GOCE DELCEV UNIVERSITY, STIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2025

THIRD INTERNATIONAL CONFERENCE

24-25 SEPTEMBER, 2025

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“, ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

GOCE DELCEV UNIVERSITY, STIP
FACULTY OF ELECTRICAL ENGINEERING

ТРЕТА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
THIRD INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2025

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

24-25 септември 2025 | 24-25 September 2025

ISBN: 978-608-277-128-1
DOI: https://www.doi.org/10.46763/ETIMA2531

Главен и одговорен уредник / Editor in Chief
проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Дарко Богатинов / Darko Bogatinov

Издавач / Publisher
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10А / Adress: Krste Misirkov, 10A
Пош. фах 201, Штип - 2000, С. Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (3 ; 2025 ; Штип)
Зборник на трудови [Електронски извор] / Трета меѓународна конференција ЕТИМА 2025, 24-25 септември 2025 ; [главен и одговорен уредник Сашо Гелев] = Conference proceedings / Third international conference, 24-25 September 2025 ; [editor in chief Saso Gelev]. - Текст во PDF формат, содржи 357 стр., илустр. - Штип : Универзитет "Гоце Делчев", Електротехнички факултет ; Stip : "Goce Delchev" University, Faculty of Electrical engineering, 2025

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima/en. - Наслов преземен од екранот. - Опис на изворот на ден 30.10.2025. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-277-128-1

а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Инфоматика -- Примена -- Собири

COBISS.MK-ID 67297029

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Дарко Богатинов / Darko Bogatinov
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Георги Иванов Георгиев / Georgi Ivanov Georgiev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет,
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владо Гичев / Vlado Gicev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Марија Чекеровска / Marija Cekerovska
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Мишко Џидров / Misko Dzidrov
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Александар Крстев / Aleksandar Krstev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ванчо Аџиски / Vancho Adziski
Факултет за природни и технички науки,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Natural and Technical Sciences,
Goce Delcev University, Stip, North Macedonia;

Томе Димовски / Tome Dimovski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Зоран Котевски / Zoran Kotevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Никола Рендевски / Nikola Rendevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Илија Христовски / Ilija Hristovski
Економски факултет,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Economy,
University St Climent Ohridski, North Macedonia;

Христина Спасовска / Hristina Spasovska
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Роман Голубовски / Roman Golubovski
Природно-математички факултет,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Mathematics and Natural Sciences,
Ss. Cyril and Methodius University, North Macedonia;

Маре Србиновска / Mare Srbinovska
Факултет за електротехника и информациски технологии,
Универзитет „Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Златановска / Biljana Zlatanovska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Александра Стојанова Илиевска / Aleksandra Stojanova Ilievska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Мирјана Коцалева Витанова / Mirjana Kocaleva Vitanova
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ивана Сандева / Ivana Sandeva
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Наташа Стојковиќ / Natasa Stojkovik
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

PREFACE

The Third International Conference “Electrical Engineering, Technology, Informatics, Mechanical Engineering and Automation – Technical Sciences in the Service of the Economy, Education and Industry” (ETIMA’25), organized by the Faculty of Electrical Engineering at the “Goce Delchev” University – Shtip, represents a significant scientific event that enables interdisciplinary exchange of knowledge and experience among researchers, professors, and experts in the field of technical sciences. The conference was held in an online format and brought together 78 authors from five different countries.

The ETIMA conference aims to establish a forum for scientific communication, encouraging multidisciplinary collaboration and promoting technological innovations with direct impact on modern life. Through the presentation of scientific papers, participants shared the results of their research and development activities, contributing to the advancement of knowledge and practice in relevant fields.
The first ETIMA conference was organized four years ago, featuring 40 scientific papers. The second conference took place in 2023 and included over 30 papers. ETIMA’25 continued this scientific tradition, presenting more than 40 papers that reflect the latest achievements in electrical engineering, technology, informatics, mechanical engineering, and automation.

At ETIMA’25, papers were presented that addressed current topics in technical sciences, with particular emphasis on their application in industry, education, and the economy. The conference facilitated fruitful discussions among participants, encouraging new ideas and initiatives for future research and projects.

ETIMA’25 reaffirmed its role as an important platform for scientific exchange and international cooperation. The organizing committee extends sincere gratitude to all participants for their contribution to the successful realization of the conference and its scientific value.

