Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Languages

Bachelor Thesis

Securing the Digital Frontier: Ethical and Technical Approaches to Cybersecurity for Organizations and Users

Elsayed Ibrahim Elsayed Mohamed

© 2026 CZU Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Elsayed Ibrahim Elsayed Mohamed

Informatics

Thesis title

Securing the Digital Frontier: Ethical and Technical Approaches to Cybersecurity for Organizations and Users

---

Objectives of thesis

The main objective of the thesis is to explore the technical challenges and solutions in cybersecurity, with a focus on how organizations and individuals can implement effective measures to protect data and systems, while addressing ethical considerations in the digital age.

Methodology

The work consists of two parts – theoretical and practical. The theoretical part will be based on the study of secondary sources. The empirical part will be compiled on the basis of outputs from quantitative/qualitative research.

The proposed extent of the thesis

30 – 40 pages

Keywords

Cybersecurity dilemmas, Digital ethics, Information security industry, Corporate cybersecurity responsibility, Data protection, Cybersecurity frameworks, IT security governance, Cybersecurity decision-making, Professional cybersecurity ethics, Cybersecurity operations

---

Recommended information sources

Easttom, Chuck (2020). Computer Security Fundamentals. Pearson. ISBN: 978-0135774779.

Erickson, Jon (2008). Hacking: The Art of Exploitation. No Starch Press. ISBN: 978-1593271442.

Meeuwisse, Raef (2017). Cybersecurity for Beginners. Cyber Simplicity Ltd. ISBN: 978-1541016509.

Sammons, John and Cross, Michael (2016). The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Syngress. ISBN: 978-0124166509.

Stallings, William (2017). Network Security Essentials: Applications and Standards. Pearson. ISBN: 978-0134527338.

Expected date of thesis defence

2024/25 SS – PEF

Thesis supervisor

Ing. Kristýna Kučírková, MSc

Supervising department

Department of Languages

Electronic approval: 03. 06. 2025

PhDr. Mgr. Lenka Kučírková, Ph.D.

Head of department

Electronic approval: 25. 09. 2025

prof. Ing. Lukáš Čechura, Ph.D.

Dean

Prague on 13. 03. 2026

Declaration

I declare that I have worked on my bachelor's thesis, titled “Securing the Digital Frontier: Ethical and Technical Approaches to Cybersecurity for Organizations and Users” by myself, and that I have used only the sources listed at the end of the thesis. As the author of the bachelor's thesis, I declare that the thesis does not break any copyrights.

In Prague on 15.03.2026

Acknowledgement

I would like to thank Ing. Kristýna Kučírková, MSc and all other persons for their advice and support during my work on this thesis.

Securing the Digital Frontier: Ethical and Technical Approaches to Cybersecurity for Organizations and Users

Abstract

This bachelor's thesis examines technical and ethical approaches to cybersecurity for organizations and individual users, with a practical emphasis on phishing as a frequent socio-technical threat. Cybersecurity is treated not only as a set of technical controls, but also as an area in which responsibility, decision-making, and user trust are shaped by organizational practice. The work consists of two parts: theoretical and practical. The theoretical part draws secondary sources and outlines key cybersecurity challenges, protection measures, and governance procedures, while also addressing ethical considerations, including privacy, transparency, accountability, and proportionality. The practical part compiles outputs from published quantitative and qualitative research; a documented phishing-resilience case is reconstructed into comparable metrics and interpreted using qualitative findings. Layered protection, combining technical controls with awareness policies and ethically balanced governance, is identified as the most realistic approach.

Keywords: Cybersecurity dilemmas, Digital ethics, Information security industry, Corporate cybersecurity responsibility, Data protection, Cybersecurity frameworks, IT security governance, Cybersecurity decision-making, Professional cybersecurity ethics, Cybersecurity operations

Zajištění digitální hranice: Etické a technické přístupy ke kybernetické bezpečnosti pro organizace a uživatele

Abstrakt

V této bakalářské práci jsou zkoumány technické i etické přístupy ke kybernetické bezpečnosti organizací a jednotlivých uživatelů, přičemž praktický důraz je kladen na phishing jako častou socio-technickou hrozbu. Kybernetická bezpečnost je chápána nejen jako soubor technických kontrol, ale také jako oblast ovlivněná odpovědností, rozhodováním a důvěrou uživatelů v rámci organizačních postupů.

Práce se skládá ze dvou částí – teoretické a praktické. Teoretická část vychází ze sekundárních zdrojů a shrnuje klíčové hrozby, ochranná opatření a postupy řízení, přičemž jsou diskutována etická témata, jako je soukromí, transparentnost, odpovědnost a přiměřenost. Praktická část syntetizuje výstupy publikovaného kvantitativního i kvalitativního výzkumu; zdokumentovaná případová studie odolnosti vůči phishingu je převedena do srovnatelných metrik a interpretována s využitím kvalitativních zjištění. Vrstvený přístup kombinující technická opatření, osvětu a eticky vyvážené řízení je označen za nejrealističtější.

Klíčová slova: dilemata kybernetické bezpečnosti, digitální etika, odvětví informační bezpečnosti, odpovědnost organizací za kybernetickou bezpečnost, ochrana dat, rámce kybernetické bezpečnosti, řízení IT bezpečnosti, rozhodování v oblasti kybernetické bezpečnosti, profesní etika v kybernetické bezpečnosti, operace kybernetické bezpečnosti

Table of Contents

1 Introduction 11

2 Objectives and Methodology 13

2.1 Objectives 13

2.2 Methodology 13

3 Literature Review 15

3.1 Cybersecurity and Phishing in the Digital Environment 15

3.1.1 Cybersecurity in the Digital Environment 15

3.1.2 Small Organizations and Cybersecurity Challenges 15

3.1.3 Phishing as a Cybersecurity Threat 16

3.1.4 Social Engineering and Human Error in Phishing Attacks 17

3.1.5 Ethical Dimensions of Cybersecurity 17

3.2 Basic Technical Protections Against Phishing 18

3.2.1 Email Filtering and Spam Protection 18

3.2.2 Multi-Factor Authentication 18

3.2.3 Email Authentication Protocols (SPF, DKIM, DMARC) 18

3.2.4 Software Updates and Patch Management 19

3.2.5 Basic Network and Web Protection Measures 19

3.3 User Cybersecurity Awareness Policies 20

3.3.1 Security Awareness Training 20

3.3.2 Recognizing Suspicious Emails and Websites 20

3.3.3 Reporting Policies for Suspicious Messages 20

3.3.4 Password Practices and Safe User Behavior 21

3.3.5 Building a Security-Aware Organizational Culture 21

3.4 Combining Technical and Human Protection Measures 22

3.4.1 Why Technical Measures Alone Are Not Enough 22

3.4.2 Why Awareness Alone Is Not Enough 22
3.4.3 The Value of a Layered Security Approach in Small Organizations 22
3.4.4 Ethical Balance Between Protection, Privacy, and Responsibility 23
4 Practical Part 24
4.1 Introduction to the Selected Case 24
4.2 Case-Study Workflow and Analytical Setup 24
4.2.1 Reconstructed Environment and Roles 25
4.2.2 Scenario Logic and Contextual Factors 25
4.3 Data Collection, Metrics, and Evaluation Criteria 26
4.4 Results 27
4.4.1 Results by Phase 28
4.4.2 Results by Intervention Path 28
4.4.3 Contextual Comparison of the Analytical Phases 29
4.5 Compare-and-Contrast Analysis 31
4.6 Contribution of the Practical Part 32
5 Discussion of Results and Recommendations 33
5.1 Discussion of the Main Findings 33
5.2 Practical Recommendations for Small Organizations 34
5.3 Threats to Validity and Transferability 34
5.4 A Minimum Anti-Phishing Baseline for Small Organizations 35
5.5 Limits of the Thesis 35
6 Conclusion 37
7 References 38
8 List of pictures, tables, graphs and abbreviations 42
8.1 List of pictures 42
8.2 List of tables 42
8.3 List of graphs 42

8.4 List of abbreviations 43

Appendices 44

Appendix A: Metric Definitions and Calculation Logic 44

Appendix B: Example Minimal Phishing Response Workflow for a Small organization 45

1 Introduction

Cybersecurity has become part of ordinary daily life for both organizations and individual users. Communication, payments, file sharing, internal administration, and account access are increasingly dependent on digital systems. This shift creates clear advantages, but it also exposes people to constant security threats. Among these threats, phishing remains highly relevant because it is simple, adaptable, and effective. It usually does not depend on highly advanced technology; rather, it often succeeds by exploiting trust, distraction, urgency, and routine behavior. This topic was selected because it connects a broad cybersecurity problem to a practical, observable risk. In many real situations, successful attacks are not initiated by complex malware or sophisticated exploitation. They are initiated by an email, a link, a fake login page, or a message that appears routine enough to avoid suspicion. For that reason, phishing is used here as a lens through which broader cybersecurity issues can be examined. It is thereby shown that digital security is not only shaped by software and technical systems, but also by people, decisions, habits, and the way responsibility is shared within an organization.

