennale per migliorare la consapevolezza e la conoscenza dei fondamenti della cyber security.
 - campagne mensili di phishing etico adattivo, che utilizzano fino a dieci template simultanei, i risultati mostrando una crescita costante del **Normalized Reliability Score** (punteggio di affidabilità).



- un meccanismo di gamification per team che incoraggia la competizione per migliorare il proprio ranking e quello del team di appartenenza.
 - una web series con un approccio docu-film con storytelling avvincente, che aumenta l'impatto emotivo; ogni episodio esplora una situazione realistica e spiega come evitare o mitigare il rischio.
 - una dashboard completa che fornisce un monitoraggio delle prestazioni e dettagli sul coinvolgimento degli utenti.
- L'utilizzo di campagne di phishing, che ci hanno permesso di identificare con precisione dove intervenire con **azioni formative mirate** per rimediare alle lacune di alcuni cluster.
 - L'utilizzo di **strategie di comunicazione passiva** mediante l'uso di infografiche sulla sicurezza informatica (come tovagliette nelle mense e poster negli spazi comuni), che hanno permesso di migliorare la consapevolezza degli utenti sulle **"Misure minime di sicurezza"**.
 - **Il coinvolgimento emotivo:** nel corso del 2023 abbiamo effettuato una simulazione di incidente di sicurezza e disaster recovery che ha coinvolto il management; successivamente abbiamo organizzato un workshop non convenzionale dall'evocativo titolo "Il colpo di stato del CISO", per favorire l'adozione della piattaforma di CyberSecurity Awareness. Nell'ottobre 2024 abbiamo sperimentato una Cyber Escape Room fisica, sul tema della sicurezza informatica, con risultati promettenti: oltre il 94% dei partecipanti ha dichiarato che l'esperienza aveva contenuti formativi molto interessanti e altamente coinvolgenti. Dal maggio 2025 è operativa ed in evoluzione una Cyber Escape room in realtà virtuale (CybEE), il cui teaser è disponibile su YouTube: <https://www.youtube.com/watch?v=T4ZvI4dhLN8>.



Lo sforzo finora descritto è radicato nel Piano Strategico 2023-2025 dell'UCSC, che ha garantito le risorse, l'impegno del top management e il quadro di governance, fondamentali per il raggiungimento degli obiettivi.

Abbiamo quindi lavorato su 4 pilastri:

- **Consapevolezza (Awareness):** il primo obiettivo che ci siamo posti è stato quello di creare consapevolezza nei nostri colleghi PTA e nella nostra organizzazione sull'importanza della sicurezza informatica. Questo è in un certo senso un leit motiv in tutto ciò che abbiamo fatto.
- **Abilità (Ability):** il secondo obiettivo era quello di dotare i nostri colleghi di un set minimo di abilità, come ad esempio come gestire un'e-mail di phishing o con una procedura di risposta agli incidenti. Le abilità sono più complesse delle competenze e si riferiscono alla "capacità dimostrabile di applicare diverse conoscenze e abilità". Il nostro obiettivo, prima ancora di sviluppare competenze o conoscenze specifiche, era quello di insegnare alle persone come agire e reagire alle minacce.
- **Conoscenza (Knowledge):** la conoscenza è ovviamente importante, ma, contro-intuitivamente, non siamo partiti dalla formazione tradizionale. Abbiamo concentrato i nostri sforzi su questo pilastro dopo aver raggiunto un livello minimo di consapevolezza e capacità. Una maggiore conoscenza si raggiunge più facilmente non appena la consapevolezza dell'importanza e dei rischi e le abilità di base vengono assimilate dalla comunità.
- **Coinvolgimento emotivo:** il potere del coinvolgimento emotivo ci è stato evidente dopo l'evento "Il colpo di stato del CISO". Consapevoli della sua importanza, sono state sviluppate due nuove esperienze: una escape room fisica realizzata nell'ottobre 2024 (Mese europeo della sicurezza informatica) e una escape room in realtà virtuale, attualmente in corso.

Abbiamo chiamato questo approccio "**Aw.A.K.E.**" dall'inglese **A**wareness, **A**bilities, **K**nowledge and **E**motional Engagement.

Abbiamo ancora davanti a noi alcuni compiti:

- Stiamo coinvolgendo un primo gruppo di docenti e ricercatori, e probabilmente avremo bisogno di mettere a punto l'approccio e gli strumenti che utilizziamo. I PTA potranno avere un ruolo guida importante anche in questa fase, in spirito di collaborazione tra componente accademica e amministrativa. Stiamo progettando percorsi simili per gli studenti
- La Cyber Escape Room virtuale (CybEE) è in fase di evoluzione per permettere a più giocatori di partecipare simultaneamente e per introdurre l'Intelligenza Artificiale nelle dinamiche di gioco, rendendo il tutto ancora più realistico e coinvolgente.
- Il team di sicurezza dell'UCSC ha collaborato con la Fondazione EDUCatt e l'Ospedale Gemelli (enti associati UCSC) per le strategie di comunicazione passiva e, in stretta connessione con il gruppo di Digital Transformation di CODAU, con il MUR e con ACN, per il brainstorming e il miglioramento delle tecniche di consapevolezza.

Come descritto, la nostra idea di difesa informatica si basa su una prima linea di resistenza: le persone e in particolare i PTA. Questo non significa che non crediamo negli strumenti, nelle politiche, nelle procedure, negli standard e nell'infrastruttura tecnica. Siamo consapevoli che tutti questi mezzi sono fondamentali, ma crediamo che senza il coinvolgimento delle persone anche il castello più forte possa facilmente cadere: *“Non c'è bisogno di migliaia di uomini per conquistarlo, basta un addetto ai lavori che apre i cancelli”*.

Il panorama delle minacce è in continua evoluzione, come dimostrato chiaramente dai nuovi attacchi informatici basati sull'intelligenza artificiale. La postura di sicurezza di qualsiasi organizzazione deve essere costantemente rivalutata e migliorata per stare al passo con la velocità del cambiamento.

Importante sottolineare infine che sia le piattaforme che le metodologie sono riutilizzabili, adattabili e diffondibili a tutta la comunità universitaria. In particolare, la piattaforma di realtà virtuale e gamification CybEE potrebbe essere utilizzata anche in altri atenei per migliorare la consapevolezza e il coinvolgimento emotivo dei PTA.

Piano del costo degli interventi

L'intervento ha previsto le seguenti voci di spesa:

- Formazione e certificazione degli ambasciatori della sicurezza
- Noleggio della piattaforma di cybersecurity awareness
- Sviluppo e gestione della escape room fisica
- Sviluppo e gestione della escape room in realtà virtuale

Costo totale degli interventi: circa 90.000€ IVA inclusa.