We extend our sincerest gratitude to all colleagues who, through the presentation of their papers, ideas, and active engagement in discussions, contributed to the success and scientific significance of ETIMA’25.

The Organizing Committee of the Conference

ПРЕДГОВОР

Третата меѓународна конференција „Електротехника, Технологија, Информатика, Машинство и Автоматика – технички науки во служба на економијата, образованието и индустријата“ (ЕТИМА’25), организирана од Електротехничкиот факултет при Универзитетот „Гоце Делчев“ – Штип, претставува значаен научен настан кој овозможува интердисциплинарна размена на знаења и искуства меѓу истражувачи, професори и експерти од техничките науки. Конференцијата се одржа во онлајн формат и обедини 78 автори од пет различни земји.

Конференцијата ЕТИМА има за цел да создаде форум за научна комуникација, поттикнувајќи мултидисциплинарна соработка и промовирајќи технолошки иновации со директно влијание врз современото живеење. Преку презентација на научни трудови, учесниците ги споделуваат резултатите од своите истражувања и развојни активности, придонесувајќи кон унапредување на знаењето и практиката во релевантните области.

Првата конференција ЕТИМА беше организирана пред четири години, при што беа презентирани 40 научни трудови. Втората конференција се одржа во 2023 година и вклучи над 30 трудови. ЕТИМА’25 продолжи со истата научна традиција, презентирајќи повеќе од 40 трудови кои ги отсликуваат најновите достигнувања во областа на електротехниката, технологијата, информатиката, машинството и автоматиката.

На ЕТИМА’25 беа презентирани трудови кои обработуваат актуелни теми од техничките науки, со посебен акцент на нивната примена во индустријата, образованието и економијата. Конференцијата овозможи плодна дискусија меѓу учесниците, поттикнувајќи нови идеи и иницијативи за идни истражувања и проекти.

ЕТИМА’25 ја потврди својата улога како значајна платформа за научна размена и интернационална соработка. Организациониот одбор упатува искрена благодарност до сите учесници за нивниот придонес кон успешната реализација на конференцијата и нејзината научна вредност. Конференцијата се одржа онлајн и обедини седумдесет и осум автори од пет различни земји.

Изразуваме голема благодарност до сите колеги кои со презентирање на своите трудови, идеи и активна вклученост во дискусиите придонесоа за успехот на ЕТИМА’25 и нејзината научна вредност.

Организационен одбор на конференцијата

СОДРЖИНА / TABLE OF CONTENTS:

Трета меѓународна конференција ЕТИМА
Third International Conference ETIMA

UDC: 004.49.056
https://www.doi.org/10.46763/ETIMA2531304m

THE ROLE OF CYBERSECURITY AWARENESS TRAINING TO PREVENT PHISHING

Hristijan Miceski[1], Dimitar Bogatinov[2]
[1]Ministry of Defence
[2]Military Academy General Mihailo Apostolski, Skopje
email: hristijan.miceski@mod.gov.mk
email: dimitar.bogatinov@ugd.edu.mk

Abstract

Phishing remains one of the most common cyber threats today, with email being the primary attack vector. Cybersecurity awareness training plays a critical role in strengthening an organization's defence against persistent threats. This research paper examines the impact of cybersecurity awareness training on employees' "online" behavior. The analysis utilizes results from earlier research to evaluate baseline cyber hygiene and assess how training impacts employees' ability to recognize and respond to phishing threats. Following the results, a comprehensive cybersecurity awareness training program was implemented, focusing on recognizing and reporting phishing emails, safe browsing practices, and maintaining strong passwords. The results indicate a significant improvement in the organization's cyber hygiene post-training. The data reveals a substantial decrease in the number of employees' falling victim to phishing attempts, alongside a notable increase in the reporting of phishing emails to the IT department. These findings suggest that the training not only enhanced employees' ability to recognize phishing attempts but also encouraged them to stay alert and report suspicious activities. Furthermore, this study underscores the importance of continuous training and periodic phishing simulations to sustain high levels of cybersecurity awareness. Regular training programs equip employees with the necessary skills to identify and respond to cyber threats, ultimately creating a more secure and resilient digital environment.

Key words:

phishing, cybersecurity, awareness, training.

