FH JOANNEUM
University of Applied Sciences

PHISHING ATTACKS TARGETING HEALTHCARE SYSTEMS: RISKS, STRATEGIES AND SOLUTIONS

A Bachelorarbeit by

NIKLIND HAXHIJA

advised by

Baptiste Alcalde, MSc PhD

and submitted to the

Institute for eHealth

of the

Graz University of Applied Sciences

in partial fulfillment of the
requirements for the degree of a

Bachelor of Science (BSc)

This work is dedicated to my parents, for always having my back, supporting me unconditionally and inspiring me to reach for my goals.
I also extend my deepest gratitude to all those working in the healthcare sector, from doctors and nurses on the front lines to IT support, supply chain teams and every staff member, whose tireless efforts, especially during crises like COVID-19, keep communities safe and cared for.

Acknowledgements

First and foremost, I would like to thank my supervisor, Baptiste Alcalde, MSc, PhD, for his expert guidance, constructive feedback and encouragement through every stage of this project.
I am also grateful to the professors of the eHealth department at FH Joanneum, whose rigorous teaching and practical insights laid the foundation for my studies and this research.
Finally, I thank all the authors and researchers whose work laid the groundwork for this thesis; their scholarship has been invaluable, and any errors or omissions remain my responsibility.

Graz, July 2025 Niklind Haxhija

Abstract

Increasing digitalization within the healthcare industry could bring advantages in terms of networking and efficiency, but at the same time, could pose threats to the security of confidential patient data. Phishing attacks, above all, are one of the most common and dangerous threats to IT systems within the healthcare industry. This bachelor thesis will analyze the specific threats of phishing attacks on healthcare systems systematically as well as identify and propose relevant prevention and response measures.
The research question is: How can healthcare systems be effectively protected from phishing attacks, and what are the most useful technological, organizational and human steps to reduce the risks? In order to identify this, technological protective steps such as firewalls and multifactor authentication and organizational and human factors including training and awareness-raising measures will be reviewed.
The research process includes case studies that are analyzed to identify typical attack patterns and the effectiveness of existing countermeasures. Special focus will be given to analyzing actual phishing attacks in the healthcare industry, for instance, the Magellan Health attack.
Combining theoretical frameworks with empirical insights, this thesis formulates policy recommendations that improve IT security in healthcare by systematically addressing human-factor weaknesses, including phishing susceptibility, insufficient training, and inconsistent adherence to security procedures.

Kurzfassung

Die zunehmende Digitalisierung im Gesundheitswesen kann Vorteile in Bezug auf Vernetzung und Effizienz mit sich bringen, gleichzeitig aber auch Risiken für die Sicherheit vertraulicher Patientendaten darstellen. Phishing-Angriffe gehören dabei zu den häufigsten und gefährlichsten Bedrohungen für IT-Systeme im Gesundheitsbereich. Diese Bachelorarbeit analysiert systematisch die spezifischen Gefahren von Phishing-Angriffen auf Gesundheitssysteme und identifiziert sowie entwickelt relevante Präventions- und Reaktionsmaßnahmen.

Die Forschungsfrage ist: Wie können Gesundheitssysteme effektiv vor Phishing-Angriffen geschützt werden und welche technologischen, organisatorischen und menschlichen Schritte sind dabei am hilfreichsten, um Risiken zu verringern? Zur Beantwortung dieser Frage werden technologische Schutzmaßnahmen wie Firewalls und multifaktorielle Authentifizierung sowie organisatorische und menschliche Faktoren wie Schulungen und Sensibilisierungsmaßnahmen betrachtet.

Der Forschungsprozess umfasst die Analyse von Fallstudien, um typische Angriffsmuster und die Wirksamkeit bestehender Gegenmaßnahmen zu identifizieren. Ein besonderer Fokus liegt auf der Untersuchung realer Phishing-Angriffe im Gesundheitswesen, wie etwa dem Angriff auf Magellan Health.

Durch die Kombination theoretischer Rahmenkonzepte mit empirischen Erkenntnissen entwickelt diese Arbeit Handlungsempfehlungen zur Verbesserung der IT-Sicherheit im Gesundheitswesen, indem systematisch menschlich bedingte Schwachstellen adressiert werden, darunter Phishing-Anfälligkeit, unzureichende Schulungen und inkonsistente Einhaltung von Sicherheitsprozessen.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Context

The healthcare industry has undergone a profound transformation with the adoption of digital technologies [Alotaibi, Y. K. and Federico, F., 2017]. Innovations, such as electronic health records (EHRs), telemedicine, and AI-driven diagnostics, have revolutionized patient management by improving diagnostic accuracy, enabling real-time data sharing, and facilitating remote care. These developments have markedly increased both the efficiency and effectiveness of healthcare delivery. As further emphasized by [Alotaibi, Y. K. and Federico, F., 2017], "The impact of health information technology on patient safety is profound, enhancing the quality of care and reducing medical errors".

However, this digital shift has introduced serious cybersecurity challenges. Healthcare organizations, which handle highly sensitive data, have become prime targets for cyberattacks. Phishing, in particular, exploits human error, outdated software, and procedural gaps to exfiltrate data, disrupt operations, and endanger patient safety. As Kruse et al. note, "Cybersecurity in healthcare is a growing concern, with phishing attacks among the most prevalent and dangerous threats" [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Phishing uses deceptive emails, spoofed websites, and malicious links to induce individuals to disclose confidential information or grant unauthorized access. By exploiting emotions, such as fear or urgency, it prompts victims to act without verification. "Social engineering attacks, including phishing, are a significant threat to the healthcare and public health sector" [U.S. Department of Health and Human Services, 2022], and as Schneier observes, these tactics rely heavily on psychological manipulation [Schneier, 2015].

Successful phishing attacks can have severe consequences in healthcare: data breaches, operational downtime, financial losses, regulatory fines, and erosion of public trust. For example, the Magellan Health breach resulted in the exposure of over 364 000 patient

records and significant service disruptions [HIPAA Journal, 2020a]. These incidents underscore the urgent need for robust, multi-layered cybersecurity defenses.
Given these high stakes, it is crucial for healthcare organizations to implement strong cybersecurity defenses. Protecting sensitive patient data and ensuring the smooth operation of healthcare services require a comprehensive approach. This includes technological solutions like firewalls and multifactor authentication, as well as organizational policies and training programs to raise awareness and reduce risks. [Herzig, 2013] emphasizes the importance of a multi-layered approach to cybersecurity in healthcare, combining technology, policies, and human factors to mitigate risks.
This thesis aims to analyze the specific threats posed by phishing attacks on healthcare systems and develop relevant prevention and response measures to mitigate these risks.

1.2 Research Questions

- **Main research question: How can healthcare systems be effectively protected against phishing attacks, and which technological, organizational, and human strategies best minimize these risks?**
- Sub-questions:
  - Which specific vulnerabilities make healthcare systems particularly susceptible to phishing attacks?
  - What are the impacts of successful phishing attacks on patient data security and healthcare operations?
  - How can training and awareness programs prevent phishing attacks within the healthcare sector?

1.3 Research Objectives

The primary objective of this thesis is to systematically analyze the specific threats posed by phishing attacks on healthcare systems and develop effective prevention and response measures. This research aims to provide a comprehensive understanding of the vulnerabilities within healthcare IT infrastructures and the impact of phishing attacks on patient data security and healthcare operations.
To achieve this primary objective, the thesis will focus on the following specific goals:

1. **Identify Vulnerabilities:** Examine weaknesses in healthcare IT systems, such as outdated software, inadequate protocols, and human factors, that facilitate phishing attacks.

2. **Analyze Attack Patterns:** Investigate common phishing tactics targeting healthcare, using case studies (e.g., Magellan Health [HIPAA Journal, 2020a]) to illustrate attacker methods.

3. **Evaluate Existing Countermeasures:** Assess the effectiveness of technical solutions (e.g., firewalls, MFA), organizational policies, and training programs in mitigating phishing risks [Herzig, 2013].

4. **Develop Prevention Strategies:** Propose integrated measures addressing technology, processes, and human factors for robust phishing defense.

5. **Formulate Response Plans:** Outline incident-response procedures, detection, containment, and recovery, to limit the impact of phishing breaches.

By achieving these objectives, this thesis aims to contribute valuable insights and practical recommendations to enhance the cybersecurity resilience of healthcare systems. The findings will help healthcare organizations better protect sensitive patient data and ensure the continuity of their operations in the face of evolving cyber threats.
The scope of this thesis encompasses a comprehensive analysis of phishing attacks targeting healthcare systems, with a focus on identifying vulnerabilities and developing effective countermeasures. Given the increasing digitization in healthcare, this thesis aims to explore the multifaceted nature of phishing threats and their impact on patient data security and healthcare operations.
The research will delve into the historical evolution of phishing attacks, examining how these threats have adapted to exploit technological advancements in healthcare. As [Alotaibi, Y. K. and Federico, F., 2017] highlight, "the impact of health information technology on patient safety" is profound, necessitating robust cybersecurity measures. This thesis will investigate contemporary phishing techniques, as discussed by [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017], who provide a systematic review of modern threats and trends in healthcare cybersecurity.
A comparative analysis will be conducted to understand how phishing impacts healthcare relative to other industries, identifying specific vulnerabilities unique to healthcare systems. Case studies, such as those presented by [U.S. Department of Health and Human Services, 2022], will offer practical insights into real-world phishing incidents and the effectiveness of existing countermeasures.

Furthermore, the thesis will review global guidelines for phishing mitigation, drawing on recommendations from cybersecurity bodies like [Amoroso, 2012] emphasizes, protecting national infrastructure from cyber-attacks is crucial, and this principle extends to safeguarding healthcare systems.
By examining emerging trends and future directions in phishing and cybersecurity, this thesis aims to provide actionable recommendations for healthcare organizations to enhance their defenses against phishing attacks. The scope of this thesis is thus defined by its focus on technological, organizational, and human factors in mitigating phishing risks in healthcare.

1.4 Methodology Overview

This thesis employs a mixed-methods approach:

- **Systematic Literature Review:** Following the PRISMA framework, sources from databases (PubMed, IEEE Xplore) and industry reports were analyzed to identify phishing threats and defenses.
- **Case-Study Analysis:** Real-world incidents (e.g., the Magellan Health breach) were examined to uncover attack patterns and assess the effectiveness of existing countermeasures.

