UNICC | Cybersecurity

Cybersecurity Awareness Landscape Report 2024

July 2025

TLP: CLEAR

CONTENTS

Executive Summary

As cyberthreats continue to grow in scale and sophistication, the UNICC Cybersecurity Awareness Landscape Report 2024 provides a data-driven assessment of how user behaviour and targeted training strengthen organizational resilience. This year's report presents observations, best practices, and lessons learned from organizations subscribed to UNICC's common security awareness solutions. The insights draw on collective experience and aim to support the ongoing mission of each UNICC Partner.

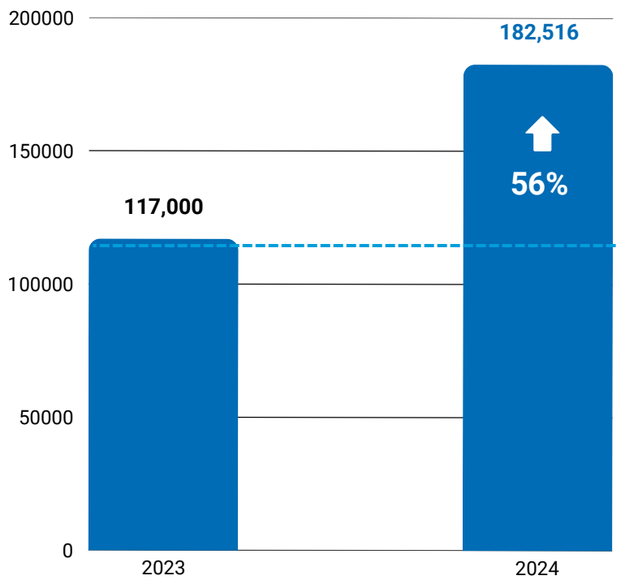
Data from the UNICC Cyber Threat Landscape Report 2024, released in April 2025, indicates that phishing remained the most frequently used initial attack vector, accounting for an estimated 57% of attacks. This underscores the importance of a strong security awareness program within an organization. Equipping users with the sills to identify and respond to phishing attempts is more essential than ever in preventing cyberattacks.

In 2024, UNICC delivered 182,516 phishing test messages-an increase of 56% compared to 2023-bringing the total number of tests sent since service inception to over 558,000. This milestone reflects the expansion of security awareness activities across subscribed organizations.

558,604

Phishing test since service inception

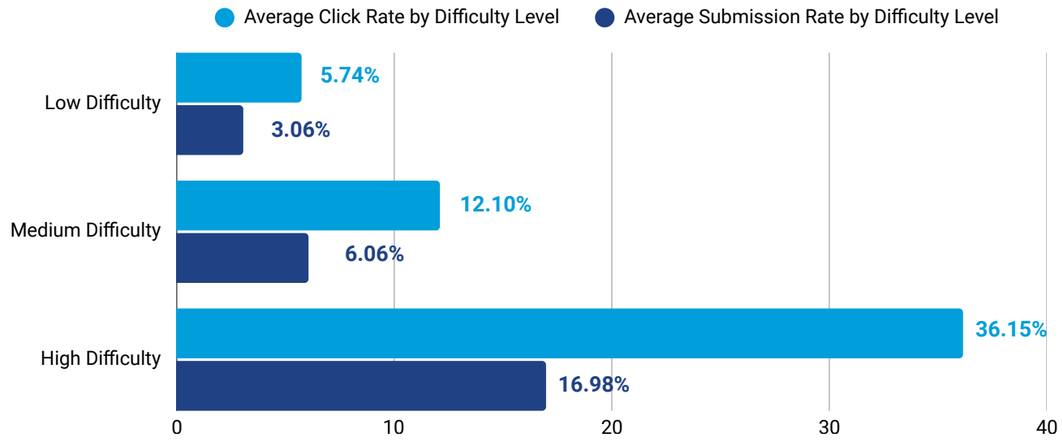
Phishing Tests Sent by UNICC



This year's analysis includes new data segmented by simulation type and difficulty level, revealing key insights:

- QR code-based phishing simulations had an average failure rate of 6.45%, significantly lower than the overall average of 15.36%, likely due to the extra step required to scan a code. However, such attacks can bypass traditional security controls and still pose substantial risk.
- Attachment-based simulations recorded a higher failure rate of 22.65%, highlighting the need for continued user education on the risks posed by malicious attachments, despite the protection offered by scanning tools.
- Difficulty level trends show that higher simulation complexity correlates with increased user susceptibility, reinforcing the importance of tailoring training to different skill level.