The main focus is placed on small organizations. This focus is intentional. Large organizations often have dedicated security teams, formal procedures, and broader technical resources. By contrast, small organizations are frequently operated under tighter constraints. Security responsibilities may be shared informally, protections may be only partly implemented, and employees may receive limited training. As a result, even a basic phishing attempt may cause disproportionate damage. Credential theft, financial loss, service disruption, data exposure, and reputational harm may result from a single user action. Because of this, cybersecurity measures are needed that are not only effective but also realistic and manageable. An ethical dimension is also present in cybersecurity practice. Systems and data must be protected, but protection should be implemented in a way that respects users, encourages responsible reporting, and avoids a culture of fear or blame. In practice, secure behavior is more likely to be sustained when the reasons for rules are understood, when reporting routes are clear, and when organizational response is predictable. Cybersecurity is therefore treated not only as a technical challenge, but also as a question of communication, trust, accountability, and digital responsibility. This thesis

explores technical challenges and solutions in cybersecurity, with attention to how organizations and individual users can implement effective measures to protect data and systems, while also addressing ethical considerations. For practical clarity, phishing is used as a representative threat scenario to observe the interaction among technical controls, user behavior, and organizational policy. Two connected perspectives are considered. First, technical measures are considered, including email filtering, authentication mechanisms, multi-factor authentication, updates, and basic network or endpoint protections. Second, human and organizational measures are considered, including awareness training, recognition of suspicious communication, reporting procedures, and the development of a security-aware culture. Stronger protection is assumed to be achieved when measures are combined within a consistent governance approach. The thesis is divided into a theoretical and practical part. In the theoretical part, the role of phishing in the digital environment is explained, and the technical, human, and ethical dimensions of cybersecurity are discussed. In the practical part, this framework is applied through a secondary case-study analysis. Rather than presenting original field research, a documented case is examined and reorganized into an analytical discussion focused on weaknesses, protective measures, comparison, and lessons that may be transferred to smaller organizations. The final chapters present the main findings, interpret their meaning, and propose practical recommendations. This structure reflects the intention to connect theory with a practical and realistic problem. The goal is to show that cybersecurity improvement is not limited to complex or expensive solutions. In many small organizations, meaningful improvement can be achieved through a sensible baseline of technical protection, repeated awareness efforts, and clear organizational responsibility.

2 Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to explore the technical challenges and solutions in cybersecurity, with a focus on how organizations and individuals can implement effective measures to protect data and systems, while also addressing ethical considerations in the digital age. Within this scope, phishing is used as a concrete and realistic threat context to illustrate how technical controls and human-oriented policies interact in practice. The following partial objectives are pursued: to summarize technical cybersecurity measures relevant to everyday operations (identity and access management, email security, device and network protection, and baseline governance controls); to discuss ethical dilemmas related to security interventions, including privacy, transparency, accountability, and proportionality; to compile and analyze outputs from published quantitative and qualitative research, using a documented case reconstruction to calculate comparable metrics; to formulate practical and feasible recommendations for organizations and users, especially in resource-constrained environments.

The following research question is addressed:

How can ethical and technical cybersecurity measures be combined to protect data and systems for organizations and individual users, and what practical lessons can empirical evidence on phishing mitigation offer? To support a clear practical focus, the following sub-question guides the analysis: How do combined basic email and network protections, together with awareness and reporting policies, influence phishing-related outcomes in a documented empirical case?

2.2 Methodology

The work consists of two parts – theoretical and practical. The theoretical part will be based on the study of secondary sources. The empirical part will be compiled on the basis of outputs from quantitative/qualitative research.

In the theoretical part, academic articles, professional literature, and relevant standards are reviewed in order to describe current cybersecurity challenges, technical controls, governance practices, and ethical considerations that arise when protective measures affect users. Cybersecurity is treated as a socio-technical issue, meaning that technology, policies,

and user behavior are considered together rather than in isolation. In the practical part, no primary fieldwork is conducted. Instead, empirical evidence is extracted from published quantitative and qualitative outputs and reorganized into an analytical structure with explicit evaluation criteria. Quantitative outputs are used to compute comparable metrics, while qualitative outputs are used to interpret behavioral and organizational factors and to derive realistic recommendations for small organizations and individual users. A documented study providing measurable phishing outcomes is used as the core quantitative dataset. The practical dataset is extracted from the phishing-resilience study by Morić et al. (2025), which reported simulation outcomes under different intervention conditions. Additional qualitative findings from related studies and reviews are synthesized to interpret user response patterns, organizational communication, and ethical aspects of security interventions. For transparency, the practical analysis is organized around explicit variables and metrics. Extracted variables include the reported participant count, the reported number of compromised users, the intervention type, and contextual notes such as timing and training format. Where a value is not reported in the source, it is labelled as "not reported" rather than reconstructed. The main quantitative metric used is the compromise rate, calculated as: Compromise rate (%) = (compromised users / participants) × 100. The analytical logic is based on comparison: intervention conditions are identified and structured, comparable metrics are computed, and observed differences are interpreted using qualitative evidence from the literature, with attention to privacy, proportionality, and a non-punitive reporting culture. Because the empirical evidence is based on published outputs rather than primary fieldwork, claims are limited to what the available data supports and the selected case is treated as an illustrative empirical example rather than a universal model for all organizations.

After the introduction, Chapter 2 states the objectives, research questions, and methodology. Chapter 3 provides a literature review covering technical, human, and ethical dimensions of cybersecurity, with phishing used as an illustrative threat context. Chapter 4 presents the practical part through a documented case reconstruction, including the metric logic, tables, figures, and comparisons. Chapter 5 discusses the results and provides recommendations. Chapter 6 summarizes the main outcomes and concludes the thesis.

3 Literature Review

3.1 Cybersecurity and Phishing in the Digital Environment

3.1.1 Cybersecurity in the Digital Environment

Cybersecurity has become a basic condition of modern organizational life because daily communication, storage, administration, and financial operations now depend on digital systems. In that environment, security cannot be reduced to software or hardware alone. It also includes procedures, internal communication, role clarity, and user behavior. Recent research, therefore, increasingly treats cybersecurity as a socio-technical issue rather than a purely technical one (Awan and Alam, 2025, p. 1; Pollini et al., 2022, pp. 371-372). Easttom (2020) likewise presents computer security as a layered practice that combines technical controls, process discipline, and informed human behavior rather than relying on a single defensive mechanism. This broader view matters because many attacks succeed by exploiting ordinary work routines rather than by defeating highly sophisticated technical barriers. Users respond to messages, follow links, approve requests, and make decisions under time pressure. In that sense, cybersecurity outcomes are shaped by the interaction between systems and people. Panteli et al. describe responsible cybersecurity as a multi-layered effort involving technological, human, organizational, and societal dimensions, rather than a problem to be delegated solely to technical specialists (Panteli et al., 2025, p. 2). The ethical dimension follows naturally from this broader definition. Once cybersecurity is understood as affecting people, issues such as privacy, fairness, transparency, and accountability become central rather than optional. Ababneh et al. argue that ethical principles should be built into cybersecurity governance and design, because trust and resilience depend partly on how organizations treat users while trying to protect them (Ababneh et al., 2025, p. 212444).

