WORKSHOP GARR 2026

NET MAKERS

CyberSapere

Paolo Micozzi

Ministero dell’Università e della Ricerca (MUR)

Vivere nell'era digitale: un’esposizione crescente al rischio cyber

La crescente digitalizzazione rende persone e organizzazioni sempre più esposte ai rischi informatici legati alle interazioni quotidiane.

Le interazioni digitali (login, scambio di dati, utilizzo dei servizi)



possono costituire punti di esposizione al rischio.

I dati di un’esigenza non derogabile

I dati più recenti confermano una crescita significativa della minaccia cyber in Italia, con un impatto rilevante sul settore governativo.

4.911

Incidenti cyber di particolare gravità che hanno coinvolto organizzazioni e cittadini italiani nel **primo semestre del 2026**

+105%

Numero di **incidenti cyber** registrati **in Italia** nel **primo semestre del 2026**, rispetto al semestre precedente

Il settore governativo si conferma il target maggiormente colpito dagli attacchi cyber

Fonte: Rapporto Clusit – Aggiornamento di ottobre 2026

Stato della minaccia cyber in Italia

Settembre 2026

235

Incidenti cyber

Tra le principali minacce rilevate nel mese figurano **attacchi DDoS, compromissione di caselle email e phishing**

1.036

Vittime

Concentrate soprattutto nei settori **Tecnologico, Sanitario e Manifatturiero**

10.839

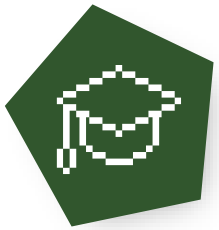
Comunicazioni inviate dal CSIRT Italia

Segnalazioni di **potenziali compromissioni e fattori di rischio** a enti e imprese

Fonte: Operational Summary: Dati ed Indicatori della Minaccia Cyber in Italia – Settembre 2026 (ACN)

Cosa abbiamo realizzato

Nell'ambito del progetto CyberSapere, sono state svolte diverse attività.



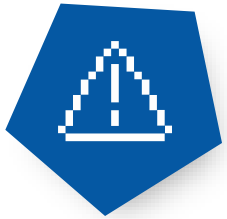
Formazione:

Percorso di acquisizione e consolidamento di **competenze** basato sulla logica del **micro-learning**. L'attività ha previsto la **diffusione di materiale info-formativo** per agevolare e rafforzare l'apprendimento.



Prevenzione:

Esercitazioni pratiche di attacchi di **phishing** finalizzate alla valutazione e al miglioramento della **capacità** del personale di individuare e comprendere le **minacce informatiche** veicolate per mezzo di e-mail, limitando in questo modo i possibili danni.



Supporto al MUR:

Selezione, configurazione e gestione di una **piattaforma** tecnologica necessaria al **monitoraggio** costante dei **rischi informatici**.

Linea di intervento Formazione

La linea di intervento della formazione mira a incrementare le competenze nell'ambito della sicurezza cyber attraverso iniziative dedicate.

- **Cyber Skill Assessment** utile ad individuare il fabbisogno formativo degli utenti target
- **Brochure periodiche** in moduli di micro-learning, per personale MUR e per Atenei e AFAM
- **Eventi info-formativi sul territorio** per studenti, personale tecnico-amministrativo e Referenti NIS 2
- **Corsi di formazione online** annui per personale MUR e di Atenei e AFAM
- **Piattaforma e-learning** contenente corsi di livello incrementale per il personale del MUR

Nelle successive slide vengono presentati i dati emersi dalle iniziative di formazione

Risultati Cyber Skill Assessment

13/25 Punteggio medio - MUR

14/25 Punteggio medio - Atenei

14/25 Punteggio medio - AFAM

Awareness Level complessivo:
Intermedio



Di seguito sono riportate le tre aree di miglioramento, per le quali il **tasso di risposta esatta è stato inferiore al 50%,** con riferimento ai risultati emersi ed ai rispettivi ambiti e domini del questionario:

Security controls:
misure tecniche e organizzative volte a proteggere sistemi e dati, verificando l'efficacia dei principali meccanismi di difesa informatica.