Average Click Rate and Submission Rate by Difficulty Level



Understanding the impact of simulation type and difficulty level is essential for accurate performance evaluation. Consistent with the 2023 findings, difficulty levels are assessed using the NIST framework. All statistics presented in his report are fully anonymized.

Note: UNICC only uses anonymized statistics in this report.

Context and Background

In a time where cyberthreats continually evolve, a robust cybersecurity awareness program is vital to strengthening an organization's overall security posture. The UNICC Cybersecurity Awareness Landscape Report serves as both an evaluation tool for ongoing initiatives and a record of progress over time. It identifies areas for improvements, and ensure that strategies remain adaptable to the rapidly changing digital environment in which the UN system operates.

In 2024, UNICC supported **22 organizations** in raising awareness of cyberthreats and promoting best practices. This collaborative approach allows for the observation of diverse adoption strategies and cultural approaches to security awareness across the UN family. Partner organizations benefit from UNICC's extensive experience in delivering shared programmes, positioning UNICC as a strategic partner for cybersecurity awareness initiatives.

During the year, UNICC delivered **182,516 phishing simulation messages** to users, contributing to a cumulative total of **over 558,000 messages** since the service began. This achievement reflects not only the scale of the programme, but also sustained relevance in equipping users with practical, scenario-based experience.

The effectiveness of these efforts is underpinned by carefully tailored cybersecurity awareness training, developed in partnership with leading industry leaders, and complemented by realistic phishing simulation designed for the UN context. The approach focuses on driving measurable behavioural change, using data from **UNICC's common solution** to track user trends and identify opportunities for targeted reinforcement.

By combining specialized training, actionable insights, and ongoing engagement, UNICC fosters a culture in which all personnel understand their role in safeguarding both personal and organizational resources. The programme's success underscores the principle that the human factor remains both the greatest vulnerability and the most powerful defence in cybersecurity.

22

UN organizations supported

182K+

Phishing Simulations Messages Delivered in 2024

558K+

Phishing Simulations Messages Delivered since Service Inception

UNICC cybersecurity awareness programms in 2024

UNICC Methodology

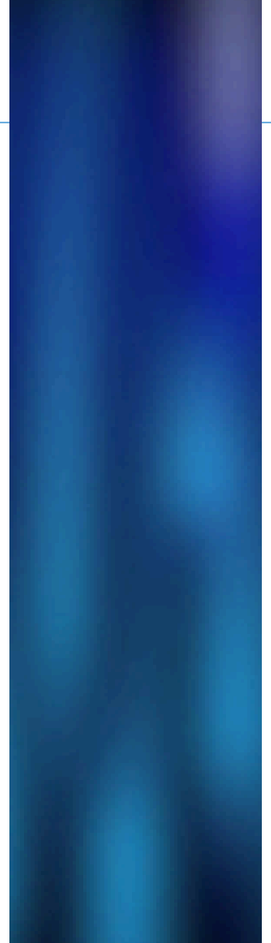
UNICC's approach to cybersecurity awareness combines industry-leading platforms, open-source tools, and in-house expertise to deliver comprehensive training and sophisticated phishing simulations. The service is offered as a common solution for the entire UN system, allowing multiple organizations to share resources, benefit from economies of scale, and leverage collective insights gained from a broad base of participants. This shared approach strengthens the overall cybersecurity posture of the UN ecosystem while ensuring consistent standards across diverse operational contexts.

The process begins with an initial assessment to understand each organization's cybersecurity landscape and identify potential weaknesses. Based on these findings, UNICC develops tailored training programmes that address specific gaps while aligning with the organization's culture and operational goals.

Training is designed to be engaging, interactive and relevant, incorporating real-world phishing simulations, and updated content to address emerging threats. The goal is to foster a security-conscious culture in which all personnel share responsibility for cybersecurity, rather than simply improving individual technical skills.

Regular reviews ensure the cybersecurity awareness programme remains effective and aligned with the evolving threat landscape. The platforms used offer robust tools for creating, managing, and measuring awareness initiatives, enabling organizations to track progress, and refine their strategies overtime. The choice of platform is guided by the specific needs and objectives of each organization, ensuring maximum relevance and impact.

Through this common service model, participating organizations not only strengthen their internal capabilities but also contribute to a collective body of knowledge that benefits the entire UN system.



Data collection methods

Accurate and consistent data collection is fundamental to evaluating the effectiveness of a cybersecurity awareness programme and identifying areas for improvement. Within the framework of UNICC's common solution, anonymized statistics from participating organizations are aggregated, enabling richer comparative analysis and the identification of system-wide trends that benefit the entire community.