Chapter 2

Understanding the Threat

2.1 The Evolution of Phishing Attacks

Phishing dates back to the mid 1990s, when attackers targeted AOL users with fake support emails. Attackers impersonated customer-support representatives to deceive users into revealing log-in credentials. These emails were generic, poorly written, and easily identifiable by their lack of personalization [Amoroso, 2012].

As internet usage became widespread and organizations relied on digital communication, phishing tactics evolved. The early 2000s saw a shift toward messages that closely mimicked the branding, tone, and formatting of legitimate institutions. These messages impersonated banks, payment services, or IT departments, embedding malicious links that pointed to spoofed websites. This evolution marked the beginning of highly organized, profit-driven phishing campaigns, establishing phishing as a preferred vector for quick financial returns [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

A major development was the emergence of spear-phishing. Unlike generic attempts, spear-phishing targets a specific individual or organization using contextual and personalized information, such as the role of the recipient, references to colleagues, or ongoing projects. Because of this customization, these attacks are far harder for standard spam filters and basic awareness training to catch [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

As illustrated in Figure 2.1, this chronological shift from crude AOL scams to highly personalized, AI-assisted deception, shows how phishing tactics have steadily matured in parallel with wider Internet adoption.

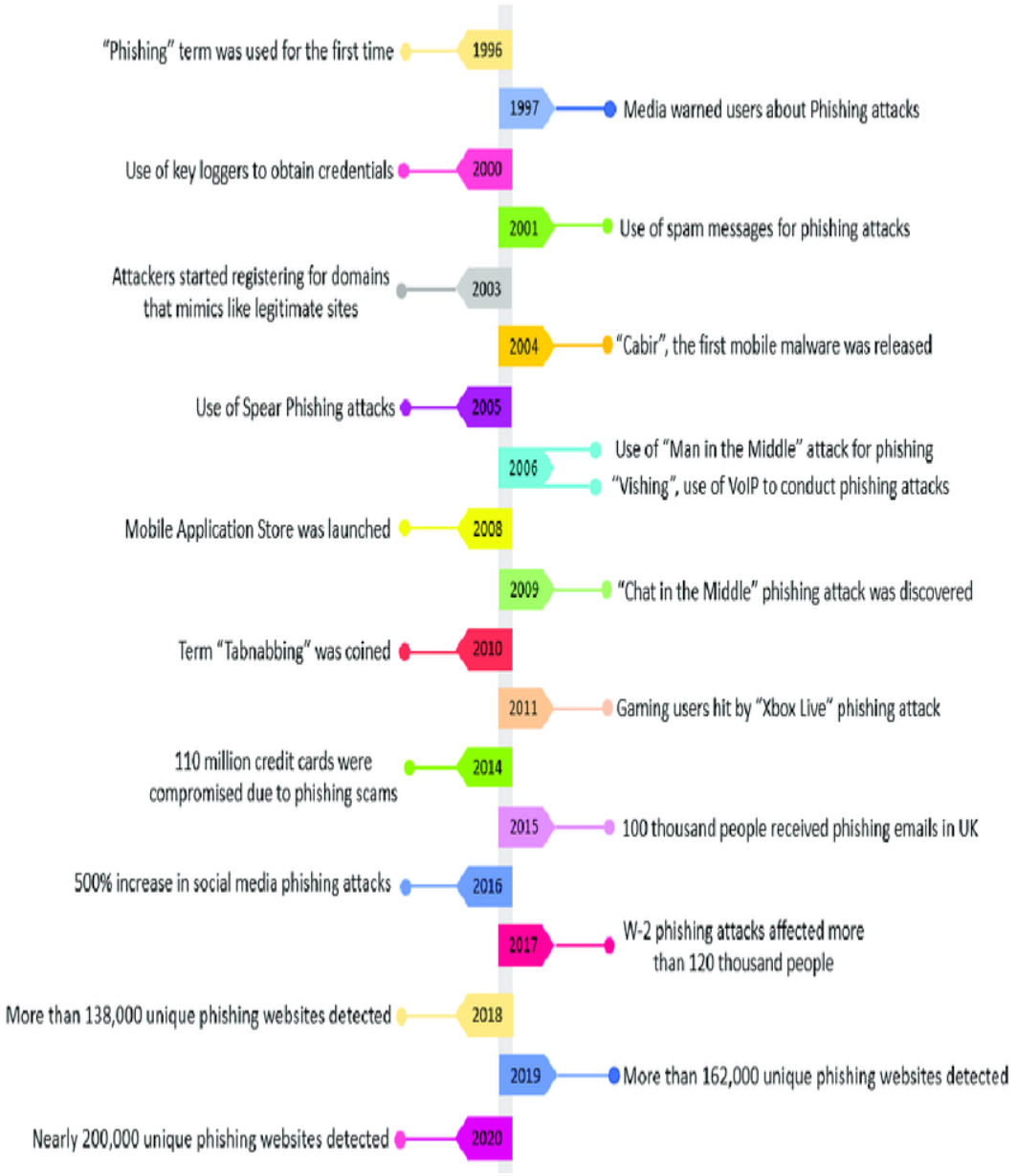

Figure 2.1: Timeline of the evolution of phishing attack techniques [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Machine learning and natural-language processing now let attackers craft highly convincing, personalized phishing emails that mimic the tone and wording of trusted brands. These emails are grammatically flawless, context-aware, and thus far more difficult for users and filters to detect [U.S. Department of Health and Human Services, 2023].
Commercial 'phishing-as-a-service' platforms on the dark web provide ready-made templates, spoofed domains, fake log-in pages and even customer support for novice attackers, lowering technical barriers to entry and driving a year-on-year rise in phishing incidents worldwide across all sectors; some vendors even offer subscription-based money-back guarantees [U.S. Department of Health and Human Services, 2023].
Modern phishing kits automate mass mailings, track clicks, redirect victims by device and include multi-language payloads, turning what was once an amateur pastime into a highly organized, service-driven criminal enterprise [FRSecure, 2021].
Researchers warn that AI-enabled campaigns will soon learn from failed attempts and refine their wording in real time, posing a formidable challenge even for advanced defense systems [U.S. Department of Health and Human Services, 2023].

2.2 Why is Healthcare a Target

Healthcare is a prime phishing target, thanks to its complex workflows and highly sensitive data. Medical records typically include not just personal identification details, but also clinical histories, diagnoses, and billing information. IBM's 2024 Cost of a Data Breach Report shows healthcare has had the highest average breach cost for 12 consecutive years [IBM, 2024b].
Another factor is the operational urgency inherent to healthcare. Clinicians often need to make rapid decisions, especially in emergency departments, which makes them less likely to scrutinize the authenticity of emails requesting information or login credentials [Amoroso, 2012]. Hospitals and small clinics may also operate with outdated IT infrastructure due to budget constraints, which limits their ability to implement modern cybersecurity measures [Amoroso, 2012].
The healthcare sector's vulnerability is further exacerbated by the high value of protected health information (PHI) on the dark web. Criminals value PHI at \$250 – \$363 per record, over 100× the price of a single credit-card number, compared to just \$1 – \$2 for credit card data, making it a highly attractive target for cybercriminals [Imprivata, 2023]. Additionally, the integration of Internet-of-Things (IoT) devices in healthcare, such as pacemakers and infusion pumps, introduces new attack vectors, which lack strong security measures to exploitation [Amoroso, 2012].

Moreover, the human factor plays a significant role in the susceptibility of healthcare organizations to phishing attacks. Employees, including administrative staff and medical professionals, may inadvertently expose sensitive information or fall victim to phishing emails, further increasing the risk of data breaches [FRSecure, 2021]. The lack of comprehensive cybersecurity training programs in many healthcare institutions contributes to this issue.

The COVID-19 pandemic has also amplified the threat landscape. The rapid shift to telehealth services and remote work environments expanded the attack surface for cybercriminals. Phishing campaigns exploiting pandemic-related fears and uncertainties have surged, targeting both healthcare providers and patients [U.S. Department of Health and Human Services, 2023].

In summary, the healthcare sector's combination of valuable data, operational urgency, outdated infrastructure, and human vulnerabilities makes it a prime target for phishing attacks.

2.3 Common Phishing Techniques Used in Healthcare

Phishing campaigns targeting healthcare institutions exploit a variety of methods. These techniques differ in terms of delivery channels, level of personalization, and technological sophistication, but all aim to deceive healthcare staff into revealing sensitive information or enabling unauthorized access to internal systems.

- **Email-phishing:** This remains the most widespread method of attack. Messages typically mimic legitimate communications, such as HR updates, billing requests, or IT service alerts. Attackers use logos, formatting, and sender spoofing to enhance credibility. These emails often contain malicious links or attachments that install malware or lead users to credential-harvesting sites [FRSecure, 2021].

- **Spear-phishing:** Unlike general email phishing, spear-phishing is highly targeted. Attackers craft messages directed at specific individuals within a healthcare organization, such as executives, IT staff, or medical personnel, using information gathered from public sources like LinkedIn or organizational websites [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

- **Smishing and Vishing:** These refer to phishing attempts conducted via SMS (smishing) and voice calls (vishing). Healthcare workers who regularly use mobile devices for scheduling or emergency response are especially vulnerable. Smishing

messages often include shortened URLs or urgent requests, while vishing calls may impersonate help desks or insurance providers to collect access credentials [FRSecure, 2021].

- **AI-generated phishing:** The use of generative language models has introduced a new wave of phishing emails that are contextually relevant, grammatically correct, and highly convincing. They can impersonate trusted contacts and adapt in real time, outpacing many detection systems. AI-generated attacks are expected to increase in frequency and sophistication [U.S. Department of Health and Human Services, 2023; TechTarget, 2024].

- **Quishing (QR-code phishing):** Attackers embed malicious URLs in QR codes posted on noticeboards, ID badges or appointment slips. When a staff member scans the code, the link silently opens a spoofed patient-portal log-in page or forces a credential prompt that exfiltrates passwords. Recent industry reports show a 51% year-on-year rise in QR-based phishing attempts across hospitals and outpatient clinics [Malwarebytes, 2024; Cloudflare, 2024].

To further illustrate the distinct characteristics of each phishing technique, Table 2.1 provides a comparative overview based on key evaluation criteria including channel, personalization level, common targets, and detection difficulty.

Table 2.1: Comparison of phishing techniques in healthcare.