3.1.2 Small Organizations and Cybersecurity Challenges

The security situation is especially difficult for small organizations. They are expected to operate in the same threat environment as larger institutions, but with lower budgets, fewer staff, and limited access to specialized expertise. Small and medium-sized enterprises are reported to be heavily exposed to phishing, ransomware, weak password practices, and related threats, because constrained resources make consistent cybersecurity management more difficult (Awan and Alam, 2025, p. 1). The problem is further complicated by the fact

that smaller organizations often rely on informal routines: responsibilities may be shared, tasks may change quickly, and security procedures may be applied inconsistently. This does not imply carelessness; rather, the security posture is typically shaped by practical constraints. For this reason, the most effective defensive strategy in such environments is not necessarily the most advanced, but the one that can be maintained over time with limited complexity (Awan and Alam, 2025, pp. 24–25, 32–33). It is also suggested that organizational culture matters strongly in these settings (Pollini et al., 2022, p. 386). Trust, usability, a security-aware culture, and the integration of policies into everyday work routines influence whether security practices are actually followed (Pollini et al., 2022, p. 386). This is especially important in smaller organizations, where a single employee action may have an immediate effect on the wider environment.

3.1.3 Phishing as a Cybersecurity Threat

Phishing remains one of the most persistent cybersecurity threats because it combines technical imitation with psychological manipulation. Attackers try to create a believable message, page, or request that prompts the user to take harmful action, such as clicking, downloading, disclosing credentials, or transferring information. Kavvadias and Kotsilieris describe phishing emails as deceptive messages that imitate legitimate communication, while Jamuna explains phishing more broadly as a social-engineering technique that exploits user trust in order to trigger unsafe actions (Kavvadias and Kotsilieris, 2025, p. 2; Jamuna, 2024, p. 2). From a practitioner perspective, Erickson (2008) is also useful because it shows how attackers often exploit predictable system and user weaknesses, which helps explain why phishing succeeds when trust and routine can be manipulated.

Phishing is also adaptable. It has moved beyond generic mass email into more targeted forms such as spear-phishing, vising, smishing, and social-media deception. This flexibility is one reason phishing is difficult to eliminate. Attackers can change language, timing, targets, and delivery channels faster than organizations can rely on one fixed defense model (Alkhalil et al., 2021, p. 2; Jamuna, 2024, p. 2). The consequences can be serious even when the initial interaction appears minor. Credential theft, malware delivery, data leakage, financial loss, productivity disruption, and reputational damage can all begin with one successful phishing message. That is why phishing is better understood as a chain of risk rather than a single event (Alkhalil et al., 2021, p. 2; Khan and Muntaha, 2024, p. 1664).

3.1.4 Social Engineering and Human Error in Phishing Attacks

Phishing works because it targets human decision-making. Messages often rely on authority, urgency, curiosity, routine, or fear. The goal is to reduce reflection time and encourage automatic action. Jamuna notes that phishing exploits cognitive and social vulnerabilities, while Kavvadias and Kotsilieris emphasize the role of urgency, familiarity, and perceived legitimacy in user response (Jamuna, 2024, pp. 2-3; Kavvadias and Kotsilieris, 2025, p. 2). At the same time, human error should not be treated as a simple individual failure. Susceptibility is shaped by context, work role, digital skill level, training quality, and organizational culture. The Applied Sciences review on phishing susceptibility shows that demographic, psychological, behavioral, and contextual factors all play a role in how users interpret suspicious messages (Kavvadias and Kotsilieris, 2025, pp. 12, 19-21). This is why user-centered security design matters. Pollini et al. and Grobler et al. both argue that security measures become weaker when they are badly communicated, too difficult to use, or detached from everyday work practices. Effective phishing defense, therefore, requires not only better users but also clearer systems and more supportive organizational design (Pollini et al., 2022, pp. 374, 386; Grobler et al., 2021, p. 14).

3.1.5 Ethical Dimensions of Cybersecurity

Cybersecurity decisions also involve ethical judgments. When an organization trains users, monitors suspicious activity, enforces authentication rules, or runs phishing simulations, it deliberately shapes user behavior. Those actions may be justified, but they still need to respect privacy, clarity, and proportionality. Ababneh et al. argue that ethical cybersecurity should integrate privacy, accountability, transparency, and fairness across governance and technical practice (Ababneh et al., 2025, pp. 2, 20). Meeuwisse (2017) similarly emphasizes that basic cybersecurity practice should be understandable and usable for ordinary people, which makes ethical clarity especially important in smaller organizations. User autonomy is particularly relevant in awareness-oriented security. Mersinas et al. note that people are more likely to trust security interventions when they understand both why the measure exists and how it operates. Once users feel manipulated rather than supported, trust can weaken, and long-term compliance may suffer (Mersinas et al., 2025, pp. 5, 12-13). For small organizations, the ethical question is practical rather than abstract. Security measures are more likely to be accepted and followed when leadership explains them clearly, limits unnecessary monitoring, and encourages reporting without blame. Cybersecurity

responsibility, therefore, becomes part of organizational legitimacy and protection (Panteli et al., 2025, pp. 2-3, 16-17).

3.2 Basic Technical Protections Against Phishing

3.2.1 Email Filtering and Spam Protection

Email filtering and spam protection form the first technical barrier against phishing because they reduce the number of dangerous messages that ever reach users. In practice, they examine sender reputation, suspicious links, attachment behavior, content patterns, and signs of spoofing. For small organizations, that first barrier matters a great deal, because every malicious message blocked before delivery is one fewer situation in which a user must make a difficult security judgment (Naqvi et al., 2023, p. 11; Awan and Alam, 2025, pp. 18-19). Still, filtering alone is not enough. Convincing messages can bypass automated checks, especially when attackers use compromised legitimate accounts or socially persuasive wording. Research, therefore, treats filtering as necessary but incomplete, and most effective when combined with other technical and human layers of defense (Kavvadias and Kotsilieris, 2025, p. 2; Awan and Alam, 2025, pp. 18-19, 32-33).

3.2.2 Multi-Factor Authentication

Multi-factor authentication is one of the most useful protections against the consequences of phishing. If an attacker steals a password, MFA can still prevent immediate account access by requiring a second factor such as a code, token, approval request, or biometric check. In that sense, MFA is especially valuable after the phishing email has already succeeded at the credential-theft stage (Makushova, 2025, pp. 5, 8-9; Alkhalil et al., 2021, p. 18).

Its limits should also be acknowledged. MFA can introduce friction; some implementations remain vulnerable to proxy attacks or SIM-based abuse, and users may approve requests too quickly when they are tired or distracted. Even so, it remains one of the strongest practical measures for reducing post-compromise harm in smaller organizational environments (Makushova, 2025, pp. 9-10; Grobler et al., 2021, p. 3).

3.2.3 Email Authentication Protocols (SPF, DKIM, DMARC)

SPF, DKIM, and DMARC are important because they make sender impersonation harder. In broad terms, SPF checks whether a server is authorized to send on behalf of a domain, DKIM supports message integrity through signing, and DMARC coordinates policy

decisions around failed checks. For phishing defense, these protocols matter most in attacks that rely on the false appearance of legitimacy (Awan and Alam, 2025, p. 18). Their practical value is clear, but so is their dependency on correct configuration, routine review, and consistent maintenance. They are especially useful against spoofing, yet they do not remove the need for awareness training or other layered controls. As a result, they are best treated as an important anti-spoofing layer rather than as a complete anti-phishing strategy on their own (Awan and Alam, 2025, p. 18; Naqvi et al., 2023, p. 11).

3.2.4 Software Updates and Patch Management

Patch management matters in phishing defense because the damage often escalates after the initial deception. A user may click a link or open a file, but the success of follow-up exploitation can depend heavily on whether browsers, operating systems, and applications are up to date. Awan and Alam identify outdated software and weak maintenance capacity as recurring SME weaknesses, which makes patching a practical baseline rather than an advanced luxury (Awan and Alam, 2025, pp. 16, 24). For smaller organizations, the key issue is consistency. Automated patching, prioritization of critical updates, and basic audit routines are often more realistic than relying on irregular manual updating. Patch management does not prevent users from being deceived, but it helps reduce the technical harm that may result from deception (Naqvi et al., 2023, p. 11; Alkhalil et al., 2021, p. 17).