Introduction

The digital transformation of modern organizations has fundamentally altered the cybersecurity landscape, creating new vulnerabilities while expanding the attack surface available to threat actors. Among the numerous cyber threats facing organizations today, phishing attacks have emerged as one of the most persistent and effective methods employed by threat actors. The sophistication and frequency of these attacks continue to escalate, with recent research indicating dramatic increases in phishing attempts across all sectors.

Phishing attacks represent a form of social engineering that exploits human psychology rather than relying only on technical vulnerabilities. This human-centric approach makes phishing particularly dangerous because it targets the one element of cybersecurity that can't be patched or updated through traditional technical means, human behavior and decision-making. The effectiveness of phishing lies in its ability to manipulate emotions, create false urgency, and exploit trust relationships within organizational contexts. The fundamental challenge in combating phishing attacks lies in their exploitation of human factors. Traditional cybersecurity approaches focusing primarily on technical controls, while necessary, prove insufficient against

attacks that specifically target human vulnerabilities. This reality has led to increased recognition of cybersecurity awareness training as a critical component of comprehensive organizational defense strategies.

Our previous research highlighted significant vulnerabilities related to employees' tendency to fall for phishing attacks. Through a series of four distinct phishing simulations, ranging from IT department impersonations requesting credentials to HR communications prompting data entry or file downloads, we identified concerning trends. The success rates of these simulated attacks ranged from 10% to as high as 26%. Even more concerning is the low number of suspicious emails reported to the IT department. Furthermore, 80% of individuals who had previously fallen victim were susceptible to being phished again. These findings strongly indicated that existing awareness levels and reporting mechanisms were insufficient and that a more effective, a focused training strategy was urgently needed to enhance employees' awareness.

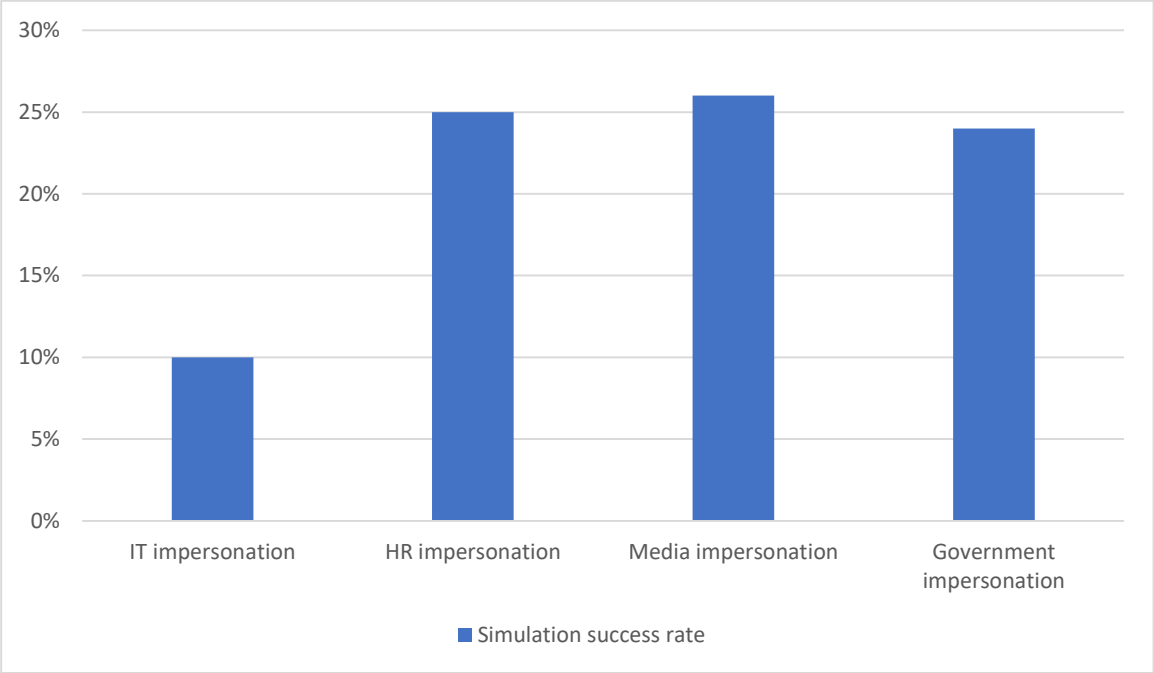

Fig. 1 Phishing simulation success rate

Source: Miceski H., Bogatinov D. (2024). THE IMPACT OF EMPLOYEES' CYBER-AWARENESS TRAINING ON THE EFFECTIVENESS OF PHISHING ATTACKS. Contemporary Macedonian Defence, (47), 65–76.