Technique	**Delivery**	**Personalization Lvl.**	**Target**	**Detection Difficulty**
Email phishing	Email	Low to Medium	General staff	Medium
Spear-phishing	Email	High	Executives, IT, clinicians	High
Smishing/Vishing	SMS / Voice call	Medium	Mobile-dependent staff	High
AI-generated phishing	Email	Very High	All staff levels	Very High
Quishing	Posters / Screens	Low to Medium	Patients, mobile staff	Medium to High

Phishing methods are combined in multi-stage campaigns that exploit both technical flaws and human behavior, such as following an email with a phone call to reinforce the deception.

2.4 Notable Case Studies

Phishing attacks have led to some of the most disruptive and costly cybersecurity incidents in healthcare. The following case studies highlight the scale and consequences of such breaches.

2.4.1 Magellan Health (2020)

In April 2020, Magellan Health was targeted by a sophisticated phishing campaign. An employee clicked a spear-phishing link and inadvertently installed malware, allowing attackers to install malware and exfiltrate sensitive data. The breach affected more than 364,800 individuals, exposing names, Social Security numbers, health insurance information, and treatment details [HIPAA Journal, 2020a].

2.4.2 Universal Health Services (2020)

Universal Health Services (UHS), operating over 400 healthcare facilities, experienced a ransomware attack in September 2020 initiated via phishing. The incident led to a three-week shutdown of electronic health records (EHR) systems, causing patient diversions and manual record-keeping. UHS reported a financial impact of $67 million due to recovery efforts and lost revenue [TechTarget, 2024].

2.4.3 Elara Caring (2020)

Elara Caring, a US home-based healthcare provider, detected a phishing campaign in December 2020 that gave an intruder access to several employee email accounts. Investigators concluded that the attacker could have viewed protected health information (PHI) for 100,487 patients (including names, dates of birth, Social Security numbers and insurance details) over a seven-day window. The case shows how the compromise of just a few mailboxes can expose large volumes of PHI and underscores the need for multi-factor authentication and rapid email log monitoring [HIPAA Journal, 2021b].

2.4.4 Roper St. Francis Healthcare (2020)

In October 2020, Roper St. Francis Healthcare experienced a phishing attack that compromised the personal and health information of approximately 190,000 individuals. The breach led to a class-action lawsuit and a $1.5 million settlement to compensate affected patients [HIPAA Journal, 2021a].

2.4.5 Brno University Hospital (2020)

Brno University Hospital in the Czech Republic was hit by a cyberattack in March 2020, forcing the hospital to shut down its IT systems. While specific details are scarce [Wired, 2020], the attack disrupted critical operations, including surgeries and laboratory tests, highlighting the vulnerability of healthcare institutions to phishing-related breaches during the COVID-19 pandemic [Wired, 2020].

2.4.6 University of Vermont Health Network (2020)

In October 2020, the University of Vermont Health Network suffered a ransom-ware attack believed to have originated from a phishing email. The attack disrupted services across multiple hospitals, leading to delayed treatments and appointments. Recovery efforts spanned several weeks, with major delays in radiology and elective care, emphasizing the operational impact of such incidents [HIPAA Journal, 2020b].

2.4.7 Finnish Psychotherapy Center Vastaamo (2020)

Vastaamo, a Finnish psychotherapy center, faced a data breach in 2020 when attackers accessed patient records through phishing tactics. Sensitive therapy session notes and other information of thousands of patients were stolen and later leaked online, causing significant distress and leading to the company's bankruptcy on 18 February of 2021 [Wired, 2021].

The concentration of documented phishing incidents from the year 2020 is not coincidental. During the COVID-19 pandemic, healthcare systems were under immense pressure, and the rapid digital transformation, including the adoption of telehealth and remote work, exposed new vulnerabilities. This created an ideal environment for phishing attacks, as cybercriminals exploited confusion, urgency, and weakened IT infrastructures. Consequently, 2020 became one of the most heavily analyzed years for cybersecurity breaches in the healthcare sector, and many public case reports and academic studies still focus on that period [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D.

K., 2017; U.S. Department of Health and Human Services, 2022]. More recent incidents are often underreported or delayed due to ongoing investigations and privacy concerns. As shown in Figure 2.2, phishing topped every other attack vector as the leading cause of reported healthcare data-breach incidents in 2020 and every other year after that, except 2025 for which we don't really have reliable data yet.

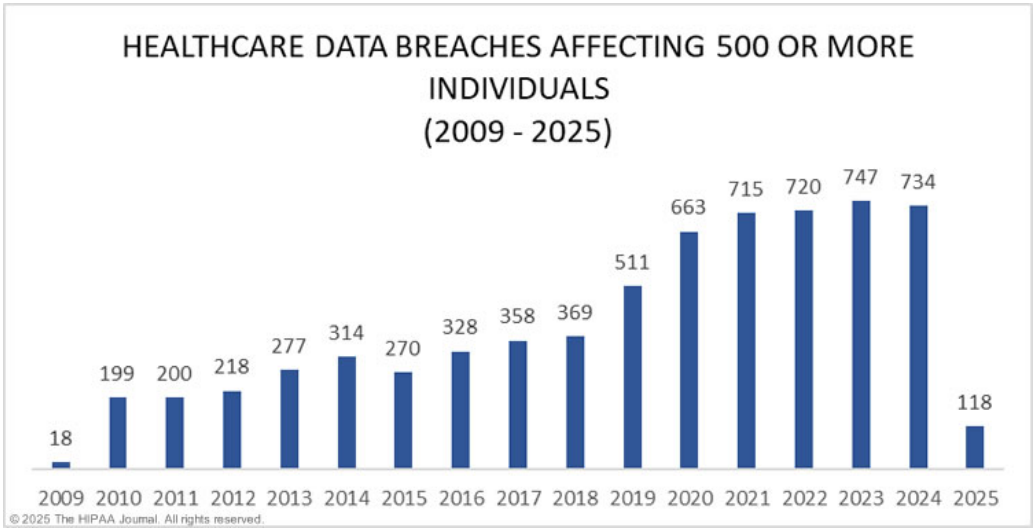

Figure 2.2: Causes of healthcare data breaches, with phishing as a leading vector [HIPAA Journal, 2024].

2.5 Comparative Industry Analysis

The healthcare sector consistently experiences the highest financial impact from data breaches across all industries. According to IBM's 2024 Cost of a Data Breach Report, the average cost of a healthcare breach reached $9.77 million, compared to the global average of $4.88 million [IBM, 2024a]. This represents a substantially higher impact than in the finance sector, where the average breach cost stands at $6.08 million [Wealth & Finance International, 2024].
While the healthcare industry is particularly exposed due to legacy infrastructure, understaffed IT departments, and strict data privacy regulations such as HIPAA and GDPR, other industries also face distinct challenges.

- **Industry sector:** Manufacturing and industrial sectors are increasingly targeted by cyberattacks due to their reliance on interconnected systems and automation. Data breaches can disrupt production lines, leading to significant financial losses

and operational downtime. The complexity of industrial control systems (ICS) and the integration of IoT devices further exacerbate vulnerabilities [IBM, 2024b].

- **Energy sector:** The energy sector faces unique cybersecurity challenges due to its critical infrastructure and the convergence of IT and operational technology (OT) networks. Cyberattacks can lead to widespread disruptions in energy supply, affecting national security and economic stability. The sector's reliance on third-party vendors also introduces significant risks [Resecurity, 2025; SecurityScorecard, 2024].

- **Pharmaceutical sector:** Pharmaceutical companies are prime targets for cyberattacks due to their valuable intellectual property and sensitive patient data. Breaches can compromise clinical trial results, proprietary research, and regulatory filings, leading to significant financial and damage to reputation. The extensive supply chains in the pharmaceutical industry also present multiple entry points for cybercriminals [Pharmaceutical Technology, 2021; Supply Chain Magazine, 2024].

- **Finance sector:** Although highly targeted, financial institutions often demonstrate a higher level of cybersecurity maturity. Their investment in layered defenses, endpoint detection, incident response automation, and threat intelligence contributes to relatively lower breach costs and shorter containment times [IBM, 2024b; Hartman Executive Advisors, 2021].

- **Healthcare sector:** The combination of outdated systems, fragmented networks, high-pressure workflows, and the critical nature of patient services make healthcare uniquely susceptible. Breaches in this industry not only incur high monetary losses but can also impact patient safety and erode public trust [IBM, 2024b].

- **Education sector:** Educational institutions encounter similar phishing threats but typically operate with fewer regulatory constraints and budgetary resources. They often lack dedicated security teams, resulting in longer detection and response times and increased vulnerability to social engineering attacks. The education sector faces significant financial and operational risks from cyber threats, including ransomware and phishing attacks, which disrupt learning environments and compromise sensitive student data [Blackbaud, 2025].

- **Retail sector:** Retail businesses are frequently targeted by cybercriminals due to the vast amount of customer data they handle. Data breaches can lead to significant financial losses, reputational damage, and legal consequences. The retail sector must

invest in robust cybersecurity measures to protect against threats such as payment card fraud and identity theft [Blackkite, 2025].

- **Logistics sector:** The logistics industry faces cybersecurity challenges due to its reliance on interconnected systems for supply chain management. Data breaches can disrupt operations, leading to delays and increased costs. The sector must address vulnerabilities in its digital infrastructure to ensure the security of sensitive shipment and customer data [Blackkite, 2025].

Figure 2.3 visualizes these cross-industry differences. These differences reflect not only the sensitivity and volume of healthcare data but also the operational and regulatory complexity within the sector.