Minacce informatiche e tecniche di attacco

Internet Security:
best practice idonee a prevenire attacchi informatici perpetrati tramite un utilizzo poco sicuro di Internet e delle reti Wi-Fi.

Utilizzo sicuro della rete WiFi

Corso di cybersecurity: dai fondamenti alle tecniche avanzate di sicurezza - 2025

DURATA
32 ore di formazione, erogate in 8 lezioni da 4 ore ciascuna

ATENEI 100

AFAM 148

Numero partecipanti IFS
1.932

Numero partecipanti MUR
38

Numero partecipanti totali
1.970

Piattaforma di fruizione
Microsoft Teams

Numero compilazioni del test finale*
1448

Numero utenti che hanno superato il test finale*
1444

*__Nota__: dati aggiornati in data 10/12/2025

Corso di cybersecurity: dai fondamenti alle tecniche avanzate di sicurezza - 2026

DURATA
28 ore di formazione, erogate in 16 lezioni

ATENEI 74

AFAM 68

Numero partecipanti IFS**

1.537

Numero partecipanti Atenei*

1.102

Numero partecipanti AFAM*

431

Piattaforma di fruizione

Moodle

Data di chiusa del corso per il personale IFS

1 dicembre



Il **corso** sarà **prossimamente erogato** anche al **personale** del **Ministero**

***Nota**: dati aggiornati in data 09/10/2026.
****Nota:** dall'estrazione effettuata è emerso che quattro partecipanti hanno effettuato l'accesso al corso di formazione utilizzando un indirizzo e-mail personale, per cui non è possibile ricondurli ai rispettivi Istituti di appartenenza.

Brochure periodiche

Di seguito si offre una panoramica delle tematiche oggetto delle pubblicazioni realizzate, rivolte agli Atenei, alle Istituzioni AFAM e al personale del Ministero:

2025

1. Phishing
2. Social Network
3. Attento a quel software
4. Proteggi le tue informazioni
5. Ransomware
6. Festeggia in sicurezza

2026

1. L'arte dell'inganno
2. Smishing e Vishing
3. L'uso consapevole della piattaforma online
4. QRishing
5. Utilizzo dei dispositivi mobili
6. Connessioni in sicurezza

Eventi info-formativi

Di seguito si offre una panoramica delle principali informazioni emerse a seguito dell'erogazione delle lezioni formative frontali presso gli Istituti ospitanti:

LEZIONI EROGATE IN TOTALE
18

LEZIONI 2025 3

LEZIONI 2026 15

Numero partecipanti totali*
709

Atenei ospitanti*
14

AFAM ospitanti*
4

Livello di gradimento rilevato*
4,65/5

Prossima lezione presso:

- **Università degli Studi di Genova**

*__Nota__: dati aggiornati in data 29/10/2026

Linea di intervento Prevenzione

La linea di intervento della prevenzione mira a incrementare le competenze nell'ambito della sicurezza cyber attraverso iniziative dedicate.