Effective cybersecurity awareness training must go beyond simple information dissemination to create meaningful behavioral change. It requires understanding the psychological mechanisms that make phishing effective, designing training programs that address these vulnerabilities, and maintaining awareness through consistent and repeated training efforts. The training must also be adaptive, evolving to address new attack vectors and social engineering techniques as they emerge.

This study explores how structured cybersecurity awareness training can improve employees' ability to recognize and respond to phishing attacks. Using data from a previously implemented training program, the research evaluates how targeted, interactive training can strengthen an organization's overall cybersecurity posture. The goal was to see whether focused training

could reduce the number of employees' falling for phishing attempts and increase the reporting of suspicious emails.

Literature review

The academic literature consistently emphasizes the human factor as the most critical element in cybersecurity defense systems. The NIST Phish Scale framework, provides a scientific approach to measuring phishing message detection difficulty through the concept of premise alignment. This framework establishes that the stronger the premise alignment between a phishing email and the recipient's work context, the more difficult it becomes to detect the fraudulent nature of the message. This theoretical foundation supports the development of targeted training programs that address specific organizational contexts and employees' roles.

Grimes (2024) in „Fighting Phishing" emphasizes that effective phishing defense requires a mix of methods combining technical controls with comprehensive user education. The research highlights that organizations achieving the greatest success in phishing prevention implement continuous training programs rather than one-time awareness sessions. This approach recognizes that cybersecurity awareness is not a static state but requires ongoing reinforcement and adaptation to emerging threats.

Studies by Bada et al. (2019) on security awareness training retention demonstrate that traditional training methods often fail to create lasting behavioral change. Their research reveals that training programs incorporating gamification, real-world scenarios, and regular repetition achieve significantly higher retention rates and improved security behaviors compared to conventional presentation-based training.

Analysis of baseline security culture assessment

Based on analysis from our previous research, beyond individual vulnerability measurements, the initial assessment revealed systemic issues in organizational security culture that would need to be addressed through comprehensive training programs. The extremely low reporting rate indicated that employees either lacked knowledge about proper reporting procedures, feared negative consequences for reporting false positives, or did not understand the importance of threat intelligence sharing within the organization. Interviews with employees who participated in the baseline simulations revealed additional insights into organizational security culture challenges. Many employees expressed uncertainty about how to verify the authenticity of suspicious communications, particularly when they appeared to come from internal sources. Others indicated that they had noticed suspicious elements in phishing emails but were unsure whether these observations warranted formal reporting. The baseline assessment also revealed gaps in employee understanding of the broader cybersecurity threat landscape and their role in organizational defense. Many employees viewed cybersecurity as primarily an IT department responsibility rather than understanding their individual contributions to overall organizational security posture.

Research methodology

This study was conducted within the same organization as the initial research, allowing for a direct follow-up and assessment of interventions. The methodology involved two primary phases: the implementation of a targeted training program and the subsequent evaluation of its effectiveness.

The training intervention specifically targeted the group of employees who were identified as vulnerable in our previous research, those who had failed one or more of the initial four phishing simulations. This focused approach aimed to directly address the most significant human-factor risks within the organization by providing remedial and enhanced training to those most in need.

To enhance employees' resilience against phishing attacks, a diverse training program was developed and deployed. The program moved beyond general awareness to focus on practical skills and real-world application. Key elements included:

- Content focus: The training materials explored the anatomy of phishing emails, examining specific elements from the header to the signature. It emphasized recognizing 'cues', such as sender discrepancies, odd domains, language irregularities, undue urgency, and hidden or mismatched URLs, based on real-world examples.
- Interactive tools: To engage employees and provide hands-on experience in a safe environment, a suite of online training tools was utilized. These platforms included Jigsaw's Phishing Quiz, Guardey, ProProfs User-Generated Quizzes, Infosequre, and Egress. These tools offered various interactive scenarios, quizzes, and simulations to reinforce learning objectives.
- Delivery: The training was delivered ensuring that all members of the focus group completed the necessary modules, confirmed via completion notifications.

