MUR
Ministero dell'Università e della Ricerca

Ministero dell'Università e della Ricerca

Report risultati Campagna di Phishing C-5

Conservatorio di Musica statale Giuseppe Verdi - Milano

Agenda

01 Contesto e Approccio Metodologico

02 Risultati dell’Istituto

03 Conclusioni e Prossimi passi

04 Appendice

01
Contesto e Approccio Metodologico

Contesto di riferimento

Premesse e obiettivi

Al fine di **innalzare il livello di sicurezza informatica degli Atenei e delle istituzioni dell'Alta Formazione Artistica e Musicale** (di seguito **«AFAM»**) e di rafforzare la consapevolezza degli utenti rispetto ai rischi cyber, il Ministero dell'Università e della Ricerca, ha avviato un percorso formativo finalizzato a **promuovere una cultura della sicurezza digitale** condivisa ed a rispondere alle crescenti minacce in materia di cybersecurity. Nell'ambito delle **attività di prevenzione** previste dal progetto, è stata programmata l'attivazione di **sei campagne di simulazione di phishing nel biennio 2025-2026**, rivolte al personale tecnico-amministrativo degli Atenei e delle istituzioni AFAM, con i **seguenti obiettivi:**

AWARENESS

Attività volta ad **aumentare la consapevolezza degli utenti coinvolti** rispetto ai rischi legati alle attività di Phishing.

VALUTAZIONE RISCHI

Misurare il **rischio associato a questa tipologia di minaccia**, evidenziando le possibili conseguenze di un eventuale attacco.

IDENTIFICAZIONE MINACCE

Incrementare la **capacità di individuare gli attacchi basati sul Phishing**, limitando al minimo i possibili danni che potrebbero causare.

A seguito della **conclusione** della **quinta campagna di Phishing**, nelle prossime slide verranno presentati i **risultati emersi** dall'attività condotta. L'obiettivo è fornire una **visione chiara** e **strutturata** dell'efficacia dell'iniziativa e delle lezioni apprese, così da orientare al meglio le future azioni di **sensibilizzazione** e **formazione**.

Contesto di riferimento

Approccio Metodologico

La **campagna di Phishing,** rientrante nell'ambito delle attività di **Prevenzione,** destinata al **personale tecnico-amministrativo degli Atenei e delle AFAM**, è stata erogata tramite la collaborazione diretta dei **Referenti IT** di ogni Istituto in perimetro, che si sono occupati della configurazione ed invio (direttamente tramite una casella di posta interna all'Istituto o tramite l'utilizzo della soluzione **Attack Phishing Simulation** di **Microsoft Defender**) del **principale vettore d'attacco**: la **fake e-mail.**

Di seguito, vengono riportate le diverse **fasi** che sono state seguite per svolgere la Campagna di Phishing:

01. Selezione Perimetro

Definizione degli obiettivi strategici dell'attività di Phishing con l'identificazione degli Atenei e AFAM coinvolti. Analisi del **pubblico di destinazione** per adattare il linguaggio e il contenuto delle e-mail simulate. Sono inoltre stati individuati gli **indicatori di successo**, come il numero di accessi alla pagina, per misurare l'efficacia dell'iniziativa.

02. Disegno

Preparazione degli **elementi grafici** (codice UTF o HTML dell'e-mail) e **tecnici** (creazione di una **pagina web con sistema di tracciamento**) da condividere con i Referenti IT di Atenei e AFAM, che si sono occupati dell'invio interno oppure il supporto alla **configurazione** della campagna tramite **Microsoft Defender**.

03. Svolgimento

Avvio delle campagne di Phishing con **l'invio delle e-mail da parte dei Referenti di Atenei e AFAM**, secondo le modalità scelte o stabilite. In questa fase è stato effettuato un test a campione per verificare il corretto **raggiungimento della pagina web**, monitorando lato *back-end* l'effettivo tracciamento degli accessi da parte degli utenti target.

04. Tracciamento

Controllo, monitoraggio e raccolta in tempo reale degli accessi alle pagine web da parte degli utenti appartenenti ad **Atenei** e **AFAM**. Al termine della campagna, sono stati **analizzati il numero di accessi** e le e-mail effettivamente inviate, utili per attività di **reporting** sui risultati ottenuti al termine della campagna simulata.