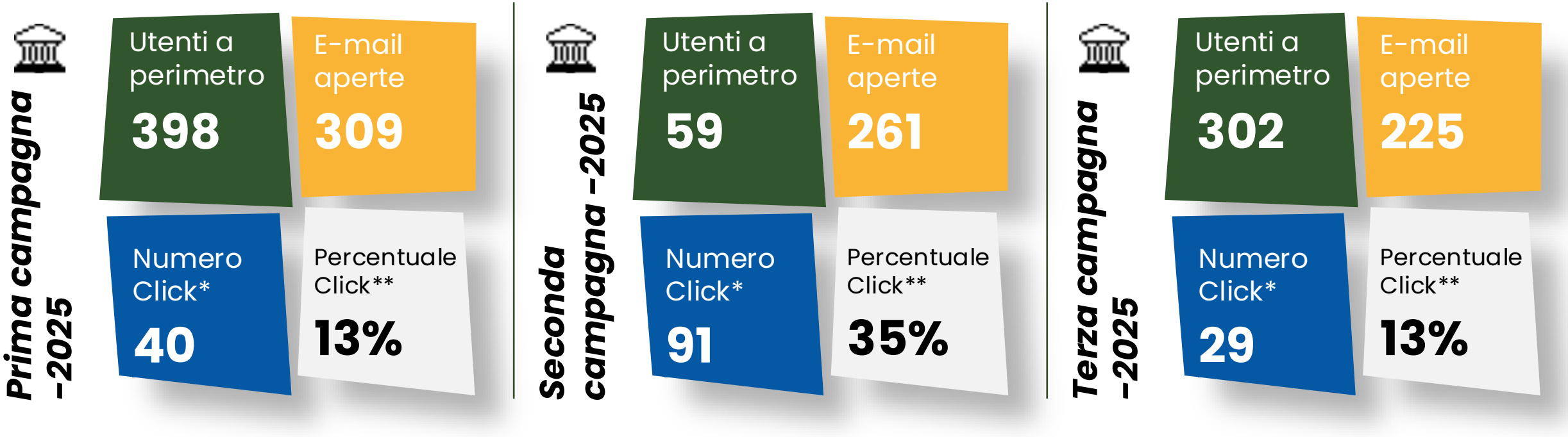
Campagne di Phishing

Attraverso simulazioni pratiche, questa iniziativa mira a sensibilizzare gli utenti e rafforzare le loro competenze nella individuazione di minacce reali veicolate tramite e-mail.

Nelle successive slide vengono presentati i dati emersi dall'iniziativa di prevenzione

Campagne di Phishing 2025 - MUR

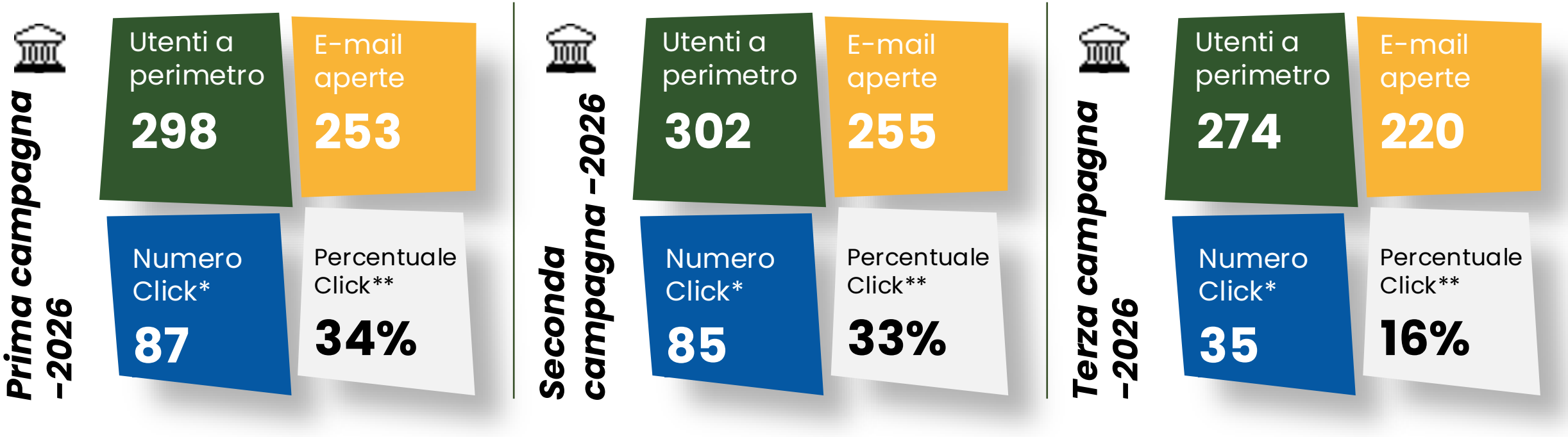
Di seguito si offre una rappresentazione dei risultati maturati dal personale del Ministero dell'Università e della Ricerca (MUR) che ha preso parte alle iniziative di prevenzione svolte nel 2025:



*Nota: numero di utenti che hanno cliccato sul link contenuto nell'email di simulazione
** Nota: percentuale di utenti che hanno cliccato sul link contenuto nell'email rispetto al totale delle email inviate

Campagne di Phishing 2026 - MUR

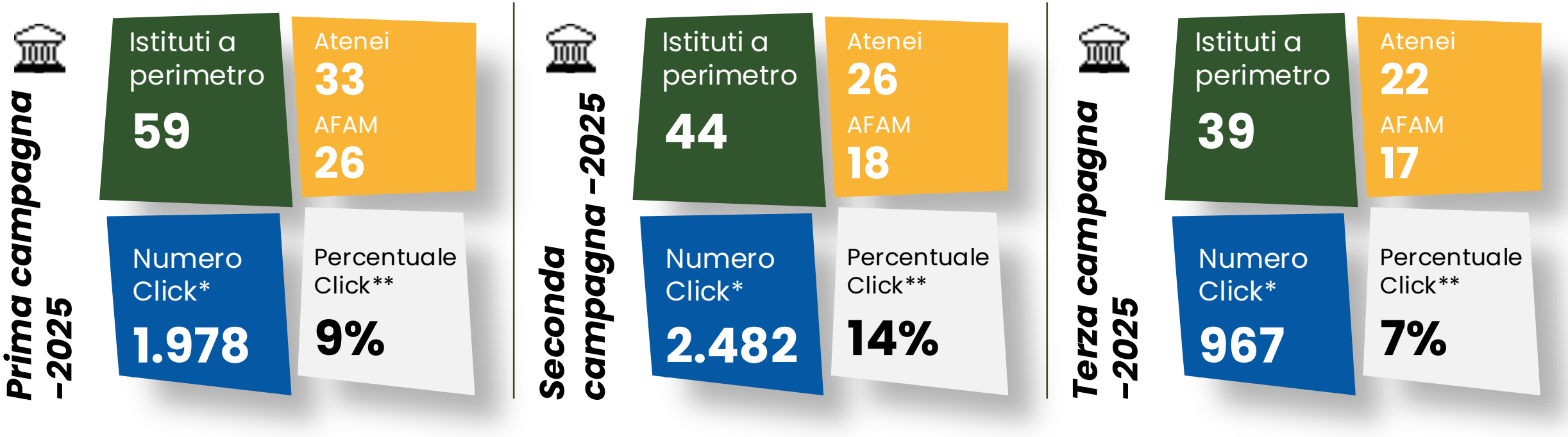
Di seguito si offre una rappresentazione dei risultati maturati dal personale del Ministero dell'Università e della Ricerca (MUR) che ha preso parte alle iniziative di prevenzione svolte nel 2026:



*Nota: numero di utenti che hanno cliccato sul link contenuto nell'email di simulazione
** Nota: percentuale di utenti che hanno cliccato sul link contenuto nell'email rispetto al totale delle email inviate