The primary data collection methods include:

- **Simulated phishing attacks:** Measuring how effectively personnel detect and respond to suspicious emails. Data includes the number of individuals who clicked links, opened attachments, scanned QR codes, submitted credentials, or reported the email as suspicious.
- **Learning Management System (LMS) analytics:** For organizations using the integrated LMS, detailed users engagement metrics are collected, along with insights into platform integration and configuration strategies.
- **Questionnaires:** Completed by each organization's Chief Information Security Officer (CISO), to provide qualitative insights into programme structure, priorities, and perceived effectiveness.

Security Awareness Programme

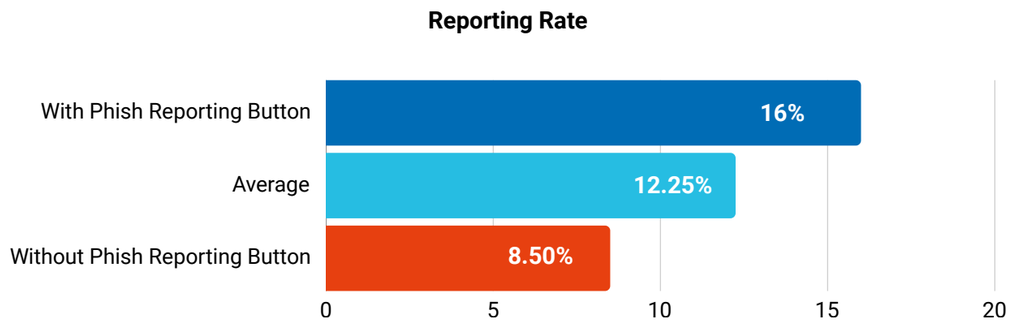
Current Cybersecurity Awareness Status

Platform Integration

Analysis of platform adoption shows a steady increase in the integration of security awareness tools and processes:

- **60%** of organizations use the Learning Management System (LMS) that is built into the security awareness platform, providing a centralized view of user progress and enabling an automation feature that enhance the programme efficiency.
- **70%** have implemented Single Sign On (SSO) for easier and more secure user access.
- **60%** have deployed System for Cross-domain Identity Management (SCIM) provisioning, enabling automatic detection of accounts for departing users and reducing administrative burden. UNICC recommends combining SCIM provisioning with SSO for optimal efficiency and security.
- **45%** of organizations have integrated the “report phish” button into corporate email clients, representing a 10% increase from the previous year. Organizations with this feature see an average phishing email reporting rate of 16%, double the rate of organizations without it (8.5%). This low-cost integration significantly reduces the workload of service desk and Security Operations Centres by enabling faster detection and response.

UNICC strongly recommends all organizations implement a simple, visible reporting mechanism for suspicious emails, paired with regular user training to reinforce its use.



Main Activities

Data from phishing simulations and custom training courses across participating organizations indicates:

- The average course completion rate for Cybersecurity Awareness Training for All Users was 72% across all organizations.
- In organizations where training is mandatory (71% of participating organizations), the completion rate increases to 80%.

UNICC recommends making cybersecurity awareness training mandatory for all personnel to ensure consistent knowledge levels and readiness across the organization.

Phishing Simulation Statistics

2024 Overview

Average Click Rate

15.36%

Average Submitted Credential Rate

7.25%

Average QR Code Scanned

6.45%

Average Opened Attachment

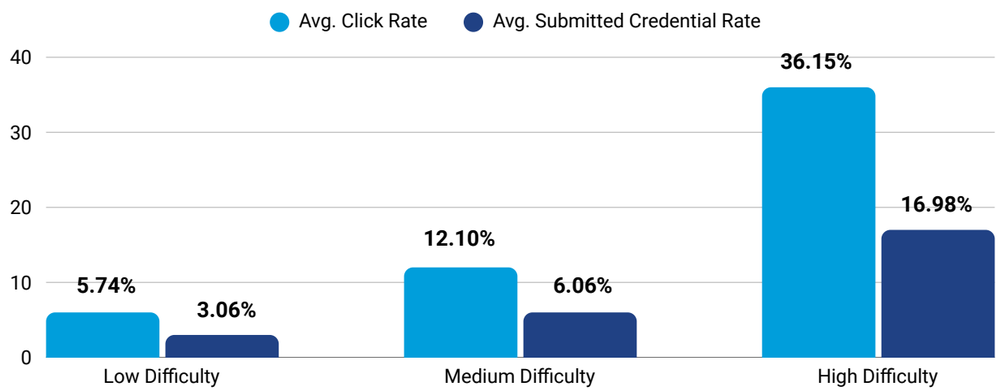
22.65%

If these had been real attacks, the potential organizational impact would have been severe.