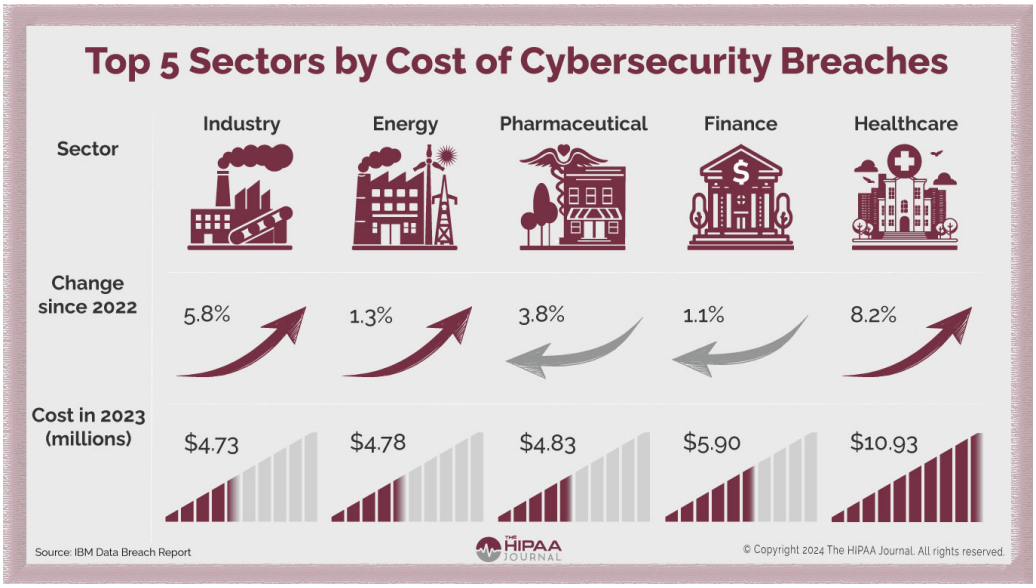

Figure 2.3: Average cost of data breaches by industry in 2024 [IBM, 2024b].

2.6 Current Trends and Emerging Threats

Several recent developments indicate a shift in phishing tactics and targets:

- **Quishing (QR phishing):** Phishing messages embedded in QR codes, often disguised as visitor check-ins or equipment registration links. These bypass traditional link scanners and exploit the growing reliance on QR codes for various services. Quishing attacks have become increasingly prevalent, with cybercriminals creating malicious QR codes that, when scanned, lead to fraudulent websites or prompt downloads of harmful software [Malwarebytes, 2024; Cloudflare, 2024].

- **Deepfake impersonation:** AI-generated voice or video is increasingly used to simulate trusted colleagues or executives in phishing attacks, like the 2019 case in which a German CEO's voice was cloned to deceive a UK manager into sending $243,000, posing a serious risk of identity-based fraud and financial loss [Damiani, 2019; Europol, 2022].

- **Supply chain compromise:** Vendors with inadequate security protocols become points of entry into larger healthcare networks. Cyberattacks targeting the supply chain can cause severe disruptions to patient care, as they often lead to delays in receiving vital medical supplies or test results. These breaches have a ripple effect across the healthcare sector, impacting patient outcomes and increasing mortality rates [Cyber Magazine, 2024; Supply Chain Magazine, 2024].

These emerging threats highlight the evolving nature of phishing attacks and the need for adaptive security strategies. The healthcare sector, in particular, must remain vigilant and proactive in implementing robust cybersecurity measures to mitigate these risks. As phishing tactics become more sophisticated, healthcare organizations must invest in advanced threat detection and response systems, employee training, and collaboration with cybersecurity experts to safeguard sensitive patient information and maintain operational integrity.

The rise of quishing, deepfake impersonation, and supply chain compromise underscores the importance of a multi-layered security approach. By understanding and addressing these threats, healthcare providers can better protect their networks and ensure the safety and privacy of their patients. Continuous monitoring, regular security assessments, and the adoption of best practices in cybersecurity are essential to staying ahead of these evolving threats.

Chapter 3

Countermeasures and Security Strategies

3.1 Technological Defenses

Technological defenses are a critical component in combating phishing attacks within healthcare. Email filtering systems have evolved significantly, moving beyond basic keyword detection to incorporate machine-learning (ML) and artificial-intelligence (AI) to detect anomalies in message structure, sender metadata, and embedded URLs [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017]. Organizations using AI-based threat detection reduced breach life cycles by up to 28% compared with those relying on traditional methods, according to IBM's 2024 X-Force Threat Intelligence Index [IBM Security, 2024]. An overview of these mechanisms is shown in Figure 3.1.

Multi-factor authentication (MFA) remains one of the most effective strategies against credential-based phishing attacks. MFA requires users to provide additional verification, such as biometric data or a one-time password (OTP), significantly complicating an attacker's efforts to compromise accounts even when initial credentials are leaked. A report by Microsoft highlights that MFA can block over 99% of automated phishing attempts [Microsoft, 2023].

Endpoint Detection and Response (EDR) solutions strengthen defenses by continuously monitoring endpoint devices for suspicious activity. In healthcare, where endpoints range from administrative laptops to imaging systems, EDR platforms delivers early-warning alerts, enabling security teams to isolate the initial compromised device before attackers pivot from it to other internal systems, a tactic known as lateral movement [Amoroso, 2012]. Properly tuned EDR platforms also flag phishing-related payloads, such as malware embedded in document attachments, in real time.

Another technological best practice is network segmentation. By dividing networks into isolated zones, healthcare organizations can limit the movement of malicious actors who manage to infiltrate the perimeter. For example, patient record databases can be isolated from email servers, reducing the risk of wide-scale data exfiltration after a phishing attack [European Union Agency for Cybersecurity, 2023]. The National Institute of Standards and Technology (NIST) likewise lists network segmentation as a "multi-layered defense" in critical-infrastructure sectors, including healthcare [National Institute of Standards and Technology, 2020].

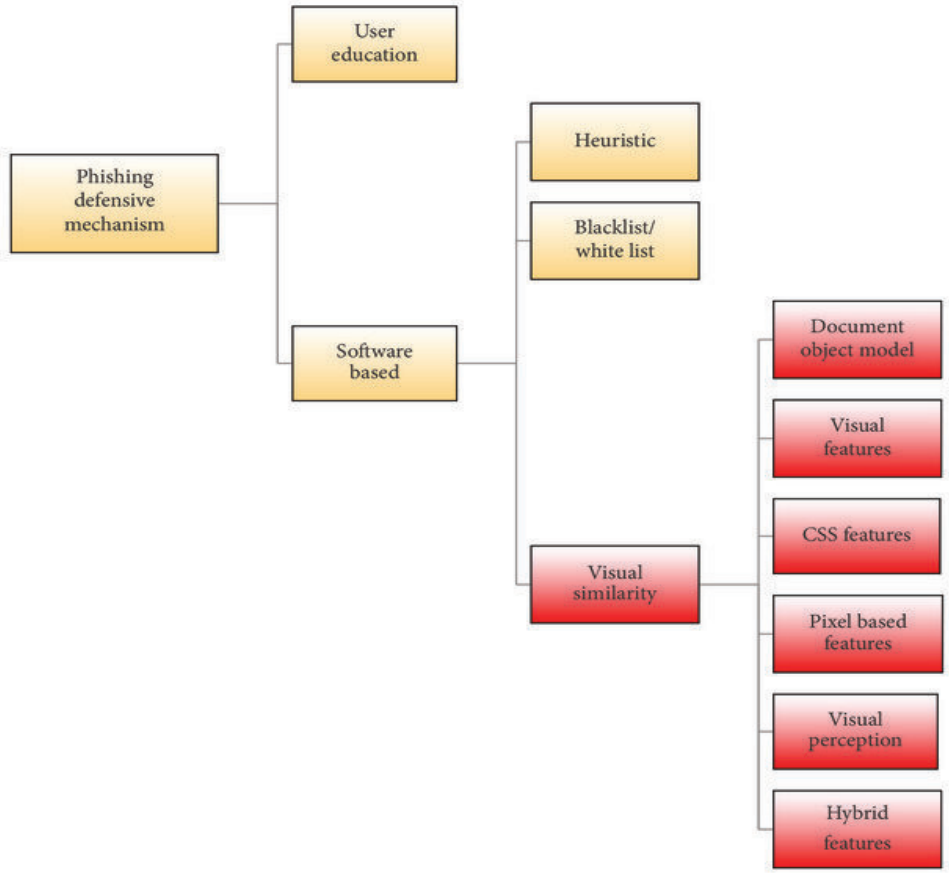

Figure 3.1: Overview of phishing defensive mechanisms, user education, heuristic methods, and software-based solutions [Jain, Ankit Kumar and Gupta, B. B., 2017].

However, while technological tools are indispensable, they are not foolproof. Attackers are increasingly adapting phishing campaigns to bypass advanced filters by mimicking trusted vendors and embedding phishing links into cloud services like OneDrive [TechTarget, 2024]. This underscores the need for a layered defense approach, combining technological, organizational, and human-centered measures to effectively mitigate phishing risks.

3.2 Organizational Measures

While technological solutions are critical for the initial defense perimeter, organizational measures are equally important for building a resilient posture against phishing in healthcare [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017]. Proper governance, clear communication protocols and continuous-improvement cycles help mitigate human and procedural vulnerabilities [Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024; HIMSS, 2023].

A foundational measure is the development and enforcement of comprehensive security policies. These define acceptable communication practices, email standards, authentication procedures and incident-reporting pathways [Herzig, 2013]. Clear policies reduce ambiguity and ensure employees know how to act when encountering suspicious activities. Regular risk assessments evaluate vulnerabilities in infrastructure, staff behavior, and third-party interactions, enabling institutions to prioritize mitigations by likelihood and impact [U.S. Department of Health and Human Services, 2022]. The HICP framework recommends including phishing simulations and targeted scans to uncover weaknesses in both technical systems and human factors [U.S. Department of Health and Human Services, 2022].

Third-party risk management is also crucial. Many providers rely on vendors for EHRs, billing, and cloud services, making vendor oversight a key security concern. Contracts must clearly define data-protection responsibilities, incident-response obligations, and breach-reporting timelines. Several high-profile breaches have been attributed to third-party failures, highlighting the need for regular audits and strong contractual controls [U.S. Department of Health and Human Services, 2023].

High employee awareness and an open reporting culture further increase resilience. Healthcare workers juggle time-sensitive duties, making them prime targets for social engineering. Establishing a non-punitive environment where staff report suspected phishing without fear of retribution is essential [Schneier, 2015]. Organisations with strong internal reporting detect phishing sooner and limit data exposure [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Another emerging practice is embedding phishing awareness into broader risk-management strategies. Forward-looking institutions reinforce vigilance through regular training, leadership support and reward systems [HIMSS, 2023; PhishMe Inc., 2016; Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and Hossain, Mohammad Alamgir, 2022]. This holistic approach recognizes that resilience depends on behavioral change as well as technical defenses.

Healthcare organizations are also encouraged to adopt frameworks such as ISO/IEC 27001, which provide structured guidance for implementing and auditing an information-security management system (ISMS) [International Organization for Standardization, 2022]. Certification strengthens defenses and demonstrates compliance with regulations such as HIPAA and GDPR.

