Progetto PNRR M1C1 I 1.5 – Cybersecurity -
”Assessment e potenziamento della resilienza cyber di ARPAC”

Valutazione del livello di consapevolezza del personale tramite campagne di phishing simulato

Sommario

1 Corso di Formazione sulla Sicurezza Informatica Cyber Guru

Arpa Campania ha adottato un percorso strutturato di formazione in ambito Cyber Security Phishing, avvalendosi della piattaforma **Cyber Guru**. L'iniziativa è finalizzata a rafforzare il presidio del fattore umano all'interno dell'organizzazione, trasformandolo da elemento vulnerabile a prima linea difensiva contro le minacce cyber, in linea con quanto richiesto dai principali framework di sicurezza.

In questo documento verranno pubblicati i risultati ottenuti dalle varie campagne simulate volte ad attuare il Programma di Cybersecurity Awareness, con l'intento di analizzare i benefici in tema di consapevolezza sulla sicurezza informatica.

L'attività è stata svolta con il supporto tecnico specialistico del Fornitore Esterno – Pentaqo Srl - nell'ambito del Progetto PNNR M1C1 | 1.5 "Cybersecurity".

2 Sviluppo del programma formativo

L'Organizzazione ha intrapreso un programma continuativo di formazione in Cyber Security tramite l'utilizzo di uno dei due moduli principali della piattaforma Cyber Guru

Cyber Guru Phishing (CGP), programma esperienziale di simulazione di attacchi phishing, dotato di un motore di Machine Learning che adatta le simulazioni al livello di preparazione dei singoli utenti, che include:

- Simulazioni di attacchi via e-mail;
- Reportistica avanzata e strumenti di analisi per la governance e il monitoraggio dei comportamenti.

3 Conformità Normativa e Certificazioni

La piattaforma Cyber Guru è conforme ai più elevati standard di settore ed è certificata per:

- **ISO 9001:2015** settore EA 37 – Progettazione ed erogazione di corsi in ambito Cyber Security;
- **ISO/IEC 27001**, **ISO/IEC 27017**, **ISO/IEC 27018** – Sicurezza delle informazioni e protezione dei dati in ambienti cloud;
- Registrazione presso **ACN** come fornitore qualificato di servizi cloud per la Pubblica Amministrazione.

4 Obiettivi e Risultati Attesi

L'adozione della piattaforma Cyber Guru da parte di Arpa Campania risponde ai seguenti obiettivi:

- Promuovere una cultura della sicurezza informatica a tutti i livelli organizzativi;
- Mitigare il rischio legato all'errore umano.

In coerenza con tali finalità, le campagne di phishing simulato sono state progettate come uno strumento operativo di **sensibilizzazione continua**, finalizzato a valutare nel tempo il livello di consapevolezza del personale rispetto alle principali minacce di tipo cyber, nonché a stimolare comportamenti corretti nell'utilizzo degli strumenti digitali e nella gestione delle comunicazioni elettroniche.

I risultati attesi dall'esecuzione delle campagne riguardano, in particolare, la progressiva riduzione dell'esposizione al rischio di attacchi di social engineering, il miglioramento della capacità di riconoscere messaggi fraudolenti e l'incremento dell'attenzione verso i segnali di allerta tipici delle comunicazioni malevole.

Parallelamente, l'iniziativa consente di misurare in modo oggettivo l'efficacia delle attività formative e di **Awareness**, individuando eventuali aree di miglioramento su cui concentrare ulteriori azioni correttive.

L'analisi aggregata delle dieci campagne consente inoltre di osservare l'evoluzione dei comportamenti degli utenti nel tempo, fornendo un quadro complessivo dello stato di maturità dell'organizzazione in materia di cybersecurity e contribuendo a supportare le decisioni strategiche in ambito di prevenzione e gestione del rischio informatico.