3.2.5 Basic Network and Web Protection Measures

Basic network and web protections include firewalls, endpoint security, browser safeguards, intrusion detection, access control, and simple web filtering. These measures are especially useful once a user has interacted with suspicious content, as they can block malicious traffic, restrict lateral movement, and reduce the impact of follow-up (Awan and Alam, 2025, pp. 18-21). This aligns with Stallings (2017), who describes network security as an application of layered standards and controls rather than a search for a single perfect barrier. Their value lies in supporting a defense-in-depth model. They do not eliminate the need for careful user behavior, but they introduce technical friction later in the phishing chain. For small organizations, layered friction is often more achievable than any attempt to find a single perfect control (Naqvi et al., 2023, p. 12; Awan and Alam, 2025, p. 32).

3.3 User Cybersecurity Awareness Policies

3.3.1 Security Awareness Training

Security awareness training aims to improve how users interpret and respond to suspicious communication. In phishing defense, the goal is not to turn every employee into a security specialist. It is to create better habits: pausing, checking, verifying, and reporting. Recent research consistently treats awareness training as a core part of anti-phishing protection rather than a secondary add-on (Kavvadias and Kotsilieris, 2025, p. 5; Khan and Muntaha, 2024, pp. 1664, 1671). The quality of training matters as much as its existence. Scenario-based exercises, examples adapted to real work situations, and periodic refreshers tend to work better than generic one-time lectures. The literature therefore suggests that reinforcement over time is necessary if organizations want awareness gains to last (Alluqmani et al., 2025, p. 183; Khan and Muntaha, 2024, p. 1671).

3.3.2 Recognizing Suspicious Emails and Websites

One of the most practical awareness skills is recognizing the signals that something is wrong. These may include unfamiliar sender addresses, domain irregularities, urgent language, unexpected attachments, credential requests, or links that do not match the apparent service. Training studies show that users can improve significantly when exposed to concrete examples rather than abstract warnings (Khan and Muntaha, 2024, p. 1669). Fraudulent websites are a similar problem. Attackers increasingly imitate legitimate design and may use familiar visual elements to create a false sense of trust. Recognition, therefore, depends on checking several cues at once instead of relying only on professional appearance or one symbolic sign of legitimacy (Alkhalil et al., 2021, p. 18).

3.3.3 Reporting Policies for Suspicious Messages

Recognition is useful, but reporting turns individual caution into organizational defense. When users report a suspicious message early, the organization can warn others, quarantine similar content, block links, or investigate a broader campaign. Reporting, therefore, connects awareness with operational response (Khan and Muntaha, 2024, p. 1664; Kavvadias and Kotsilieris, 2025, p. 5). For reporting policies to work, they must be easy to follow and free from unnecessary fear. Employees should know whom to contact, how quickly to respond, and what information to provide. They should also feel safe reporting something that turns out to be harmless. That kind of supportive reporting culture tends to

strengthen resilience more than a blame-based approach (Alkhalil et al., 2021, p. 16; Khan and Muntaha, 2024, p. 1664).

3.3.4 Password Practices and Safe User Behavior

Good password behavior remains relevant because many phishing campaigns aim directly at credentials. Avoiding password reuse, enabling MFA, refusing to share passwords, and using password managers where possible all reduce the damage a successful phishing message can cause (Naqvi et al., 2023, p. 11). In a similar practical spirit, Sammons and Cross (2016) stress that everyday cyber safety depends on repeatable safe habits on both computers and mobile devices, not only on formal policy documents. Safe behavior also goes beyond passwords. Users should verify unusual requests through another channel, avoid acting too quickly under pressure, and treat the sense of urgency itself as a warning sign. Research suggests that distraction, overconfidence, stress, and routine clicking all increase phishing susceptibility, which means safer behavior depends partly on slowing down rather than simply knowing more terminology (Grobler et al., 2021, pp. 3-4; Khan and Muntaha, 2024, p. 1666; Kavvadias and Kotsilieris, 2025, p. 21).

3.3.5 Building a Security-Aware Organizational Culture

A security-aware culture helps translate policy into everyday practice. When leadership treats cybersecurity as a normal organizational responsibility, employees are more likely to take suspicious communication seriously, complete training, and report concerns early. Panteli et al. describe robust security culture, shared responsibility, and visible leadership commitment as important dimensions of responsible cybersecurity (Panteli et al., 2025, pp. 7, 14). This matters particularly in small organizations, where informal routines strongly shape daily decisions. Clear communication, executive support, and user-centered design can make security requirements feel understandable rather than burdensome. Pollini et al. argue that unclear or impractical rules are more likely to be ignored, which underscores the close connection between organizational culture and usability in phishing defense (Pollini et al., 2022, p. 374).

3.4 Combining Technical and Human Protection Measures

3.4.1 Why Technical Measures Alone Are Not Enough

Technical controls are essential, but phishing still succeeds when messages bypass filtering and reach a user who is persuaded to act. In those moments, security depends less on software's existence and more on the interaction among the message, the user, and the work context. Several studies, therefore, argue that technical controls alone cannot effectively manage phishing (Darem, 2021, p. 7944; Pollini et al., 2022, pp. 371-372). This does not make technical controls less important. It means their strengths are concentrated in certain parts of the attack chain: reducing exposure, blocking spoofing, and limiting post-click exploitation. Once the attack becomes persuasive at the user interface level, human factors become decisive. A realistic security model must acknowledge both sides simultaneously (Makushova, 2025, pp. 9-10).

3.4.2 Why Awareness Alone Is Not Enough

Awareness training also has clear limits when it stands alone. Even trained users may make mistakes when they are rushed, distracted, or presented with a particularly convincing message. In addition, training effects weaken over time if they are not reinforced. The literature, therefore, treats awareness as necessary but not self-sufficient (Gwenhure, 2025, p. 2; Alluqmani et al., 2025, p. 183). Awareness becomes stronger when technical systems reduce the number of dangerous situations users face in the first place. Training people to recognize malicious emails is useful, but it is much more effective when spoofed messages are also filtered, suspicious domains are controlled, and credential theft is limited by MFA. In that sense, awareness should complement technical protection rather than replace it (Darem, 2021, p. 7944; Makushova, 2025, p. 9).

3.4.3 The Value of a Layered Security Approach in Small Organizations

A layered approach is especially suitable for small organizations because it does not rely on a single perfect solution. Instead, it combines affordable measures that work at different stages: filtering before delivery, awareness at the point of interaction, MFA after credential capture, and patching or endpoint protection to reduce follow-on harm. That logic fits smaller environments better than any enterprise-scale expectation of total technical control (Makushova, 2025, pp. 9-10; Awan and Alam, 2025, pp. 18-20, 32-33). The main strength of a layered approach is realism. It accepts that technical systems may miss some messages

and that users may still make errors. By distributing protection across several layers, the organization becomes less dependent on flawless performance from any single tool or person. That logic appears consistently across the literature reviewed in this thesis (Pollini et al., 2022, pp. 371-372, 386; Makushova, 2025, pp. 9-10).

3.4.4 Ethical Balance Between Protection, Privacy, and Responsibility

Layered protection must also remain ethically balanced. Organizations have a duty to protect systems and users, but that duty does not justify disproportionate surveillance, opaque policy design, or blame-oriented awareness practices. Responsible cybersecurity requires measures that are effective and still respectful of user dignity and privacy (Ababneh et al., 2025, pp. 14, 20; Mersinas et al., 2025, pp. 12-13). In practical terms, this means that anti-phishing measures work better when users understand what is expected of them, why data may be logged, and how reports will be handled. Leadership responsibility matters here as much as technology. Panteli et al. argue that accountability and stewardship are central to responsible cybersecurity, which is particularly relevant in smaller organizations where trust can either strengthen or undermine daily security practice (Panteli et al., 2025, pp. 2-3, 17).

4 Practical Part

4.1 Introduction to the Selected Case

The practical part of this thesis is based on the case study by Morić et al. (2025), which examined phishing resilience in a Croatian university by combining phishing simulations with structured online education. The case was selected because it offers a documented intervention process, measurable outcomes, and a direct connection to the research question of this thesis. It is important to clearly state the scope. The case does not represent a small private organization in a strict sense, and it was not produced by the author of this thesis. Its value lies elsewhere: it provides a real organizational setting in which phishing exposure, user response, intervention type, and contextual timing can be compared. That makes it suitable for a bachelor-level practical analysis focused on interpretation and lessons for smaller organizations.