Campagne di Phishing 2025 - IFS

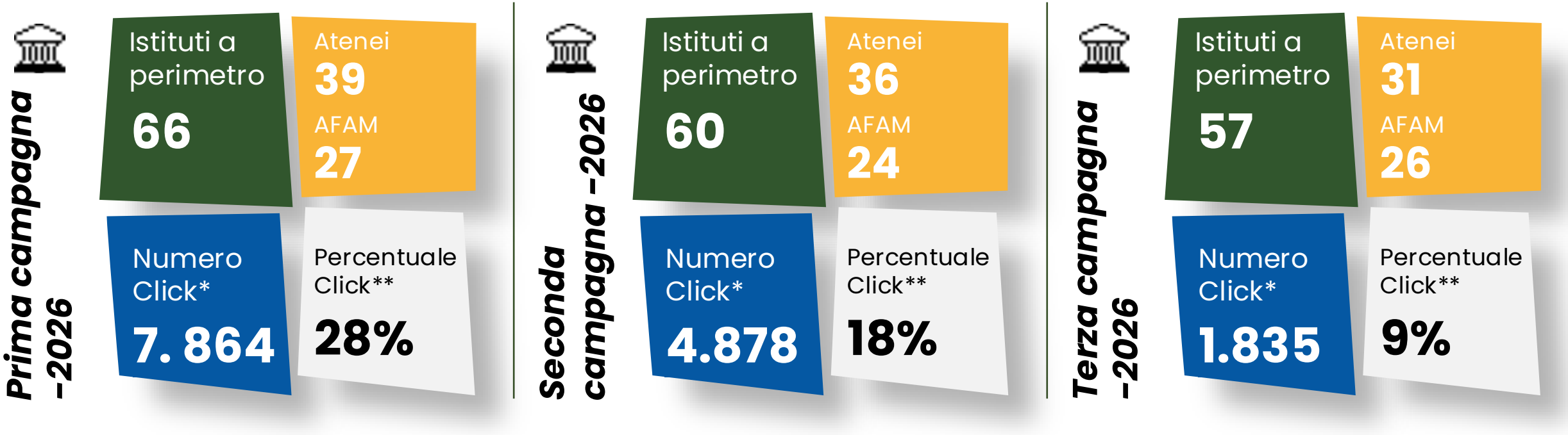
Di seguito si offre una rappresentazione dei risultati maturati dal personale tecnico-amministrativo di Atenei e AFAM che ha preso parte alle iniziative di prevenzione svolte nel 2025:



*Nota: numero di utenti che hanno cliccato sul link contenuto nell'email di simulazione
** Nota: percentuale di utenti che hanno cliccato sul link contenuto nell'email rispetto al totale delle email inviate