Architettura della campagna

Modalità di invio delle e-mail

Considerata l'**eterogeneità organizzativa e tecnologica degli Atenei e delle istituzioni AFAM** coinvolte, è stato necessario adottare un approccio flessibile e differenziato per la realizzazione e l'invio delle e-mail di phishing simulato. Le modalità operative sono state definite in base alle caratteristiche tecniche di ciascun Ente, scegliendo una delle seguenti **soluzioni**.

UTF Model E-mail

Prevede la condivisione di un **file in formato UTF-8** che descrive il contenuto e la struttura dell'e-mail di phishing simulato. Gli Enti hanno potuto utilizzare questo modello come base per **inviare** le comunicazioni tramite i propri **strumenti di posta elettronica** che accettano tale formato.

È stato predisposto e condiviso un **link univoco** che è stato inserito all'interno dell'e-mail simulata. Questo link ha reindirizzato a una **pagina di atterraggio dedicata**, progettata per **tracciare i click ricevuti**. Ogni Ente ha disposto di un link personalizzato, così da permettere la registrazione separata e anonima delle interazioni.

HTML E-mail

Prevede la condivisione del **codice HTML** completo dell'e-mail, pronto per essere integrato nei sistemi di invio dell'Ente. Tale alternativa è stata pensata per le realtà che gestiscono direttamente l'invio delle e-mail tramite **strumenti tecnologici** (interni o esterni) per l'invio massivo di comunicazioni.

Microsoft Defender

Prevede l'uso della **piattaforma integrata in Microsoft 365** per la simulazione di attacchi. Gli Enti dotati di questa soluzione hanno potuto configurare la campagna in modo **guidato**, beneficiando di strumenti di creazione, avvio e tracciamento offerti da **Microsoft Defender**.

È stata condivisa una **guida** per **configurare** la campagna tramite Microsoft Defender, comprensiva dell'**HTML** dell'email e della pagina.

Altro

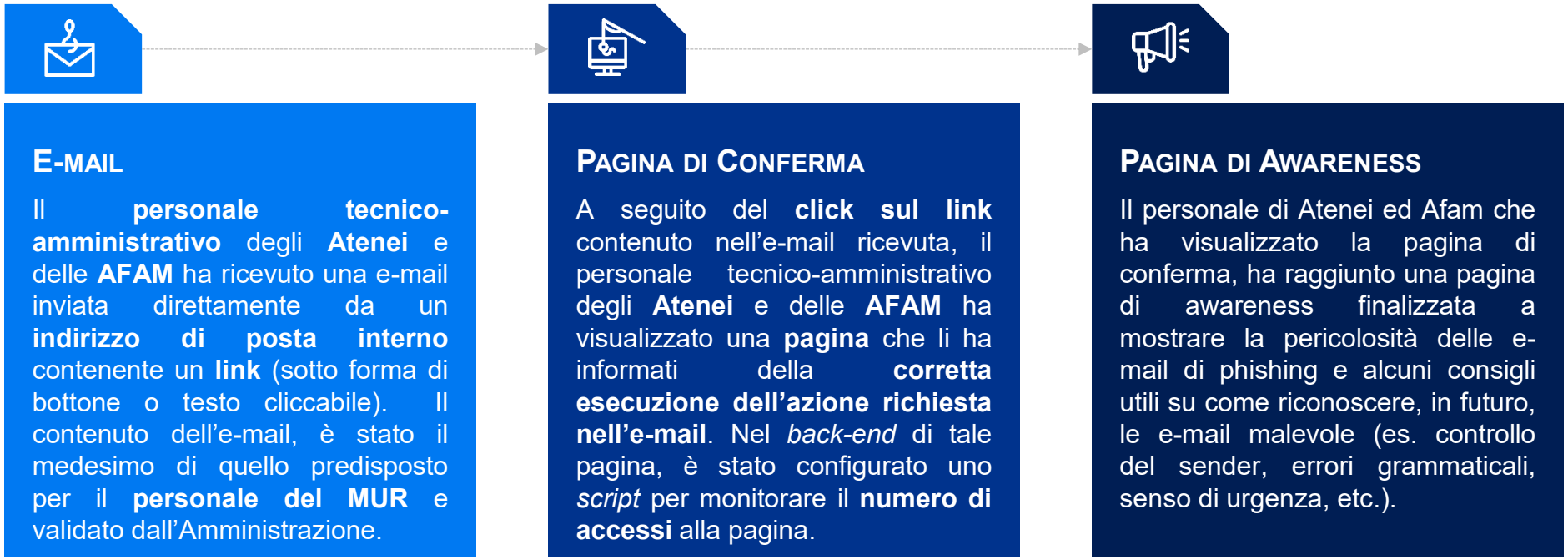
Prevede l'utilizzo di **architetture alternative** rispetto a quelle precedentemente descritte quali CyberGuru, soluzioni interne, etc.