4.2 Case-Study Workflow and Analytical Setup

Figure 1 shows the practical workflow used in the case study and its interpretation in this thesis. The process began with a baseline phishing simulation, moved to an intervention split between repeated simulations and structured education, and ended with a final phishing round conducted during a pre-holiday period. The final stage is especially important because it allows a direct comparison between two intervention paths. For the purposes of this thesis, the case was reorganized into three analytical steps. First, reported participant and outcome data were extracted from each phase. Second, comparable compromise rates were calculated where the denominator was available. Third, the simulation-only path and the education path were compared in the final round, and the implications for small organizations were interpreted.

4.2.1 Reconstructed Environment and Roles

For the purposes of this thesis, the case is reconstructed as a small organizational environment with several core elements: end users, an email delivery channel, a phishing simulation process, and an organizational response layer. Even though the original case took place in a university setting, the analytical logic is relevant to smaller organizations because the same basic flow still applies. Messages reach users; users either interact or report; and the organization either resolves the issue promptly or reacts too late. In this reconstructed environment, the most important roles are the message recipient, the security or administrative function that receives reports, and the organizational leadership that determines whether awareness is treated as a recurring task or as a one-off activity. This role distribution is useful because many small organizations lack a dedicated security team. Security responsibilities are often shared between management, IT support, and ordinary employees.

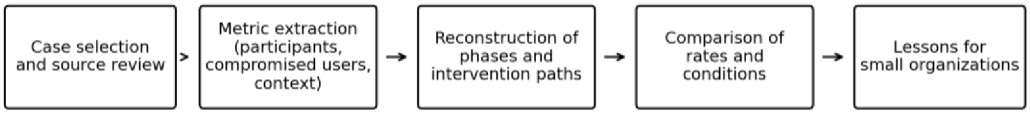

Figure 1: Reconstructed workflow of the secondary phishing case analysis used in the practical part.

Source: Processed by the author based on Morić et al, (2025).

4.2.2 Scenario Logic and Contextual Factors

A useful lesson from the case is that phishing success cannot be explained only by the message content. Context also matters. Timing, workload, expectations, and organizational routine influence how a message is interpreted. In the analyzed case, the final stage took place shortly before a holiday period, which likely increased time pressure and reduced careful inspection. This is analytically important because small organizations often experience exactly this kind of pressure during payroll periods, invoicing cycles, procurement deadlines, or holiday coverage. The case, therefore, supports a broader reading of phishing defense: a message may look technically similar across rounds, but the surrounding conditions can still change the outcome. This is one reason why static annual awareness training is weak. Users need repeated reminders, practical examples, and a reporting route that remains visible during busier work periods.

4.3 Data Collection, Metrics, and Evaluation Criteria

The practical analysis uses five variables: intervention type, number of participants, reported clicks (when available), number of compromised users, and contextual notes. The primary outcome emphasized in this thesis is the compromise rate, because it most directly reflects harmful impact within the selected case narrative. Two evaluation criteria are applied. First, a lower compromise rate is treated as a better defensive outcome. Second, results are interpreted more cautiously when contextual conditions appear to have changed, as occurred in the final pre-holiday simulation. This matters because timing and routine work pressure can influence outcomes alongside the intervention itself. Not every metric is reported for every stage in the selected source. Where a value is unavailable, it is marked as "not reported" in the tables. This limitation is treated as part of the analysis rather than something to hide, because it affects what can and cannot be concluded from secondary evidence. Within the context of the selected case, the term "compromised" is treated as the most direct indicator of harmful outcome. It is used to describe situations where the phishing interaction moved beyond mere exposure and resulted in a reported account-level or user-level security failure. This focus is deliberate. From the perspective of a small organization, operational risk becomes significant once an account is compromised, because follow-on risks such as unauthorized access, data exposure, or fraudulent actions become possible. For that reason, the analysis priorities outcome rather than only user interaction. Other indicators can be useful in phishing analysis, such as click rate (clicks/delivered messages), reporting rate (reports/delivered messages), or time-to-report. However, those measures require consistent reporting across all phases. Because the published case does not provide complete values for every stage, missing click or report data are not reconstructed. This approach avoids artificial precision and keeps the practical part aligned with what the available evidence supports.

Because participant counts differ across phases and across intervention paths, the compromise rate is used to normalize outcomes and support comparison. For example, in the baseline round, 2 compromised users out of 220 participants correspond to a compromise rate of approximately 0.9%, while final simulation values rise sharply above that baseline. Although the dataset is incomplete in some dimensions, the magnitude of change between early and late stages is large enough to justify interpretation, especially when contextual notes suggest reduced attention and higher workload in the final phase.

A cautious interpretation remains necessary because the label “compromise” can cover multiple pathways (for example, credentials submitted, unsafe actions taken, or account access achieved), and the thesis does not claim to observe the full technical chain behind each outcome. The metric is therefore treated as an outcome signal rather than a causal proof. Where differences are observed, they are discussed as plausible mechanisms in the Discussion chapter, rather than presented as confirmed causes.

Finally, the evaluation criteria are designed to reflect realistic improvement rather than perfect prevention. An intervention is treated as beneficial if it reduces the proportion of compromised users, improves organizational response readiness, or strengthens verification and reporting habits. Residual risk is expected to remain, which is why later chapters emphasize layered protection and basic governance rather than reliance on a single measure.

4.4 Results

Table 1 summarizes the extracted case-study results used in this thesis. The table focuses on the measurable information available from the documented phishing rounds and on the intervention split that became central in the final stage. Table 1. Extracted case-study results used in the practical analysis. *Calculated using the reported participant count available for the intervention phase. The first two rounds show relatively limited compromise, while the final round shows a much sharper increase. The rise is evident even before comparing the two intervention paths. This indicates that phishing susceptibility in the case was not stable across time. Conditions around the final round made the environment significantly more vulnerable. A neutral reading of the results leads to three observations. First, phishing success remained possible in every stage of the case. Second, the final round was clearly worse than the earlier ones. Third, the education path showed a more favorable outcome than the simulation-only path, but the difference was not large enough to support any claim that awareness alone provides strong protection.

*Table 1: Extracted case-study results used in the practical analysis. *Calculated using the reported participant count available for the intervention phase.*

Phase	Participants	Intervention	Clicked	Compromised	Compromise rate	Note
Round 1 baseline simulation	220	Initial phishing simulation	26	2	0.9%	Early assessment of user susceptibility
Round 2 intervention phase	237	Group split introduced	Not reported	4	1.7%*	Short-term outcome across the phase
Final simulation: Group A	117	Repeated simulations only	Not reported	39	33.3%	Pre-holiday period
Final simulation: Group B	120	Structured education path	Not reported	30	25.0%	Pre-holiday period

Source: Processed by the author based on Morić et al, (2025).

4.4.1 Results by Phase

Table 1 reports the phase-level results extracted from the documented case. The first baseline round and the intervention phase show relatively low reported compromise rates. In contrast, the final split simulation produced much worse outcomes in both intervention paths. Even without over-interpreting the incomplete dataset, the change is large enough to justify closer discussion. The value of presenting the results in this way is that it separates description from interpretation. At this stage, the thesis only records what happened in the available data: how many participants were involved, how many users were reported as compromised, what type of intervention was in place, and whether the source reported the metric directly or whether it had to be calculated from available participant counts.

4.4.2 Results by Intervention Path

Table 2 narrows the focus to the final comparison between the simulation-only and education paths. This is the clearest contrast in the practical part because both groups were exposed in the same late-stage context while receiving different forms of preparation. The education path performed better, but the difference is not large enough to justify a simplistic claim that awareness training solves the phishing problem on its own. The practical value of this comparison is that it shows improvement and limitation at the same time. That kind of result

is more realistic than a perfect success story. Small organizations usually need to know not only whether an intervention helped, but also how much residual risk remained after the intervention.

Table 2: Comparison of the two intervention paths in the final phishing simulation.