Finally, continuous improvement is vital. Phishing tactics evolve rapidly, leveraging AI-generated messages and deepfake impersonations. Policies, training and controls must therefore be updated regularly using fresh threat intelligence [U.S. Department of Health and Human Services, 2023]. Static measures are insufficient; dynamic, data-driven updates are key to long-term protection.

In conclusion, organizational measures, policies, assessments, vendor oversight, open communication, standards adoption and continuous updates provide the governance structure that turns technical controls into a robust, multilayered defense against phishing in healthcare.

3.3 Human Factors and Training

Human error accounts for over 90% of data breaches, often via phishing or social engineering, which highlights the need for human-centered defenses alongside technical controls. Phishing was implicated in 82% of observed breaches, making it the most exploited attack vector in healthcare environments [Verizon Communications Inc., 2023]. Under high workload and time pressure, healthcare employees are particularly susceptible to deceptive emails, with simulated click-through rates reaching as high as 25% in some organizational assessments. These factors demonstrate that, beyond technical safeguards, cultivating vigilant user behavior through targeted training and awareness is essential to reducing human-related vulnerabilities.

Tailoring training content to different organizational roles is a critical success factor. IT and security teams require in-depth technical modules on attack vectors, malware payloads, and incident response, whereas clinicians and administrative staff benefit from concise, behavior-focused sessions. As [Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024] emphasize, adapting cybersecurity education to user roles improves engagement, relevance, and effectiveness.

To deliver those role-specific programs effectively, many organizations rely on simulated phishing exercises. These expose employees to realistic attack scenarios and have been shown to reduce successful incidents over time [Schneier, 2015; PhishMe Inc., 2016]. Sim-

ulations teach staff to recognize common red flags, suspicious URLs, urgent language, and unexpected attachments (see Figure 3.2).

Figure 3.2: The five most common phishing red flags employees should learn to spot [Optimal Networks, Inc., 2020].

Moreover, fostering a non-punitive culture around cybersecurity reporting is essential. Employees should be encouraged to report suspected phishing attempts without fear of blame or disciplinary action [Schneier, 2015]. Studies show that organizations promoting a culture of trust and openness achieve faster detection and response rates for phishing incidents [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017]. Conversely, punitive environments often discourage reporting, allowing breaches to escalate undetected.

Healthcare organizations are increasingly adopting gamified training models to enhance engagement and learning outcomes. Gamification techniques, such as point scoring,

leaderboards, and scenario-based challenges, have been demonstrated to improve knowledge retention and motivate employees to apply cybersecurity principles in practice [Microsoft Corporation, 2022]. Such approaches address the cognitive fatigue often associated with traditional, lecture-based security training.

Another important aspect of human factor management is the reinforcement of learned behaviors through ongoing communication. Monthly newsletters, security bulletins, and brief refresher sessions can help maintain employee awareness and vigilance [Microsoft Corporation, 2022]. Phishing tactics evolve rapidly, with new trends such as QR-code phishing (quishing) and deepfake impersonations becoming more prevalent. Regular updates ensure that employees are prepared for emerging threats rather than solely historical ones.

Finally, leadership engagement is a crucial but sometimes overlooked dimension of successful training initiatives. When executives and department heads actively participate in cybersecurity training and visibly prioritize phishing defense efforts, employees are more likely to internalize the importance of vigilance [U.S. Department of Health and Human Services, 2022]. Leadership-driven initiatives signal that cybersecurity is an organizational priority rather than an isolated technical issue.

In summary, addressing human factors through targeted training, cultural development, and continuous reinforcement is essential for building healthcare resilience against phishing attacks. Technological defenses alone are insufficient; sustainable protection requires active, informed, and empowered human participants across the entire organization.

3.4 Evaluating the Effectiveness of Existing Measures

Despite the widespread implementation of defense mechanisms, phishing remains a persistent and highly damaging threat to healthcare organizations. Reports consistently demonstrate that many breaches occur not because of the absence of security technologies, but due to lapses in their implementation, gaps in human behavior, and outdated organizational processes [FRSecure, 2021; Verizon Communications Inc., 2023].

A review by HIPAA-Journal highlights that inconsistent security training, lack of regular system updates, and poor endpoint protection remain significant contributors to successful phishing incidents in healthcare [FRSecure, 2021]. In particular, healthcare institutions that treat phishing simulations as a one-time event, rather than a continuous training process, show substantially higher susceptibility rates among staff [PhishMe Inc., 2016].

Case studies reinforce these findings. The Magellan Health breach serves as a cautionary example. Despite basic e-mail filtering, attackers crafted a believable spear-phish that tricked an employee into surrendering credentials (see Sect. 2.4) [HIPAA Journal, 2020a]. These cases demonstrate that a purely technological defense strategy is insufficient. Even the most sophisticated filters, firewalls, and antivirus systems cannot prevent all phishing attempts, especially those that rely on social engineering and psychological manipulation [Schneier, 2015]. As a result, a multi-layered defense strategy, often referred to as defense in depth, has emerged as a best practice across critical industries [National Institute of Standards and Technology, 2024].

Defense in depth incorporates technical tools, human-centric initiatives, organizational policies, and continuous monitoring. Each layer is designed to mitigate different attack vectors, ensuring that if one control fails, others can detect or contain the breach. In healthcare settings, this approach is particularly important because of the sensitive nature of medical data, the high operational urgency, and the often fragmented IT environments [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Furthermore, evaluating the true effectiveness of existing measures requires objective metrics and regular reassessments. According to the Verizon 2023 Data Breach Investigations Report, organizations that conduct regular phishing simulations and track click-through rates, reporting rates, and time-to-detection metrics demonstrate stronger resilience over time [Verizon Communications Inc., 2023]. Without quantitative measures, organizations risk overestimating their defenses, leaving hidden vulnerabilities unaddressed.

One common weakness in many healthcare organizations is the lack of quick response plans designed just for phishing attacks. While general response procedures may be in place, phishing-specific guides, listing clear steps like resetting passwords, locking systems and reporting the attack, are often missing or outdated [U.S. Department of Health and Human Services, 2022]. Organizations that have written and practiced response plans are usually able to stop phishing attacks more quickly and with less cost than those without [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Another critical weakness is the limited integration of threat intelligence into phishing defense strategies. Many healthcare systems rely on internal indicators of compromise (IoCs) without leveraging external threat feeds that track phishing domains, newly registered fraudulent websites, or known attack campaigns targeting healthcare [U.S. Department of Health and Human Services, 2023]. Incorporating external threat intelligence allows organizations to proactively update their defenses and block new threats before they cause harm.

Vendor-related vulnerabilities remain a serious concern in healthcare cybersecurity. Third-party service providers often have access to critical systems and sensitive data, yet their security practices can vary significantly. To reduce risk, organizations must conduct regular audits of vendors' security measures, enforce clear contractual obligations for breach notification, and require phishing awareness training. According to recent findings, 55% of healthcare organizations experienced a breach caused by a third party, highlighting the urgent need for proactive vendor risk management, especially in the context of phishing [HIPAA Journal, 2025].

Moreover, leadership involvement in cybersecurity evaluations remains inconsistent. Studies show that healthcare institutions where senior management actively supports and funds cybersecurity initiatives experience fewer successful attacks and faster recovery times [HIMSS, 2023]. Leadership buy-in ensures that cybersecurity is viewed as an organizational priority rather than a technical afterthought.

Healthcare-specific guidelines, such as the Health Industry Cybersecurity Practices (HICP) by the U.S. Department of Health and Human Services, recommend regular tabletop exercises, threat modeling, and risk assessments tailored to phishing threats [U.S. Department of Health and Human Services, 2022]. Despite these recommendations, compliance is often uneven, particularly among smaller organizations with limited resources. Addressing these disparities is crucial for sector-wide resilience.

In conclusion, the current evaluation of phishing defenses within healthcare organizations reveals a landscape of partial successes and critical weaknesses. While many institutions have deployed technical controls and conduct basic employee training, the effectiveness of these measures is often undermined by inconsistent application, lack of continuous improvement, insufficient threat intelligence integration, and organizational complacency. Only through a multi-layered, dynamic, and metrics-driven approach can healthcare systems hope to achieve sustained resilience against the evolving threat of phishing attacks.

3.5 Global Guidelines and Best Practices

Given the growing sophistication of phishing threats, various international and national bodies have issued cybersecurity guidelines tailored to critical sectors, including healthcare. These frameworks aim not only to enhance technical defenses but also to strengthen organizational resilience and improve human factors in cybersecurity [U.S. Department of Health and Human Services, 2022; European Union Agency for Cybersecurity, 2023].

One of the most influential healthcare-specific guidelines is the Health Industry Cybersecurity Practices (HICP) published by the U.S. Department of Health and Human Services.

The HICP framework offers detailed technical advice focused on mitigating prevalent threats, including phishing. It emphasizes the deployment of multi-factor authentication, routine phishing awareness training, endpoint protection, and network segmentation [U.S. Department of Health and Human Services, 2022]. The comprehensiveness of HICP is reflected in its layered approach, recommending simultaneous technical, procedural, and training initiatives to build resilience.

At the European level, the European Union Agency for Cybersecurity (ENISA) plays a critical role in issuing sector-specific cybersecurity recommendations. ENISA's 2022 Threat Landscape Report identifies phishing as a primary attack vector against healthcare and urges institutions to implement real-time threat monitoring, rapid incident response, and continuous employee training programs [European Union Agency for Cybersecurity, 2023]. Unlike broader information security frameworks, ENISA's healthcare reports offer practical, role-based cybersecurity guidelines, recognizing the operational realities of hospitals, clinics, and laboratories.

Internationally, ISO/IEC 27001 stands as the most widely adopted global standard for information security management systems (ISMS). While not healthcare-specific, ISO/IEC 27001 provides a structured, auditable framework for identifying information security risks, including phishing, and implementing systematic controls to mitigate them [International Organization for Standardization, 2022]. Organizations certified under ISO/IEC 27001 must perform regular risk assessments, establish clear policies, and document incident management procedures, which indirectly strengthens defenses against phishing attacks.

Applying these standards yields significant operational and compliance benefits. Studies show that healthcare organizations adhering to recognized cybersecurity frameworks report fewer successful phishing incidents and faster incident response times compared to non-compliant counterparts [HIMSS, 2023]. Compliance with frameworks like HICP or ISO 27001 also reduces legal liabilities in the event of a data breach and improves patient trust, an increasingly critical factor in digital healthcare ecosystems.