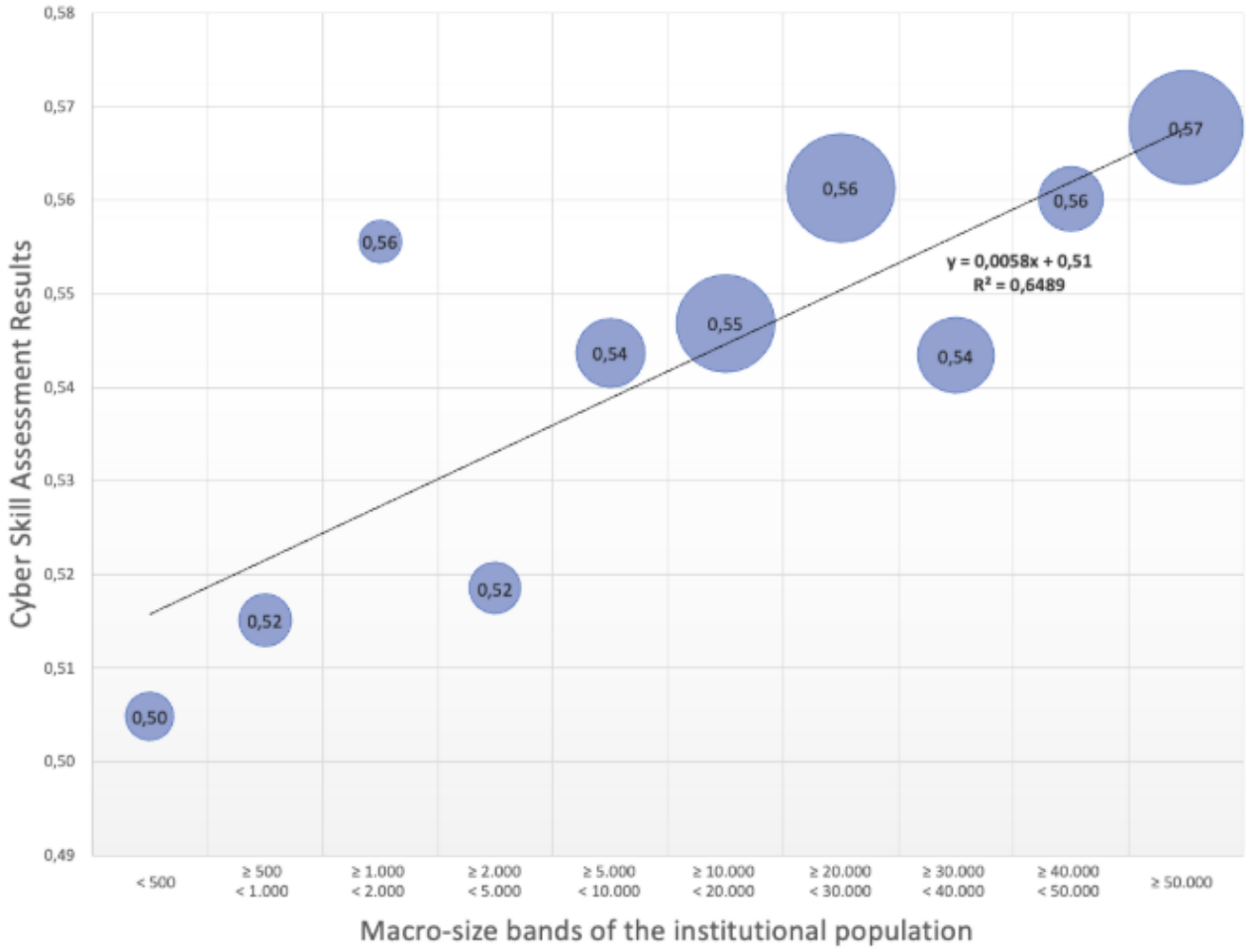
Campagne di Phishing 2026 - IFS

Di seguito si offre una rappresentazione dei risultati maturati dal personale tecnico-amministrativo di Atenei e AFAM che ha preso parte alle iniziative di prevenzione svolte nel 2026:



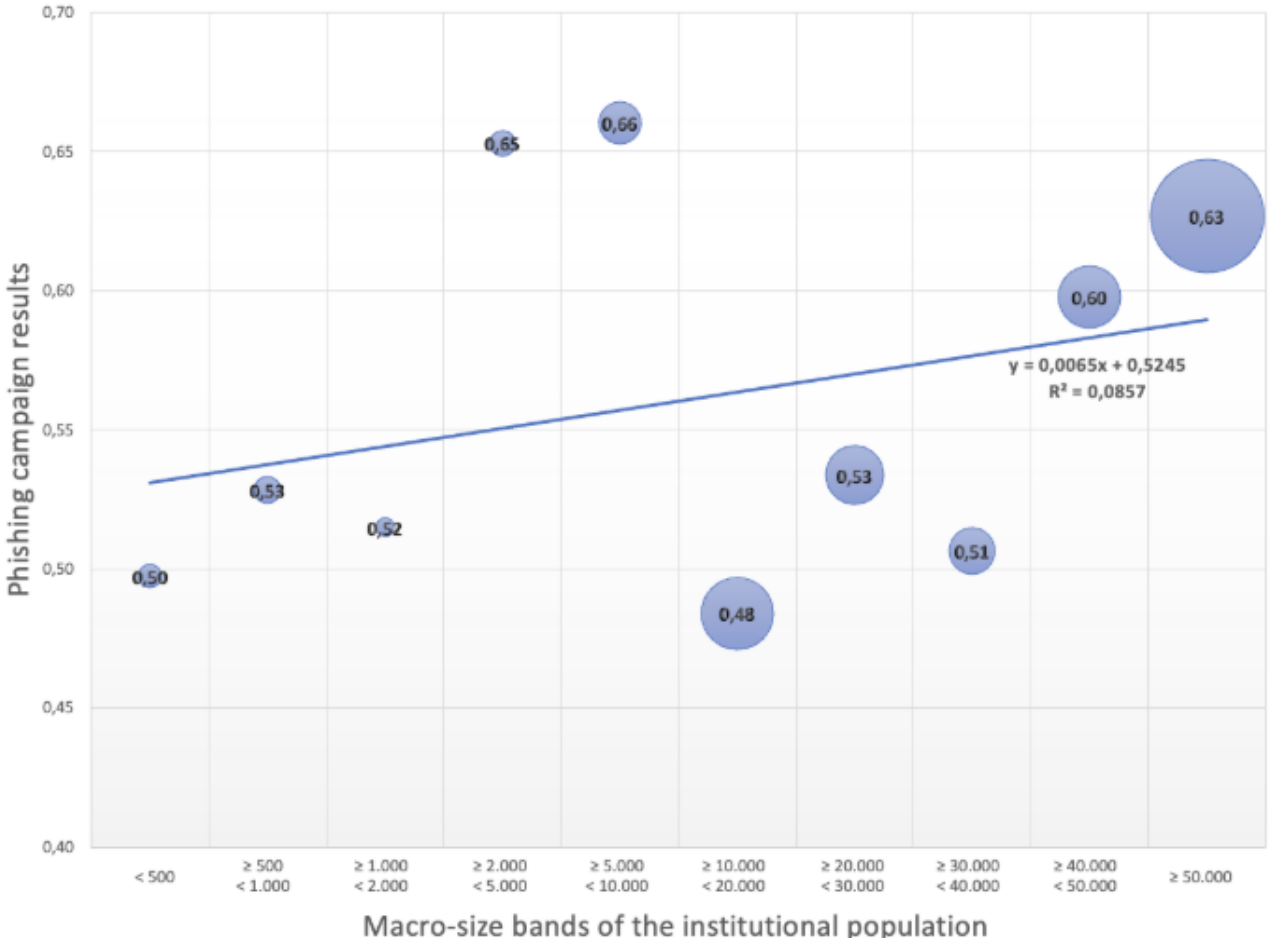
*Nota: numero di utenti che hanno cliccato sul link contenuto nell'email di simulazione
** Nota: percentuale di utenti che hanno cliccato sul link contenuto nell'email rispetto al totale delle email inviate

Analisi del Cyber Skill Assessment



Organizational size range	Number of participating institutions	Population involved	Weighted average of scores[22]
0 ≤ OS < 500	77	501	0,50
500 ≤ OS < 1.000	45	596	0,52
1.000 ≤ OS < 2.000	23	378	0,56
2.000 ≤ OS < 5.000	16	559	0,52
5.000 ≤ OS < 10.000	15	1.021	0,54
10.000 ≤ OS < 20.000	20	2.096	0,55
20.000 ≤ OS < 30.000	14	2.541	0,56
30.000 ≤ OS < 40.000	8	1.242	0,54
40.000 ≤ OS ≤ 50.000	5	895	0,56
OS > 50.000	10	2.846	0,57
TOTALS / AVERAGES	**233**	**12.675**	**0,55**

Analisi delle campagne di phishing



Organizational size range	Number of distinct participating institutions	Population involved	Weighted average of scores
0 ≤ OS < 500	29	1.648	0,50
500 ≤ OS < 1.000	19	2.161	0,53
1.000 ≤ OS < 2.000	8	975	0,52
2.000 ≤ OS < 5.000	7	2.021	0,65
5.000 ≤ OS < 10.000	9	5.558	0,66
10.000 ≤ OS < 20.000	14	16.555	0,48
20.000 ≤ OS < 30.000	9	10.986	0,53
30.000 ≤ OS < 40.000	4	6.880	0,51
40.000 ≤ OS ≤ 50.000	3	12.126	0,60
OS > 50.000	7	41.802	0,63
TOTALS / AVERAGES	**109**	**100.712**	**0,58**

Perché la sicurezza digitale siamo noi.

CyberSapere, il programma promosso dal Ministero dell'Università e della Ricerca (MUR) in collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN).

cyber_sapere@mur.gov.it

WORKSHOP GARR 2026

NET MAKERS