Path	Participants	Compromised	Rate	Analytical note
Simulation-only path	117	39	33.3%	Higher compromise rate in the final round
Education path	120	30	25.0%	Lower compromise rate, but still substantial vulnerability
Difference	-	9 fewer users	8.3 percentage points lower	Suggests an advantage for education, but not complete protection

Source: Processed by the author based on Morić et al (2025).

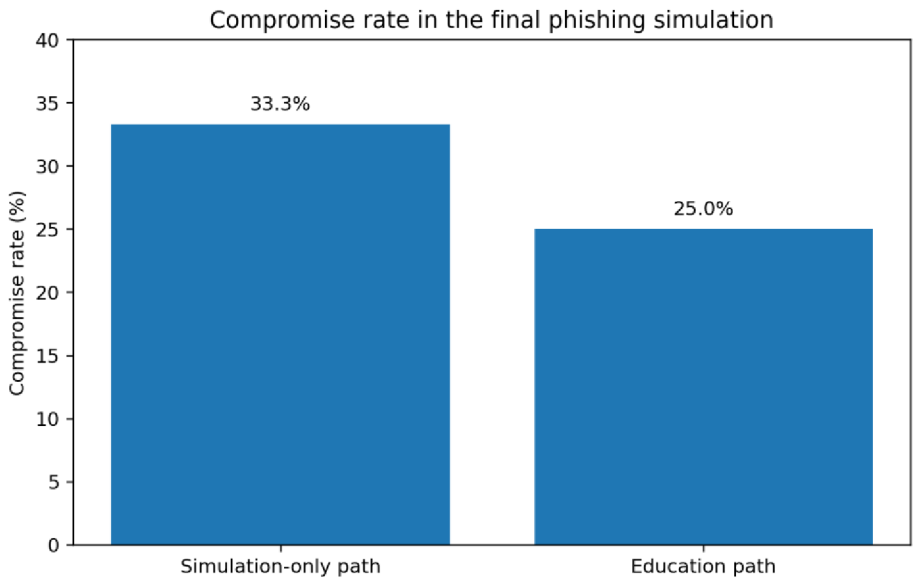

Chart 1: Compromise rate in the final phishing simulation by intervention path.

Source: Processed by the author based on Morić et al, (2025).

4.4.3 Contextual Comparison of the Analytical Phases

The case becomes easier to understand when the phases are compared not only by numbers, but also by conditions. Table 3 summarizes the main analytical contrast. The first two phases suggest relatively limited compromise, while the final phase suggests a much more

demanding context in which both intervention paths performed worse than the earlier stages. This kind of comparison is useful at the bachelor's level because it connects outcome measures with practical circumstances. It allows the thesis to move beyond simple listing and towards explanation, while still remaining transparent about the limits of the data.

Table 3: Contextual comparison of the analysis phases.

Phase	Main condition	Context	Observed pattern	Implication
Round 1	Baseline exposure	Initial measurement	Very low reported compromise	Starting point only; not enough alone
Round 2	Intervention phase	Group split begins	Still low reported compromise	Short-term improvement is still incomplete
Final stage	Different preparation paths	Pre-holiday period	Sharp increase in compromise in both groups	Context likely shaped attention and outcomes

Source: Processed by the author based on Morić et al, (2025).

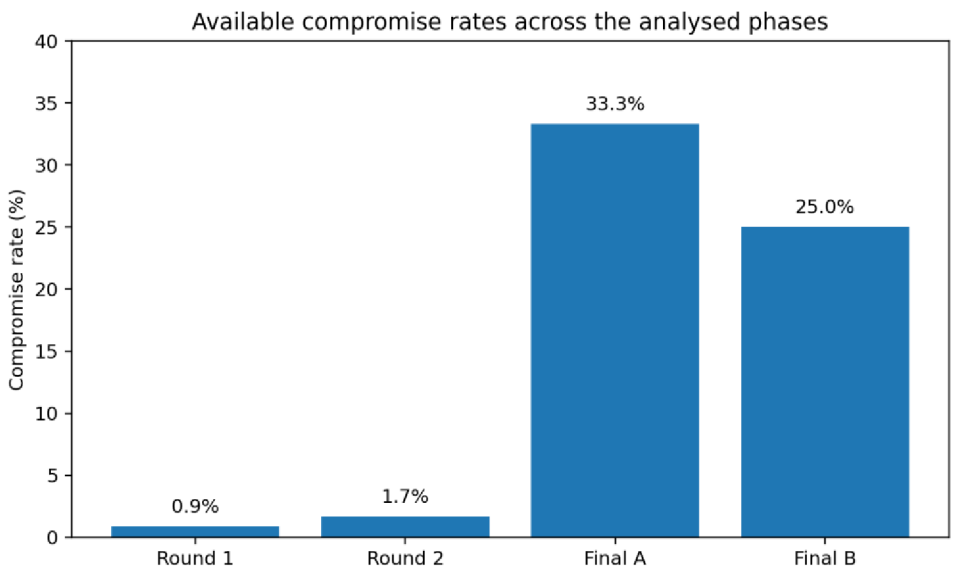

Chart 2: Available compromise rates across the analyzed phases.

Source: Processed by the author based on Morić et al. (2025).

4.5 Compare-and-Contrast Analysis

The most important comparison in the practical section is between the simulation-only path and the education path. The education path ended with a lower compromise rate in the final round, which suggests that structured awareness may have had a protective effect. At the same time, the remaining 25.0% compromise rate is too high to treat education as a sufficient response by itself. A second comparison concerns timing. Earlier stages showed relatively limited compromise, whereas the final pre-holiday stage showed a sharp deterioration. That pattern suggests that organizational context matters greatly. Users do not react to phishing in a fixed way. Pressure, routine disruptions, reduced staffing, and divided attention can substantially change outcomes. A third comparison concerns the nature of the interventions themselves. Repeated simulation without stronger educational support did not appear to create stronger resilience over time. In contrast, structured education appears to have helped somewhat, but not enough to remove the need for technical protection. This is exactly the kind of result that fits a layered interpretation better than a single-measure explanation. A more explicit comparison also helps meet the professor's requirement to clearly compare and contrast, rather than merely describe the case. Scenario A, the simulation-only path, ended with a compromise rate of 33.3%. Scenario B, the structured education path, ended with 25.0%. The difference is meaningful but not dramatic. This suggests that education improved resilience without eliminating the underlying susceptibility. The more important contrast may therefore be between the earlier and later conditions of the case. The final stage happened in a period that likely reduced careful inspection and increased routine-driven clicking. That makes the case analytically stronger because it shows that even reasonable preparation can weaken when the work context becomes less favorable. From the perspective of small organizations, the lesson is not that one intervention path wins permanently over the other. The more defensible lesson is that layered protection performs better than a narrow, single-path approach, and that organizations should prepare for fluctuations in user attention rather than assume stable behavior over time.

4.6 Contribution of the Practical Part

This practical part goes beyond a mere summary of an existing article. It converts a published case into a clearer analytical model for the thesis. Specifically, it adds a workflow figure, makes the outcome metrics explicit, separates results from discussion, calculates compromise rates, compares intervention paths directly, and translates the case into lessons tailored to small organizations. In other words, the contribution here is not the creation of new raw data, but the clearer evaluation and application of existing evidence.

5 Discussion of Results and Recommendations

5.1 Discussion of the Main Findings

The practical and theoretical parts point to the same core conclusion: phishing-related risk is reduced most effectively when technical protections and user awareness policies are implemented together. The theory chapters showed this conceptually. The case study illustrated it more concretely. No isolated intervention in the case produced anything close to complete resilience, and even the better-performing education path still left a large proportion of users vulnerable in the final stage. The results also suggest that context matters as much as intervention design. The final pre-holiday simulation appears to have created conditions in which routine was weaker and vigilance was lower. This is important because organizations sometimes treat phishing as a stable technical variable. The case indicates the opposite. Susceptibility changes with timing, attention, and local work conditions. Another important point is that repeated simulation, by itself, did not appear to produce stronger resilience. That does not make the simulation useless. It means that exposure without deeper reinforcement may have limited value. Structured education seems to offer a better direction, but the remaining compromise rate shows that awareness requires support from filtering, authentication, updates, and a reporting culture. For small organizations, this has a practical implication. They should not expect a single vendor tool, a single workshop, or a single phishing campaign to solve the problem. What they need is a modest but coherent system in which several controls compensate for one another's weaknesses. That is also why the ethical side of cybersecurity matters. Supportive communication and non-punitive reporting are not soft additions; they help create conditions in which users are more likely to act safely. One feature of the findings that stands out is how easy it would be to misread the case if the practical chapter were written only as a narrative summary. Once the evidence is reorganized into explicit metrics and comparison tables, the pattern becomes clearer: the case does not show complete success, but rather partial improvement along one path and a clear vulnerability under stressful conditions. That kind of mixed outcome is exactly what makes the case useful for a bachelor's thesis. It also seems reasonable to argue that the case indirectly supports a systems view of phishing. Users do matter, but their choices are shaped by what the organization makes easy or difficult. Clear reporting routes, stronger authentication, better filtering, and repeated reminders all influence the environment in which user decisions are made.