However, successful adoption of these guidelines faces obstacles, particularly among small and medium-sized healthcare providers. Common barriers include limited financial resources, staff shortages, and a lack of cybersecurity expertise [European Union Agency for Cybersecurity, 2023; HIMSS, 2023]. To address this, HICP and ENISA both recommend a risk-based approach, advising institutions to prioritize implementation based on the criticality of systems and data rather than aiming for exhaustive compliance immediately.

Moreover, global trends increasingly advocate for integrating cybersecurity guidelines into overall risk-management frameworks. The NIST Cybersecurity Framework (CSF), whose five core functions are outlined in Figure 3.3, has gained international acceptance and provides healthcare institutions with a scalable model for identifying, protecting, detecting, responding to and recovering from cybersecurity threats, including phishing [National Institute of Standards and Technology, 2024]. The NIST CSF is particularly lauded for its flexibility, allowing organizations of different sizes and maturity levels to adapt its principles effectively.

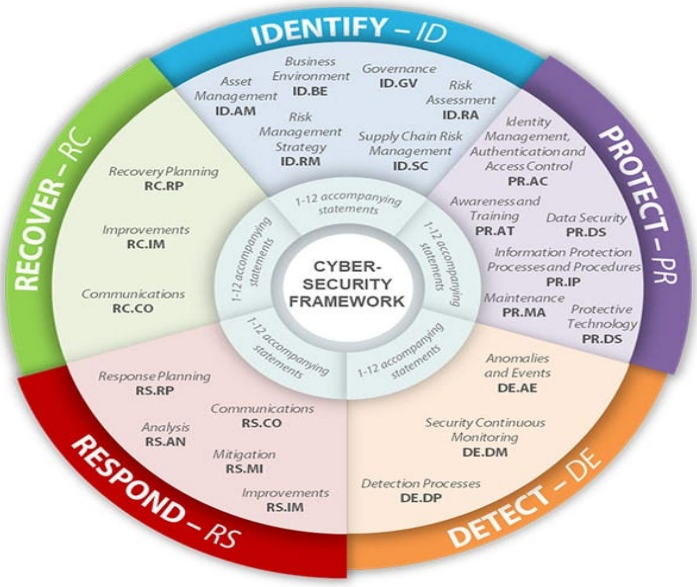

Figure 3.3: Core functions of the NIST Cybersecurity Framework 2.0. Source: NIST [National Institute of Standards and Technology, 2024].

Finally, there is a growing emphasis on harmonization across standards. Organizations that map HICP recommendations to ISO/IEC 27001 controls or align ENISA guidance with NIST principles can achieve more efficient compliance processes and better security outcomes [European Union Agency for Cybersecurity, 2023; National Institute of Standards and Technology, 2024]. This interoperability reduces administrative burdens and helps healthcare providers maintain strong cybersecurity postures even in complex regulatory environments.

In conclusion, while technological defenses remain vital, adopting global cybersecurity guidelines tailored to healthcare significantly enhances organizational readiness against phishing threats. Continuous engagement with evolving standards, supported by leadership commitment and staff training, forms the cornerstone of sustainable phishing defense strategies.

Chapter 4

Methodology

4.1 Case Selection & Data Collection

PRISMA Framework: This literature review was conducted in accordance with the PRISMA guidelines [Page et al., 2021], ensuring a transparent, replicable process of study identification, screening, eligibility assessment, and inclusion.

Databases Searched: I systematically questioned major repositories, PubMed, SpringerLink, and IEEE Xplore, to capture peer-reviewed journal articles. In addition, I searched industry whitepapers and government advisories (e.g., HHS, ENISA, HIPAA Journal) to include technical and real-world reports.

Keywords and Search Strings: Searches combined different terms like `"phishing" AND "healthcare"` as well as `("case study" OR "incidence" OR "attack")` with appropriate field tags (e.g., title/abstract), ensuring I captured all relevant discussions of phishing events in healthcare settings.

Time Window: Only sources published between 2015 and 2025 were considered, reflecting the evolution of both phishing tactics and healthcare IT in the digital era.

Inclusion and Exclusion Criteria: I included only English-language documents from credible institutions or peer-reviewed outlets and excluded non-English materials, editorials, and studies lacking substantive discussion of phishing in healthcare.

Final Source Set: Applying these criteria yielded 37 sources for in-depth thematic analysis. These were then categorized into:

- Descriptive studies of phishing incidents

- Analyses of system vulnerabilities and threat vectors
- Evaluations of technical and organizational defenses
- Investigations into human-centered interventions

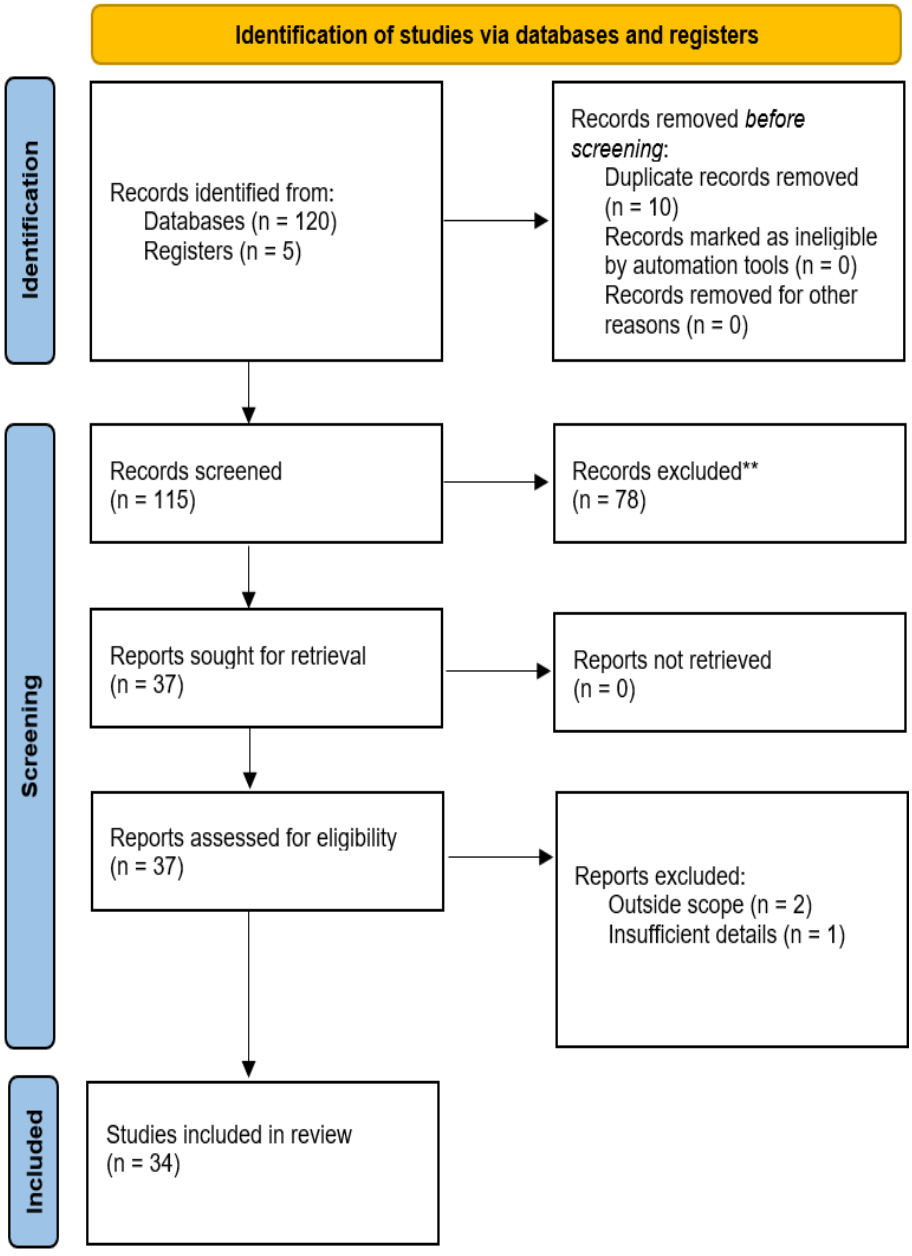

Figure 4.1: PRISMA diagram. (Own diagram.)

4.2 Analysis Procedure

4.2.1 Analytical Framework

Each selected source and case was examined using a three-dimensional coding scheme:

1. **Attack Vector**: email payloads, credential harvesting, link-based tactics
2. **Impact Type**: data loss, service disruption, patient safety risks
3. **Countermeasure Category**: technical (e.g. MFA), organizational (e.g. policies), human-centered (e.g. training)

This framework enabled consistent comparison across diverse studies and real-world incidents (e.g. the Magellan Health breach).

4.2.2 Scope & Limitations

This methodology only used English-language sources that were publicly available online. To make sure I wasn't relying on a single report, I compared information across multiple papers and applied my coding scheme twice on two example cases to check for consistency. Still, these findings might not hold true for non-English settings or for data hidden inside organizations.

Chapter 5

Implementing Comprehensive Countermeasures for Phishing in Healthcare

5.1 Identified Risks in Healthcare Systems

Phishing attacks exploit structural and behavioral weaknesses in healthcare settings, often unfolding in predictable stages such as those depicted in Figure 5.1. These stages, which include reconnaissance, delivery, exploitation, and exfiltration, leverage technological, organizational, and human vulnerabilities to compromise sensitive health information [Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido, 2022].

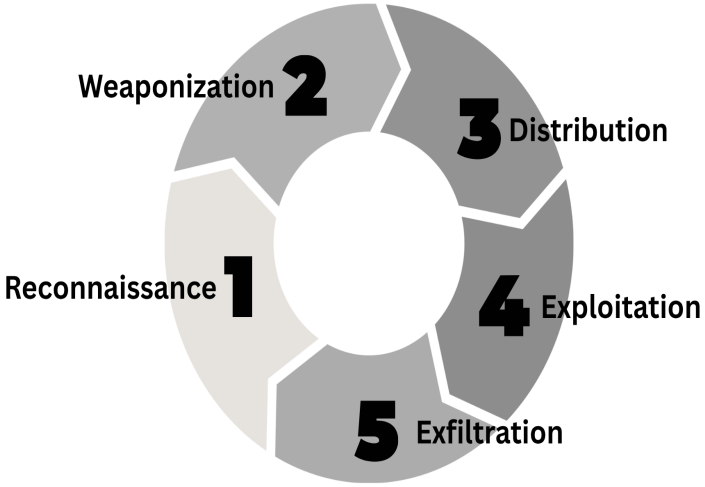

Figure 5.1: Phishing attack life cycle commonly observed in healthcare environments (Own illustration adapted from [Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido, 2022])

From a technological perspective, legacy systems with missing patches and fragmented IT infrastructures remain prevalent [Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024]. Poor network segmentation and ineffective email filtering mechanisms further expose systems to phishing-based intrusions [European Union Agency for Cybersecurity, 2023].