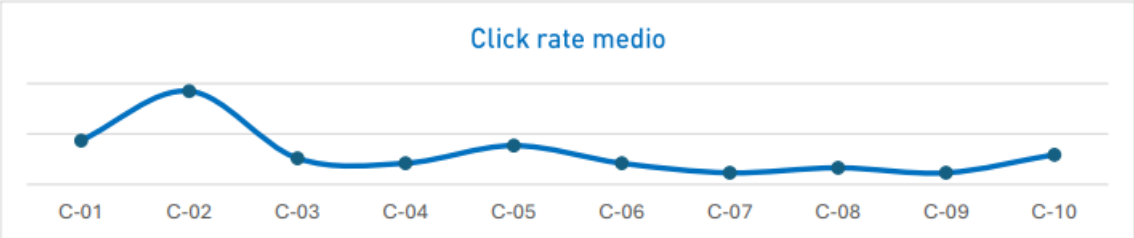
4.1 Statistiche alla data 13/01/2026

Campagna	Overview	Distribuzione del rischio per dispositivo	Distribuzione del rischio per browser	Distribuzione del rischio per sistema operativo
C-01	- 574 attacchi inviati - 50 click effettuati - 8.7% click rate medio	- 50% mobile - 50% desktop	- 28% Edge - 26% Chrome - 26% Firefox - 11% Mobile Safari - 7% Samsung Internet - 2% MIUI Browser	- 46% Windows - 39% Android - 15% iOS
C-02	- 574 attacchi inviati - 106 click effettuati - 18.5% click rate medio	- 53% desktop - 47% mobile	- 30% Chrome - 26% Firefox - 25% Edge - 8% Mobile Safari - 8% Samsung Internet - 3% Altro	- 49% Windows - 36% Android - 12% iOS - 3% Altro
C-03	- 574 attacchi inviati - 30 click effettuati - 5.2% click rate medio	- 60% mobile - 40% desktop	- 38% Chrome - 31% Edge - 19% Firefox - 8% Mobile Safari - 4% Samsung Internet	- 54% Android - 31% Windows - 15% iOS
C-04	- 574 attacchi inviati - 24 click effettuati - 4.2% click rate medio	- 58% mobile - 42% desktop	- 33% Edge - 29% Chrome - 21% Firefox - 13% Samsung Internet - 4% Mobile Safari	- 54% Android - 38% Windows - 4% iOS - 4% Mac OS
C-05	- 574 attacchi inviati - 44 click effettuati - 7.7% click rate medio	- 80% mobile - 20% desktop	- 39% Chrome - 23% Edge - 14% Mobile Safari - 12% Firefox - 12% Samsung Internet	- 53% Android - 28% iOS - 19% Windows
C-06	- 574 attacchi inviati - 24 click effettuati - 4.2% click rate medio	- 75% mobile - 25% desktop	- 42% Chrome - 33% Edge - 17% Firefox - 4% Samsung Internet - 4% Mobile Safari	- 62% Android - 25% Windows - 13% iOS
C-07	- 574 attacchi inviati - 13 click effettuati - 2.3% click rate medio	- 62% mobile - 38% desktop	- 46% Chrome - 15% Edge - 15% Firefox - 8% WebKit - 8% Mobile Safari - 8% Samsung Internet	- 59% Android - 33% Windows - 8% iOS

C-08	- 574 attacchi inviati - 19 click effettuati - 3.3% click rate medio	- 53% mobile - 47% desktop	- 58% Edge - 11% Chrome - 11% Firefox - 5% Mobile Safari - 5% IE - 5% Samsung Internet - 5% Opera	- 47% Windows - 32% Android - 21% iOS
C-09	- 574 attacchi inviati - 13 click effettuati - 2.3% click rate medio	- 69% desktop - 31% mobile	- 39% Firefox - 38% Edge - 15% Chrome - 8% Samsung Internet	- 69% Windows - 23% Android - 8% iOS
C-10	- 574 attacchi inviati - 34 click effettuati - 5.9% click rate medio	- 62% mobile - 38% desktop	- 50% Chrome - 23% Edge - 21% Firefox - 3% Samsung Internet - 3% Mobile Safari	- 56% Android - 38% Windows - 6% iOS

Di seguito una overview sulla totalità delle **10 campagne** concluse:

- **5740** attacchi inviati;
- **357** click effettuati;
- **6.2%** click rate medio.



5 Conclusioni

I risultati complessivi delle campagne di phishing simulato evidenziano un **miglioramento significativo** e misurabile del livello di consapevolezza dell'utenza rispetto alle minacce di tipo cyber.

In particolare, il passaggio da un click rate medio iniziale pari al **18,5%** ad un valore finale del **5,9%** evidenzia una **riduzione del click rate pari al 12,6%,** con una media complessiva attestata intorno al **6,2%**, testimonia una riduzione sostanziale della propensione all'errore umano ed una maggiore capacità di **riconoscere tentativi di phishing**.

Tale andamento conferma l'efficacia delle attività di sensibilizzazione e formazione continua, dimostrando come un approccio strutturato e reiterato nel tempo consenta di incidere positivamente sui comportamenti degli utenti, a tutto vantaggio della dell'Ente in materia di sicurezza Cyber.

Il miglioramento registrato rappresenta un indicatore concreto dell'accresciuta maturità dell'Organizzazione in ambito di Cybersecurity e costituisce una base solida su cui proseguire e rafforzare ulteriormente le iniziative di Awareness, in un'ottica di miglioramento continuo e di riduzione del rischio complessivo per l'Agenzia.

Il Referente per la Cybersicurezza
dott. Massimo **Di Guida**

Il Responsabile Progetto PNRR
dott.ssa Loredana **La Via**