Due to financial constraints precluding the execution of a new, large-scale controlled phishing simulation, an alternative, real-world monitoring approach was adopted. This assessment was conducted over a one-month period following the completion of the training program:

- Using mail protection software: The organization's existing email security system continuously blocks and quarantines suspected phishing emails.
- Reviewing and controlled release: Instead of discarding all blocked emails, we analyzed these quarantined messages. Emails confirmed to be phishing attempts but deemed safe (links leading to known-benign sinkholes or having no active payload) were identified.
- Targeted distribution: These reviewed, safe phishing emails were then manually released from quarantine only to the inboxes of the employees within the training focus group. This allowed for the observation of their reactions to actual phishing attempts.
- Interaction monitoring: The system and IT personnel monitored whether any employees in the focus group interacted negatively with these released emails.
- Reporting tracking: Crucially, employees were instructed during training to report all suspicious emails to the IT department via existing channels. The IT department carefully tracked every report received from the focus group concerning these released emails.

This methodology, while unconventional, allowed for an assessment based on employees' responses to realistic threats under controlled observation, providing valuable insights into the training's impact on both susceptibility and proactive reporting behavior.

Results

The post-training assessment was conducted over a one-month period immediately following the completion of the comprehensive cybersecurity awareness program. During this period, employees in the focus group were exposed to a series of reviewed, real-world phishing emails released under controlled conditions. The monitoring focused on two key performance

indicators: susceptibility (whether employees interacted negatively with the phishing attempts) and reporting behavior.

The findings a significant and positive change in employees' behavior following the targeted training intervention:

- Phishing susceptibility: Throughout the one-month assessment period, none of the employees in the focus group fell victim to the released phishing emails. There were no recorded instances of clicks on malicious links, attempts to enter credentials, or downloads of suspicious files from this group. This represents a complete turnaround from the 10-26% failure rates observed across various scenarios in the initial simulations.
- Phishing reporting: A significant increase in proactive security behavior was observed. The focus group achieved a perfect reporting rate, reflecting their strong awareness. Almost every single reviewed phishing email released to this group was subsequently reported to the IT department. Reports were made using the established channels: direct emails or phone calls to IT personnel.

These results demonstrate a substantial improvement in the cyber hygiene of the trained employees. The data clearly shows that the focused training program was highly effective in not only eliminating risky behaviors but also in fostering a strong culture of proactive reporting within the target group.

The results presented in this study demonstrate a remarkable improvement in phishing resilience among the targeted group of employees. Achieving a zero percent failure rate and very high reporting rate during the post-training assessment period provides strong evidence for the effectiveness of the implemented cybersecurity awareness program. This section interprets these findings, explores the potential reasons for this success, acknowledges limitations, and proposes future directions. The dramatic shift from significant vulnerability to near-perfect vigilance suggests that the training intervention resonated deeply with the focus group. Several factors likely contributed to this success.

Firstly, the departure from standard classroom-style training towards interactive, online tools likely enhanced engagement and knowledge retention. These platforms provided practical, hands-on experience in identifying real-world phishing scenarios.

Secondly, the training's messaging appears to have been crucial. By emphasizing that employees are a vital asset in the organization's defense, the program likely fostered a greater sense of personal responsibility and empowerment. However, this positive reinforcement was coupled with a clear message of accountability. Employees were reminded of the Standard Operating Procedures (SOPs) and the potential consequences of non-compliance, such as limitations on internet access. This combination of empowerment and accountability likely served as a powerful motivator. It encouraged employees not just to learn but to actively apply their knowledge, leading to the observed double-checking behaviors and the exceptional level of reporting. The high reporting rate, in particular, signifies a growing culture of awareness, where employees moved from passive recipients to active participants in organizational security.

While the use of real-world phishing emails instead of a purpose-built simulation was dictated by operational limits, it provided a uniquely realistic assessment environment. Employees were tested against actual threats they might encounter. The fact that reporting occurred via existing,

less streamlined channels (email and phone) further underscores the employees' determination to act, suggesting a deep impact from the training.

Despite the strong positive results, certain limitations must be acknowledged.