On the organizational front, healthcare providers often allocate limited budgets to cybersecurity, prioritizing direct patient care tools instead. This results in minimal staffing for cybersecurity roles, irregular audits, and lax enforcement of IT policies [Herzig, 2013; Peltier, 2016]. Inconsistencies in access control and incident response have been reported in several breach cases, including UVM Health [HIPAA Journal, 2020b].

Human factors remain the most exploited entry point. Healthcare staff, especially under pressure, frequently overlook phishing indicators such as spoofed email addresses or urgent call to actions [Waddell, 2024]. Moreover, emerging tactics like deepfake audio and QR-code phishing (quishing) are often unfamiliar to employees [Cloudflare, 2024; U.S. Department of Health and Human Services, 2023].

Understanding the synergy of these risk factors is essential before exploring technical, organizational, and human-centric countermeasures in subsequent sections.

5.2 Consequences of Phishing Attacks in Healthcare

Phishing attacks in the healthcare sector carry disproportionately severe consequences due to the sensitivity, regulatory obligations, and operational dependencies tied to medical data. Unlike many other sectors, healthcare organizations face dual damage: compromised patient safety and systemic disruption [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017; Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024].

A critical impact is the breach of Protected Health Information (PHI). Stolen PHI can be sold on the dark web, used for identity theft, or even held for ransom [Imprivata, 2023; IBM, 2024a]. According to the IBM Cost of a Data Breach Report 2024, the healthcare industry continues to report the highest average cost of a data breach for the 13th consecutive year, reaching $11 million per incident [IBM, 2024a].

Beyond financial losses, phishing-related incidents can compromise clinical operations. For example, ransomware delivered via phishing emails may lock Electronic Health Records (EHRs), delaying critical treatments or diagnoses [HIPAA Journal, 2020b; European Union Agency for Cybersecurity, 2023]. A striking example is the 2020 ransomware at-

tack on UVM Health, which forced a month-long manual fallback and directly impacted patient care [HIPAA Journal, 2020b].

Reputational damage is another major consequence. When breaches become public, patient trust is eroded and legal liabilities often follow. Many affected organizations face class-action lawsuits or compliance penalties under regulations like HIPAA and GDPR [Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024; U.S. Department of Health and Human Services, 2022].

To better visualize the scope of consequences, Table 5.1 summarizes key impact areas and provides real-world examples of phishing incidents in the healthcare domain.

Table 5.1: Comparison of key phishing consequences in healthcare.

Consequence Type	**Description**	**Example**
Data Breach	Theft of PHI and other sensitive medical records, often sold or ransomed	Magellan Health breach impacted over 364,800 patients [HIPAA Journal, 2020a]
Operational Disruption	Downtime of EHRs, communication loss, manual fallback	UVM Health faced weeks-long EHR outage post-phishing attack [HIPAA Journal, 2020b]
Financial Losses	Recovery costs, fines, litigation, revenue loss	Average breach cost reached $11 million in 2024 [IBM, 2024a]
Reputational Damage	Loss of patient trust, negative media, regulatory scrutiny	Roper St. Francis incident affected 190,000+ patients [HIPAA Journal, 2021a]

Ultimately, phishing attacks represent more than just technical incidents. They are events with human, ethical, legal, and institutional ramifications. This underscores the need for proactive strategies, which will be discussed in the upcoming sections.

5.3 Technical Strategies Against Phishing

To reduce phishing-related risk, I describe below the key technical defenses, spanning email, authentication, network, and detection controls, framed within Zero Trust and Defense-in-Depth architectures.

- **Email Filtering and Threat Detection:** Advanced email gateways use machine learning (ML) and natural language processing (NLP) to analyze metadata,

language patterns, and sender authentication. These systems identify spoofed addresses, embedded malware, or unusual content, and block or quarantine emails using real-time threat intelligence. Such filtering effectively reduces the number of phishing emails that reach healthcare staff [Waddell, 2024; Microsoft, 2023; U.S. Department of Health and Human Services, 2023].

- **Multi-Factor Authentication (MFA):** MFA introduces a second verification step, such as a one-time code, phone prompt, or biometric scan, during log-in, blocking unauthorized access if credentials are compromised. It is especially effective at reducing account-takeover incidents in healthcare settings [Microsoft, 2023; International Organization for Standardization, 2022].

- **Zero Trust Architecture (ZTA):** ZTA assumes no user or device is inherently trusted, regardless of network location. Each access request is authenticated and evaluated continuously. This limits lateral movement after compromise and enforces strict access and device compliance policies.

- **Domain Authentication Protocols (SPF/DKIM/DMARC):** SPF, DKIM and DMARC work together to verify authorized sending IPs, ensure message integrity, and enforce domain-based policies. Although these protocols effectively block spoofed emails, fewer than 40% of healthcare providers fully deploy all three, often due to DNS misconfigurations or limited expertise, leaving critical gaps in email security [European Union Agency for Cybersecurity, 2023].

- **SIEM & SOAR Integration:** Security Information and Event Management (SIEM) aggregates logs to spot anomalies, and Security Orchestration, Automation, and Response (SOAR) can automate responses, isolating hosts or disabling accounts, to contain phishing fast. Care must be taken, because an attacker who first "sniffs" the network could forge widespread anomalous traffic and trigger a mass lockdown, effectively causing a DoS if playbooks aren't scoped carefully [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

- **AI-Driven Anomaly Detection:** Machine learning models build behavior baselines, login times, data access patterns, device usage, and flag deviations that may signal credential misuse or insider threats. These systems can provide near real-time alerts, but they must be protected against "training corruption", where an attacker gradually feeds the model malicious yet normalized traffic to desensitize its anomaly thresholds [Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and Hossain, Mohammad Alamgir, 2022].

- **Defense-in-Depth Frameworks:** The DiD model enforces overlapping barriers, firewalls, endpoint protection, segmentation, access controls, IDS, and encryption, so a breach in one layer is contained by the others. This approach is vital in healthcare's mixed legacy/modern infrastructures. Figure 5.2 shows how technical, physical, and administrative controls combine to deliver comprehensive threat mitigation [Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido, 2022].

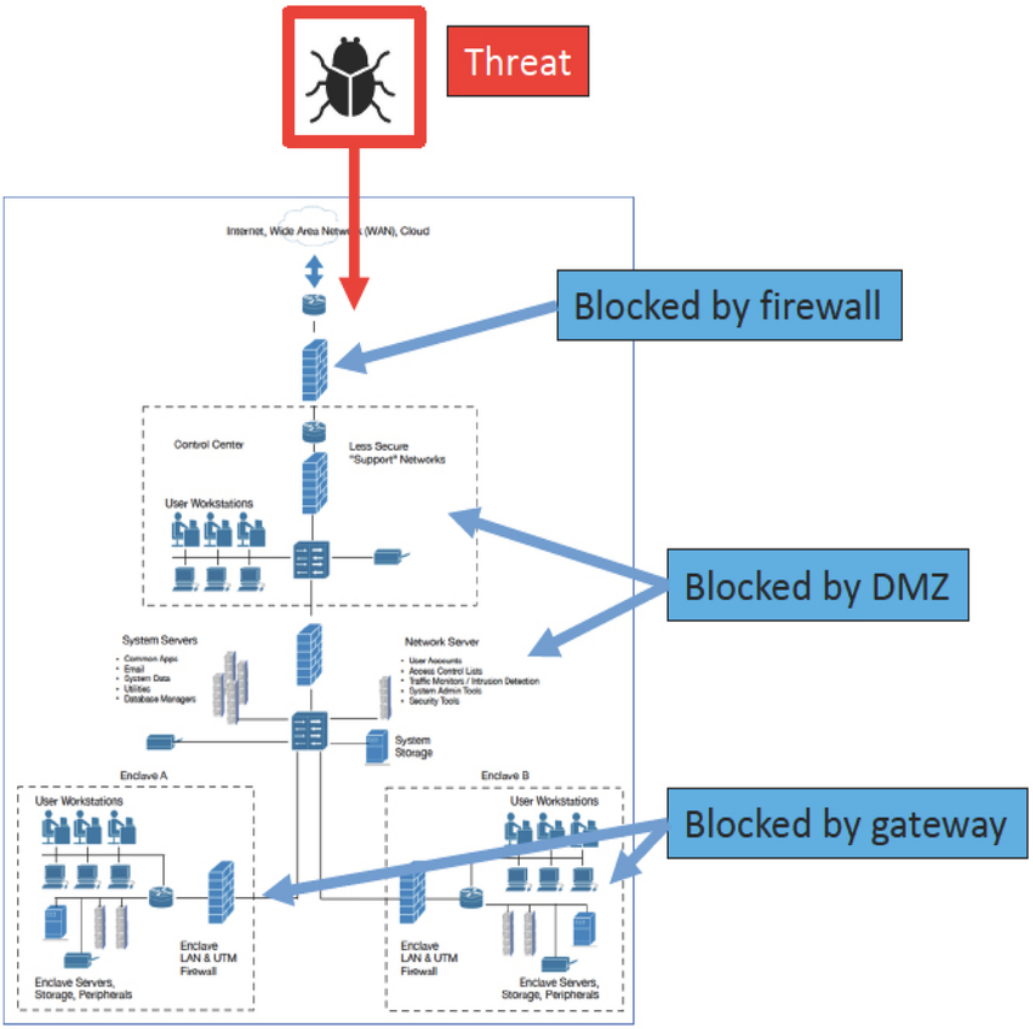

Figure 5.2: Defense-in-Depth architecture adapted for healthcare environments [Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido, 2022]

Together, these technical controls form the backbone of proactive phishing mitigation. When strategically layered, they reduce the attack surface, limit threat propagation and provide early warning signals, creating a robust digital perimeter that aligns with the realities of modern cyber threats in healthcare.