5.2 Practical Recommendations for Small Organizations

The first recommendation is to establish a technical baseline. At minimum, this should include spam and email filtering, properly configured SPF/DKIM/DMARC, regular patching, basic endpoint or web protection, and MFA for important accounts. These controls do not prevent every attack, but they reduce exposure and limit the impact of stolen credentials. The second recommendation is to run awareness as a continuous process. Short, repeated, scenario-based training is more realistic than one-off instruction. Small organizations should use examples that resemble the communication their employees receive, and they should reinforce reminders before higher-risk periods such as holidays, busy accounting cycles, or large administrative deadlines. The third recommendation is to create a simple reporting route. Users should know where to send suspicious emails, what constitutes suspicious activity, and that reporting uncertain cases is acceptable. Early reporting makes the organization more responsive and prevents phishing defense from remaining purely individual. The fourth recommendation is cultural. Leadership should communicate clearly that security is a shared responsibility and that reporting is encouraged rather than punished. A blame-focused approach may reduce openness precisely when fast reporting is most needed. The fifth recommendation is strategic. Small organizations should aim for resilience rather than perfect prevention. Some malicious messages will still arrive, and some users will still make mistakes. The real objective is to reduce the number of successful compromises and to contain the damage when errors happen.

5.3 Threats to Validity and Transferability

A practical thesis should also make its threats to validity visible. The most important threat here is source dependence: because the practical chapter is based on one documented case, any weakness in the original reporting affects the current analysis as well. Another threat is transferability. The organizational setting of a university differs from that of a small private firm, so the recommendations in this thesis should be treated as analytically transferable rather than statistically proven for every small organization. There is also a measurement threat. Some values that would have strengthened the analysis, especially click and report rates for every stage, were not fully available. For that reason, the thesis avoids over-claiming. It uses the numbers that can be justified and openly labels the limits of what can be concluded from them.

5.4 A Minimum Anti-Phishing Baseline for Small Organizations

To conclude the practical discussion, Table 4 proposes a minimum anti-phishing baseline for a small organization. The table does not describe an advanced security program. It describes the smallest combination of measures that still makes sense if an organization wants to reduce obvious and repeated phishing risk. This baseline is deliberately modest. The point is not to design an expensive enterprise framework, but to show what a small organization can realistically do first. In that sense, the table is one of the thesis's most practical outputs.

Table 4: Proposed minimum anti-phishing baseline for a small organization.

Area	Minimum measure	Why it matters	Realistic owner
Email security	Spam filtering + SPF/DKIM/DMARC check	Reduces obvious spoofing and suspicious delivery	IT support/service provider
Account security	MFA for important accounts	Limits damage when credentials are stolen	Management + users
Maintenance	Regular patching of devices and browsers	Reduces exploitation of known weaknesses	IT support
Awareness	Short recurring phishing reminders	Keeps recognition skills active in daily work	Management / HR / IT
Reporting	Simple mailbox or contact point for suspicious emails	Encourages early escalation and shared defence	Management / admin

Source: Processed by the author based on the literature review and Morić et al. (2025).

5.5 Limits of the Thesis

Several limitations are associated with this thesis. First, the practical part is based on a secondary case study rather than primary fieldwork conducted directly for this thesis. As a result, the analysis is dependent on the scope and reporting quality of the original study. Second, the chosen case was conducted in a university environment, not in a small private organization. Translation to smaller organizations is analytically useful, but it still requires caution. Some institutional conditions may not transfer directly. Third, the case study does not report all the metrics that would ideally be available for a stronger practical analysis. For example, clicks and reporting behavior are not fully documented for every stage. The thesis, therefore, uses transparent partial measurement rather than pretending the dataset is more complete than it is. Finally, phishing evolves quickly. The layered principles discussed here

are likely to remain relevant, but the exact tactics and delivery mechanisms used in phishing campaigns will continue to change.

6 Conclusion

In this thesis, the question of how basic technical email and network protections can be combined with user cybersecurity awareness policies to reduce phishing-related risks in small organizations was examined. The topic was approached as a practical problem rather than as a search for a perfect cybersecurity model. Emphasis was placed on how technology and user behavior can be connected within a realistic and sustainable defensive system. The literature review showed that phishing is a socio-technical threat. Technical measures such as filtering, email authentication, patching, endpoint protection, and MFA are all valuable, but none is sufficient on its own. Awareness measures such as training, suspicious email recognition, reporting rules, safer password behavior, and a supportive culture are equally necessary but incomplete when used without technical support. The practical case-study analysis reinforced that conclusion. Once the case was reorganized around explicit metrics, it became clear that phishing risk persisted across all stages, that the final pre-holiday simulation produced substantially worse outcomes, and that the education path performed better than the simulation-only path while still leaving meaningful vulnerability. The most reasonable interpretation is therefore a layered one: better protection comes from combining controls rather than choosing between them. A final contribution of this thesis is that it frames phishing protection not only as a technical task, but also as an organizational and ethical responsibility. Security becomes more sustainable when users understand why measures are in place, when reporting is encouraged without blame, and when leadership treats security as part of normal organizational practice. In conclusion, small organizations can reduce phishing-related risks in meaningful ways without needing highly complex systems. What they need most is a balanced baseline: basic technical protection, continuous awareness, simple reporting, stronger authentication, and a culture that supports responsible behavior. The strongest answer to phishing is therefore not one measure, but a coherent combination of measures working together.

7 References

ABABNEH, J., ALNEMARI, M.M., ATTAR, H., ALGHAMDI, H.A., AL-SHAWAHEEN, M., SAQARAT, B., ABU ROMMAN, L. and IQTAIT, M. (2025) 'Cybersecurity ethical aspects (CEA)', IEEE Access, 13, pp. 212443-212468. Link: https://scholar.google.com/scholar?q=Cybersecurity+ethical+aspects+%28CEA%29+Ababneh+2025

ALKHALIL, Z., HEWAGE, C., NAWAF, L. and KHAN, I. (2021) 'Phishing attacks: A recent comprehensive study and a new anatomy', Frontiers in Computer Science, 3, article 563060.
Link: https://scholar.google.com/scholar?q=Phishing+attacks%3A+A+recent+comprehensive+study+and+a+new+anatomy+Alkhalil+2021

ALLUQMANI, K., KARRAR, A.E., ALHAIDARI, M., ALHARBI, R. and ALHARBI, S. (2025) 'Assessing the efficacy of security awareness training in mitigating phishing attacks: A review', International Journal of Advanced Trends in Computer Science and Engineering, 14(3), pp. 177-184.
Link: https://scholar.google.com/scholar?q=Assessing+the+efficacy+of+security+awareness+training+in+mitigating+phishing+attacks%3A+A+review+Alluqmani+2025

AWAN, M. and ALAM, A. (2025) 'Cybersecurity threats and defensive strategies for small and medium firms: A systematic mapping study', Administrative Sciences, 15(12), article 481.
Link: https://scholar.google.com/scholar?q=Cybersecurity+threats+and+defensive+strategies+for+small+and+medium+firms%3A+A+systematic+mapping+study+Awan+2025

DAREM, A. (2021) 'Anti-phishing awareness delivery methods', Engineering, Technology & Applied Science Research, 11(6), pp. 7944-7949.
Link: https://scholar.google.com/scholar?q=Anti-phishing+awareness+delivery+methods+Darem+2021