- Focus group bias: The study concentrated only on employees who had previously failed. While this was a logical approach to address the highest risks, the results may not be generalizable to the entire workforce without broader implementation and testing.
- Assessment duration: The assessment period was one month. While indicative of immediate impact, it does not guarantee long-term retention of these behaviors. Cybersecurity awareness can weaken over time without regular reinforcement.
- Motivation factors: The strong influence of potential penalties makes it difficult to isolate the impact of education alone. While effective, a compliance-driven culture might differ from one driven purely by internal motivation.
- Reporting mechanism: The reliance on manual reporting (email/phone) is less efficient and harder to track long-term than a dedicated tool.

Future Directions and Recommendations

These findings strongly support investment in cybersecurity training but also highlight areas for future development:

- Continuous reinforcement and micro learning: To combat knowledge decay and maintain high levels of awareness, organizations should move towards ongoing training models. Implementing micro learning, delivering short, focused training modules regularly, and providing continuous reinforcement through periodic reminders, updates, and brief simulations is essential.
- Implement a „Report Phish" button: To streamline the reporting process, reduce friction for users, and improve tracking capabilities, implementing a dedicated „Report Phish" button within the email client is highly recommended.
- Expand training and periodic simulations: The successful program should be adapted and rolled out to all employees. Where feasible, periodic phishing simulations should be conducted to validate long-term effectiveness across the organization.
- Balance education and accountability: Further explore the interplay between positive reinforcement and negative reinforcement to create a sustainable and positive security culture.

The study confirms that focused, interactive training significantly reduces phishing risks. Moving forward, the main challenge is keeping these gains and making security awareness stick as part of everyday work culture.

Conclusion

This research shows how targeted cybersecurity training can effectively reduce phishing threats in public organizations. Based on earlier findings that revealed employee vulnerabilities and poor reporting habits, this study designed and tested a comprehensive training program for the most at-risk employees.

The results clearly show the program worked. After training, no employees fell for phishing attempts and almost all employees reported suspicious emails. This shows a major shift from being vulnerable to being alert and proactive. When employees are properly trained and

motivated, they become strong defenders against cyber-attacks. The mix of interactive tools, real examples, and clear expectations about employees' roles proved very effective.

The study confirms that investing in cybersecurity training pays off for organizational security. Training needs to be engaging, practical, and supported by clear organizational expectations. To keep these improvements and build a lasting security culture, organizations must continue with ongoing efforts like short learning sessions and regular reinforcement. This ensures employees' stay ready to handle constantly changing cyber threats.

References

[1] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. *"Phishing Attacks: A Recent Comprehensive Study and a New Anatomy."* Frontiers in Computer Science, 3, (2021).

[2] Ana Ferreira and Soraia Teles. *Persuasion: How phishing emails can influence users and bypass security measures.* International Journal of Human-Computer Studies 125 (2019), pp. 19–31.

[3] Bada, Maria & Sasse, Angela & Nurse, Jason. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*. (2015). pp. 118-131.

[4] Caputo, Deanna D., Mitre, Shari Lawrence Pfleeger, Jesse D. Freeman and Mitre M Eric Johnson. *"Going Spear Phishing: Exploring Embedded Training and Awareness."* IEEE Security & Privacy 12 (2014). pp. 28-38.

[5] Dawkins, S. and Jacobs, J. *NIST Phish Scale User Guide*. (2023).

[6] Grimes, Roger A. *Fighting Phishing: Everything You Can Do to Fight Social Engineering and Phishing*. Hoboken, NJ: Wiley, (2024).

[7] Lutchkus, P., Wang, P., Mahony, J. *Simulation Tests in Anti-phishing Training*. In: Latifi, S. (eds) ITNG 2024: 21st International Conference on Information Technology-New Generations.

[8] Miceski H., Bogatinov D. *THE IMPACT OF EMPLOYEES' CYBER-AWARENESS TRAINING ON THE EFFECTIVENESS OF PHISHING ATTACKS*. Contemporary Macedonian Defence, (47), (2024), pp. 65-76.

[9] Nasir, Sadiq. *Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions*. Advances in Multidisciplinary and scientific Research Journal Publication. 2. (2023). pp. 151-160.

[10] Richa Goenka, Chawla, M. and Tiwari, N. *A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy*. International Journal of Information Security, 23(4), (2023). pp.831–836.

[11]Wang, Jingguo, Yuan Li, and H. Raghav Rao. *"Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences."* Information Systems Research 28, no. 2 (2017). pp. 378–96.