La scelta è dipesa da **motivazioni tecniche** specifiche o di personale impiegato per meglio efficientare **l'organizzazione** della **campagna**.

Architettura della campagna

Fasi operative

Con il fine di aumentare la consapevolezza del **personale tecnico-amministrativo** degli **Atenei** e delle **AFAM** e per promuovere il **riconoscimento** delle e-mail malevole, la campagna proposta ha previsto, a seguito dell'interazione con l'e-mail mediante il ***click* sul link**, il raggiungimento di una **pagina di conferma della corretta esecuzione dell'azione** e successivamente la visualizzazione di una **pagina di *awareness*** dove gli utenti *target* hanno ricevuto una breve **formazione** sui pericoli delle e-mail di Phishing e come riconoscerle. Nello specifico, di seguito vengono presentate e descritte le **diverse fasi** del **modello di campagna di Phishing** adottato:



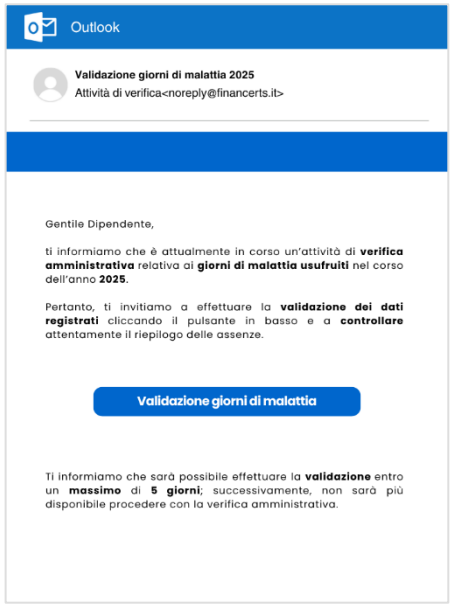
Nota: per l'organizzazione ed esecuzione delle campagne di phishing al personale tecnico-amministrativo degli Atenei e delle AFAM **non è stato previsto** alcun trattamento di dati personali, in quanto i dati sono stati oggetto di **anonimizzazione** e **non riconducibili** ai singoli utenti *target* delle campagne.

Architettura della campagna

Scenario «Giorni di malattia 2025»

Di seguito, viene riportata l'e-mail utilizzata per la presente simulazione di phishing. Nello specifico, tale e-mail informa gli utenti *target* degli Atenei e delle Afam, dell'avvio di una **verifica amministrativa** sui **giorni** di **malattia** usufruiti nel **2025** entro una determinata **scadenza.** Una volta cliccato sul link, gli utenti che vi avranno interagito visualizzeranno una pagina di **Awareness** dal contenuto formativo.

E-MAIL



CONFERMA

Popup che informa il dipendente che la richiesta è stata presa in carico con successo.

PAGINA DI AWARENESS

02
Risultati dell’Istituto

Sintesi dei risultati

ID 7250 - Conservatorio di Musica statale Giuseppe Verdi - Milano

Popolazione

84

Awareness Level:

5/10

PRINCIPIANTE

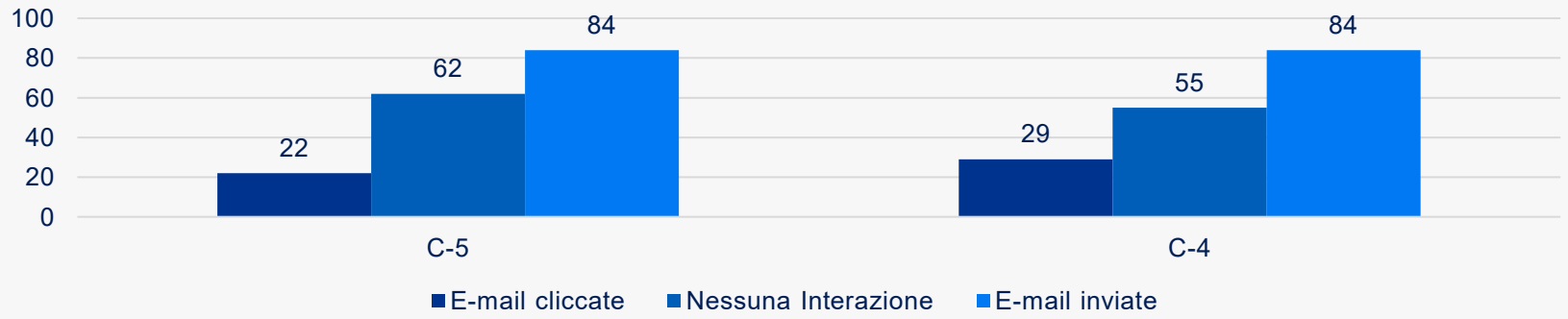
Legenda Awareness Level

- **Principiante** 3-5 punti
- **Intermedio** 6-8 punti
- **Esperto** 9 -10 punti

RISULTATI C-5:

E-MAIL INVIATE	CLICK SUL LINK		NESSUNA INTERAZIONE	
84	22	26%	62	74%

ANDAMENTO DELLE CAMPAGNE



Nota: Si specifica che per «**nessuna interazione**» si intendono sia le e-mail presumibilmente aperte ma senza alcuna azione successiva (click sul link), sia le e-mail non aperte e quindi prive di qualsiasi forma di coinvolgimento.

03
Conclusioni e Prossimi passi

Prossimi Passi
Conclusioni

L'analisi dei risultati ottenuti dalla somministrazione della presente campagna di phishing al personale tecnico-amministrativo degli Atenei e delle istituzioni AFAM ha consentito di **valutare il livello di consapevolezza** nella capacità di riconoscere potenziali e-mail malevole. Con la finalità di accrescere la consapevolezza del personale target, saranno intraprese delle ulteriori iniziative formative qui di seguito dettagliate.

Nome	Altre attività formative
MATERIALE INFO FORMATIVO	Diffusione di materiale **info-formativo** sulle principali tematiche inerenti alla **sicurezza informatica**, L'iniziativa consiste nell'invio ai dipendenti di **Brochure periodiche** nel numero di **6 rilasci nel 2026** Esse affronteranno una varietà di tematiche **analizzate in dettaglio**, contenenti **consigli utili** alla comprensione della Cybersecurity destinati ai dipendenti di Atenei ed AFAM.
CORSI DI FORMAZIONE	**Erogazione** di **corsi di formazione** che tratteranno, con **difficoltà incrementale,** le principali tematiche della sicurezza informatica. Il percorso formativo consiste di due edizioni, da effettuarsi nel corso dell'Anno 2026.

Riflessioni conclusive:

I risultati della campagna di Phishing sottolineano un **livello di consapevolezza** dei dipendenti dell'Istituto **Principiante**, richiedendo ulteriori approfondimenti da ottenersi attraverso il percorso formativo avviato in materia di sicurezza informatica.

A tal riguardo, per valutare in itinere il miglioramento e la risposta dei dipendenti di Atenei e AFAM alla formazione, verrà effettuata **un'ulteriore campagna di phishing nel 2026.**

04
Appendice

Awareness Level (HTML/UTF-Altro) - Guida al Calcolo

TABELLE ASSEGNAZIONE PUNTEGGI:

	Click sul link							
	Esperto	Esperto	Intermedio	Intermedio	Intermedio	Principiante	Principiante	Principiante
Soglia	*x≤1%*	*2%< x≤4%*	*4%<x≤5%*	*5%<x≤10%*	*10%<x≤15%*	*15%<x≤30%*	*30%<x≤35%*	*X>35%*
Punti	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*

Legenda Awareness Level

3-5 punti
Livello Principiante

6-8 punti
Livello Intermedio

10 punti
Livello Esperto


MUR
Ministero dell'Università e della Ricerca