EASTTOM, C. (2020) Computer Security Fundamentals. 4th edn. Pearson. ISBN 978-

0135774779.
Link: https://www.pearson.com/en-us/subject-catalog/p/computer-security-fundamentals/P200000000230/9780135774779

ERICKSON, J. (2008) Hacking: The Art of Exploitation. 2nd edn. No Starch Press. ISBN 978-1593271442.
Link: https://nostarch.com/hacking2.htm

GROBLER, M., GAIRE, R. and NEPAL, S. (2021) 'User, usage and usability: Redefining human centric cyber security', Frontiers in Big Data, 4, article 583723. Link: https://scholar.google.com/scholar?q=User%2C+usage+and+usability%3A+Redefining+human+centric+cyber+security+Grobler+2021

GWENHURE, A.K. (2025) 'University students' security behavior against email phishing attacks: Insights from the health belief model', Journal of Cybersecurity, article tyaf034. Link: https://scholar.google.com/scholar?q=University+students%E2%80%99+security+behavior+against+email+phishing+attacks%3A+Insights+from+the+health+belief+model+Gwenhure+2025

JAMUNA, K.M. (2024) 'Social engineering and human factors in penetration testing', International Journal for Multidisciplinary Research (IJFMR), 6(3), pp. 1-12. Link: https://scholar.google.com/scholar?q=Social+engineering+and+human+factors+in+penetration+testing+Jamuna+2024

KAVVADIAS, A. and KOTSILIERIS, T. (2025) 'Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review', Applied Sciences, 15(4), article 2236. Link: https://scholar.google.com/scholar?q=Understanding+the+role+of+demographic+and+psychological+factors+in+users%E2%80%99+susceptibility+to+phishing+emails%3A+A+review+Kavvadias+2025

KHAN, M.H. and MUNTAHA, S.T. (2024) 'Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study', World Journal of

Advanced Research and Reviews, 23(2), pp. 1663-1673. Link: https://scholar.google.com/scholar?q=Evaluating+the+effectiveness+of+cybersecurity+awareness+programs+in+reducing+phishing+attacks%3A+A+qualitative+study+Khan+2024

MAKUSHOVA, N. (2025) 'Methods of protection against phishing and online frauds', Preprints.org.
Link: https://scholar.google.com/scholar?q=Methods+of+protection+against+phishing+and+online+frauds+Makushova+2025

MEEUWISSE, R. (2017) Cybersecurity for Beginners. Cyber Simplicity Ltd. ISBN 978-1541016509.
Link: https://scholar.google.com/scholar?q=Meeuwisse+Cybersecurity+for+Beginners+2017

MERSINAS, K., BADA, M. and FURNELL, S. (2025) 'Cybersecurity behavior change: A conceptualization of ethical principles for Behavioral Interventions', Computers & Security, 148, article 104025.
Link: https://scholar.google.com/scholar?q=Cybersecurity+behavior+change%3A+A+conceptualization+of+ethical+principles+for+Behavioral+Interventions+Mersinas+2025

MORIĆ, Z., DAKIĆ, V., PLEĆAŠ, M. and OGRIZEK BIŠKUPIĆ, I. (2025) 'Evaluating end-user defensive approaches against phishing using education and simulated attacks in a Croatian university', Journal of Cybersecurity and Privacy, 5, article 38.
Link: https://scholar.google.com/scholar?q=Evaluating+end-user+defensive+approaches+against+phishing+using+education+and+simulated+attacks+in+a+Croatian+university+Mori%C4%87+2025

NAQVI, B., PEROVA, K., FAROOQ, A., MAKHDOM, I., OYEDEJI, S. and PORRAS, J. (2023) 'Mitigation strategies against the phishing attacks: A systematic literature review', Computers & Security, 132, article 103387.
Link: https://scholar.google.com/scholar?q=Mitigation+strategies+against+the+phishing+attacks%3A+A+systematic+literature+review+Naqvi+2023

PANTELI, N., NTHUBU, B.R. and MERSINAS, K. (2025) 'Being responsible in cybersecurity: A multi-layered perspective', Information Systems Frontiers. Link: https://scholar.google.com/scholar?q=Being+responsible+in+cybersecurity%3A+A+multi-layered+perspective+Panteli+2025

POLLINI, A., CALLARI, T.C., TEDESCHI, A., RUSCIO, D., SAVE, L., CHIARUGI, F. and GUERRI, D. (2022) 'Leveraging human factors in cybersecurity: An integrated methodological approach', Cognition, Technology & Work, 24, pp. 371-390. Link: https://scholar.google.com/scholar?q=Leveraging+human+factors+in+cybersecurity%3A+An+integrated+methodological+approach+Pollini+2022

SAMMONS, J. and CROSS, M. (2016) The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Syngress. ISBN 978-0124166509. Link: https://shop.elsevier.com/books/the-basics-of-cyber-safety/sammons/978-0-12-416650-9

STALLINGS, W. (2017) Network Security Essentials: Applications and Standards. 6th edn. Pearson. ISBN 978-0134527338. Link: https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials-applications-and-standards/P200000003333/9780134527338

8 List of pictures, tables, graphs and abbreviations

8.1 List of pictures

Figure 1: Reconstructed workflow of the secondary phishing case analysis used in the practical part 25

8.2 List of tables

Table 1: Extracted case-study results used in the practical analysis. *Calculated using the reported participant count available for the intervention phase 28
Table 2: Comparison of the two intervention paths in the final phishing simulation 29
Table 3: Contextual comparison of the analysed phases 30
Table 4: Proposed minimum anti-phishing baseline for a small organisation 35

8.3 List of graphs

Chart 1: Compromise rate in the final phishing simulation by intervention path 29
Chart 2: Available compromise rates across the analysed phases 30

8.4 List of abbreviations

CEA - Cybersecurity Ethical Aspects

DKIM - DomainKeys Identified Mail

DMARC - Domain-based Message Authentication, Reporting and Conformance

IEEE - Institute of Electrical and Electronics Engineers

IJFMR - International Journal for Multidisciplinary Research

ISBN - International Standard Book Number

ISO - International Organization for Standardization

IT - Information Technology

MFA - Multi-Factor Authentication

PDF - Portable Document Format

SIM - Subscriber Identity Module

SME - Small and Medium-sized Enterprise(s)

SPF - Sender Policy Framework

SPF/DKIM/DMARC - Email authentication standards used together (SPF, DKIM, DMARC)

Appendices

Appendix A: Metric Definitions and Calculation Logic

This appendix summarizes the main indicators used in the practical part. The intention is not to create a sophisticated statistical model, but to show clearly how the case-study evidence was turned into a manageable bachelor-level comparison.

Compromise rate = (number of compromised users/number of participants) x 100. This is the primary indicator used in the thesis because it could be reconstructed from the available case data more consistently than some other measures.

Difference in rate = compromise rate of path A - compromise rate of path B. In the final comparison, this shows how much lower the education-path compromise rate was than the simulation-only rate.

Not reported values were kept as 'not reported' rather than estimated. This decision was intentional. It is better for a bachelor thesis to work honestly with incomplete evidence than to fill gaps with numbers that the source did not justify.

Where context likely influenced outcomes, the thesis treats that influence interpretively rather than numerically. For example, the pre-holiday context is discussed as a plausible explanatory factor, but the thesis does not quantify its exact causal weight because the source does not provide sufficient evidence to do so.

Appendix B: Example Minimal Phishing Response Workflow for a Small organization

The following workflow is a simplified example of how a small organization could respond to a suspicious email without creating a large bureaucracy.

Step 1: The user receives a message that creates uncertainty, urgency, or unusual pressure. Instead of making a decision alone, the user stops to check the sender, link, request, and context.

Step 2: If the message still looks suspicious, the user forwards it to the designated reporting contact or mailbox. The message is not deleted immediately because the organization may still need it for review.

Step 3: The person responsible checks whether the message appears malicious, whether anyone else received it, and whether any recipient has already taken action.

Step 4: If compromise is suspected, the organization resets credentials where necessary, checks MFA status, and warns affected users. If the email appears harmless, the reporting user still receives feedback to encourage reporting.

Step 5: Short lessons from the incident are turned into a reminder or micro-training note. This closes the loop and helps the organization improve without relying only on memory or blame.