Results by difficulty level

Using the NIST framework for rating phishing detection difficulty:

- **Low difficulty** – Click rate 5.74%, submission rate 3.06%.
- **Medium difficulty** – click rate 12.10%, submission rate 6.06%.
- **High difficulty** – Average click rate 36.15%, credential submission rate 16.98%.



These results confirm that higher complexity increases user susceptibility, underlining the need for progressive training that addresses increasingly sophisticated attack patterns. The ability to benchmark performance across organizations using UNICC's shared data enables targeted improvements system-wide.

Reinforcement Activities

Reinforcement materials such as posters, newsletters, blog posts and webinars play a critical role in sustaining awareness beyond initial training. UNICC's analysis shows that:

- Engagement is highest at the start of a programme but declines if content volume is excessive.
- The most effective strategy balances necessary security information with engaging, relatable content to maintain interest without causing training fatigue.

A strong security culture goes beyond merely implementing security measures or conducting training. It involves shaping attitudes, influencing behaviours, and fostering a shared sense of responsibility. UNICC seeks to identify effective strategies and best practices to achieve this, such as through targeted education programs, ongoing communication about security issues, and the development of policies and procedures that support the instillation of secure behaviour.

UNICC strives to ensure security becomes a habitual and integral part of every employee's day-to-day activity, leading to a safer, more secure organization.

As such, UNICC's training programme offers materials (newsletters, posters, and webinars) and other activities to reinforce learning the importance of security. Targeted reinforcement activities help users:

- Recognize and report suspicious activities.
- Apply strong password practices.
- Protect sensitive data.
- Stay informed on emerging risks

Through its common solution, UNICC enables organizations to share effective reinforcement strategies, maximizing reach and efficiency while reducing duplication of effort.

The Way Forward

Cybersecurity awareness remains the foundation of a strong cybersecurity strategy. Human error continues to be the most exploited vulnerability in cyberattacks. As threats grow in sophistication, it is essential that every personnel understand their role in protecting the organization, regardless of position.

Through its common cybersecurity awareness programmes, UNICC equipes with the knowledge and skills to recognize and respond to cyberthreats, fostering a culture of shared responsibility for safeguarding people, assets and digital resources. UNICC's security awareness programme encourages employees to act safely online, to use strong passwords, enable multi-factor authentication, and perform work-related tasks within secure networks. UNICC helps foster a culture of security in which everyone understands their role in protecting the organization, its people, and its digital assets. By uniting organizations under shared framework, the UN system can raise its collective resilience against cyberthreats and set a consistent standard of cybersecurity across all entities.

To strengthen cybersecurity awareness across the organization, UNICC recommends:

1. **Leadership commitment**
visible endorsement from leadership to reinforce the importance of cybersecurity.

2. **Recognition programmes**
Reward staff who demonstrate exemplary security practices, encouraging broader engagement.

3. **Accessible reporting mechanisms**
Maintain easy-to-use tools, such as the "report phish" button, to support swift incident containment, hence limiting the impact of attacks targeting large groups of users within the organization.

4. **Positive training culture**
Present training as a growth opportunity, rather than a punitive measure.

5. **Mandatory training for all personnel**
Establish consistent baseline knowledge across the organization.

6. **Balanced content delivery**
Avoid overwhelming users with excessive information.

7. **Regular phishing simulations**
Conduct phishing simulations on a regular basis to improve detection skills.

8. **Reinforcement activities**
Use engaging training approaches such as interactive e-learning, games, quizzes, and real-world simulations to sustain awareness.

9. **Timely updates**
Share information on evolving threats and countermeasures.

10. **Reward good practices**
Whenever a user reports something suspicious or prevents a cyber-attack, this should be rewarded via recognition for the act.

11. **Incremental maturity growth**
Follow the SANS Security Awareness Maturity Model, recognizing that advancing maturity levels requires time, resources and dedicated staff. (SANS data shows maturity level 5 programmes average 4.18 Full Time Equivalent (FET)).

UNICC | Cybersecurity

www.unicc.org

TLP: CLEAR

UNICC | Cybersecurity

Cybersecurity Awareness Landscape Report 2024

July 2025

TLP: CLEAR