5.4 Organizational Strategies and Policies

Beyond technical safeguards, phishing prevention in healthcare requires strategic organizational planning and policy implementation. These efforts shape how people, processes, and technologies are governed to minimize human error, promote accountability, and enable coordinated incident response. While tools can detect or block many attacks, organizations must ensure that their structures and workflows do not introduce weaknesses that phishing can exploit.

- **Security Governance and Leadership:** Establishing a dedicated cybersecurity governance structure is foundational. This includes assigning a Chief Information Security Officer (CISO) or equivalent leadership responsible for setting security objectives, aligning them with clinical operations, and overseeing strategic investments. Organizations that have both a CISO and a formal steering committee tend to adopt more mature anti-phishing strategies. However, precise data on how many healthcare institutions maintain such committees is not publicly available. Surveys suggest only around 60% of U.S. providers even have a designated CISO, implying that committee adoption may be similarly limited [HIMSS, 2023].

- **Policies and Acceptable Use Guidelines:** Clearly defined policies regulate how employees handle emails, access systems, and report suspicious messages. Acceptable use policies (AUPs) outline do's and don'ts regarding device use, external communication, and file handling. Policy enforcement mechanisms, such as mandatory policy acknowledgement and disciplinary frameworks, enhance compliance and accountability across departments [HIPAA Journal, 2020b; Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

- **Security Awareness Training Programs:** Regular training educates staff on phishing red flags, response procedures, and real-world case studies. Organizations may run phishing simulations to evaluate awareness levels and tailor training accordingly. Studies show that institutions conducting simulations every 3-6 months experience reduced click rates and faster reporting of phishing attempts [U.S. Department of Health and Human Services, 2023; Cloudflare, 2024]. For maximum impact, content should be role-specific, for example, front desk staff versus IT personnel.

- **Incident Response and Escalation Planning:** Comprehensive response plans guide what happens after a phishing attempt is reported or detected. These plans

include containment procedures (e.g., isolating compromised devices), root cause analysis, stakeholder communication, and recovery workflows. Institutions with regularly tested incident response plans report faster time-to-containment and less data loss in phishing-related breaches [European Union Agency for Cybersecurity, 2023; International Organization for Standardization, 2022].

- **Third-Party Risk Management:** Healthcare providers frequently collaborate with external vendors for billing, telehealth, diagnostics, and data storage. Organizational policies must extend to these third parties via contractually enforced security standards and audits. Phishing attacks exploiting third-party credentials (e.g., contractor emails) are increasingly common and can bypass perimeter defenses without robust access control and vendor vetting procedures [Waddell, 2024].

When consistently applied and regularly reviewed, these organizational strategies serve as the operational backbone of a healthcare institution's phishing defense. They translate security intent into institutional culture and workflows, ensuring that human and structural vulnerabilities are proactively addressed.

5.5 Human-Centered Strategies and Future Directions

Technical and organizational defenses are essential for phishing mitigation, but the human element remains the most unpredictable and frequently targeted. Attackers exploit cognitive shortcuts, stress, and inattention, factors inherent to healthcare environments. This section outlines key human-centered interventions currently used to improve resilience against phishing, followed by an outlook on future trends in research and industry.

5.5.1 Human-Centered Interventions

Human-focused strategies form a crucial layer of protection by shaping behavior and decision-making under pressure. One common intervention is behavioral training combined with phishing simulations. These exercises, particularly when tailored to job-specific roles and delivered regularly, have been shown to reduce click-through rates on phishing emails by over 50% [U.S. Department of Health and Human Services, 2023; Cloudflare, 2024]. In tandem, Just-in-Time (JIT) warnings offer real-time nudges, such as pop-ups when clicking suspicious links, to disrupt automatic behavior and prompt reevaluation [Deanna D. Caputo and Shari Lawrence Pfleeger and Jay D. Freeman and M. Elizabeth Johnson, 2016].

A strong security culture is also fundamental. Healthcare organizations that foster a non-punitive environment encourage early reporting of suspicious messages, increasing the chances of containment. Transparency and support from leadership reinforce a learning mindset rather than fear of blame [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017; European Union Agency for Cybersecurity, 2023]. Furthermore, tailoring education to specific job roles, like front desk staff, clinicians, or IT personnel, ensures that training is both relevant and engaging. Role-specific modules address unique risks, such as vishing for call center staff or QR-code phishing for radiology teams [Waddell, 2024].

5.5.2 Emerging Trends and Research Directions

Looking ahead, the next wave of phishing mitigation in healthcare will likely involve a convergence of behavioral analytics, automation, and interdisciplinary practices. AI-powered personalized training is one promising direction. These systems track employees' interaction patterns (e.g., click rates on simulated phishing emails) and automatically deliver short, context-aware training modules after risky behavior is detected [Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and Hossain, Mohammad Alamgir, 2022]. However, collecting and analyzing such behavioral data raises privacy and consent issues. Organizations must ensure transparency, informing staff what data is collected and why, securely store and anonymize records where possible, and comply with data-protection regulations (e.g., GDPR [Parliament and of the European Union, 2016], HIPAA [U.S. Department of Health and Human Services, 2022]) to maintain trust and uphold ethical standards.

Another promising area involves cognitive nudging and interface redesign. Drawing from behavioral economics, these techniques reduce cognitive overload and help users make safer decisions without restricting autonomy. Default-blocking of risky file types, color-coded email warnings, and simplified decision trees are examples in use [Deanna D. Caputo and Shari Lawrence Pfleeger and Jay D. Freeman and M. Elizabeth Johnson, 2016; European Union Agency for Cybersecurity, 2023].

Lastly, leading institutions are beginning to establish cross-disciplinary cybersecurity teams. This approach integrates knowledge from clinical safety, psychology, and IT, promoting a deeper understanding of how human behavior interacts with digital systems. This shift marks a growing recognition that cybersecurity, especially in healthcare, must go beyond technical boundaries to be truly effective [Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and

Hossain, Mohammad Alamgir, 2022; U.S. Department of Health and Human Services, 2023].

Taken together, human-centered interventions and forward-looking innovations offer a comprehensive path for reducing phishing risk in healthcare. While no strategy is foolproof, fostering a resilient workforce, equipped with context-specific knowledge, feedback mechanisms, and cultural support, can drastically reduce susceptibility to attacks and speed recovery when incidents occur [Deanna D. Caputo and Shari Lawrence Pfleeger and Jay D. Freeman and M. Elizabeth Johnson, 2016; U.S. Department of Health and Human Services, 2023].
Building a security-conscious culture requires a combination of leadership support, behavioral feedback loops, and environment-specific interventions. As illustrated in Figure 5.3, such a culture includes components like organizational alignment, employee engagement, and long-term behavior change strategies, which underpin the most resilient phishing defense ecosystems [Consultia, 2023; Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017].

Figure 5.3: Human-centered cybersecurity culture model adapted for phishing resilience in healthcare [Deanna D. Caputo and Shari Lawrence Pfleeger and Jay D. Freeman and M. Elizabeth Johnson, 2016]

5.6 Findings and Implications

5.6.1 Reflecting Critically on the State of Research

In the preceding chapters, I examined technical and organizational anti-phishing strategies and uncovered several important gaps and limitations.

First, while many studies document the effectiveness of individual tools, such as MFA, email filtering, or SIEM, few evaluate their combined efficacy in integrated environments. Most of the literature, treats these mechanisms in isolation, neglecting the systemic synergies and potential overlaps that are critical in real-world implementation [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017; Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and Hossain, Mohammad Alamgir, 2022].

Second, there is a reliance on theoretical or vendor-sponsored research, often lacking independent, peer-reviewed empirical validation. For example, many reports on AI-driven anomaly detection or Zero Trust frameworks come from providers with commercial interests. This leads to optimistic performance claims with limited comparative benchmarking.

Third, the bulk of existing research focuses on large, well-resourced healthcare institutions, such as university hospitals, while smaller clinics and outpatient centers are often overlooked. These smaller entities typically lack dedicated IT teams or funding, yet they are frequently excluded from case studies and implementation research [Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024].

Finally, the literature tends to underexplore human factors beyond training interventions. Complex aspects such as organizational culture, change management, and behavioral adaptation are mentioned but rarely empirically examined. There is little understanding of how healthcare staff perceive security policies or adjust over time to new technologies, even though these dynamics are crucial for long-term success.

In summary, while the literature provides a solid foundation in technical and procedural defenses, it often lacks holistic assessments, independent validation, and broader applicability to diverse healthcare environments. Recognizing these limitations is essential for understanding where future research and practical improvements must focus.

5.6.2 Identifying Trends and Recurring Issues

Recent analyses of cybersecurity incidents in healthcare reveal several recurring trends that indicate persistent vulnerabilities in phishing defenses. These trends span technical,

organizational, and regulatory domains, reflecting both the evolving sophistication of attackers and the operational challenges faced by healthcare institutions.

First, AI-enhanced phishing is rising sharply. Advanced phishing campaigns now incorporate machine-generated emails, deepfake voice messages, and contextual spoofing techniques that mimic the tone and style of internal communications. These attacks are more convincing than ever and increasingly difficult for humans to detect. According to [Hoxhunt, 2025], phishing volume has increased by over 4,151% since the introduction of ChatGPT in 2022, though only a small fraction of successful attacks are fully AI-generated. Still, the trajectory suggests AI-driven attacks will become a dominant vector in the coming years.

Second, supply chains and third-party vendors remain a major attack vector. Cybercriminals increasingly target external partners, such as healthcare software vendors, cloud service providers, or outsourced billing companies, that often lack the same level of cybersecurity rigor. Attackers exploit trust relationships to gain privileged access, as seen in 2025 incidents where compromised vendor credentials or VPN connections bypassed hospital defenses [Chan, 2025].

Third, healthcare breaches are growing in both frequency and severity. From 2018 to 2023, hacking-related incidents in healthcare organizations rose by 239%, with over 168 million patient records compromised in 2023 alone [HIPAA Journal, 2024]. Many of these breaches stem from phishing attacks that lead to credential theft, followed by ransomware deployment or database exfiltration. The scale and cost of such incidents have led to reputational damage and increased insurance premiums across the sector.

Lastly, regulatory pressures are intensifying. Revised HIPAA rules now mandate multi-factor authentication (MFA), comprehensive audit logs, vulnerability assessments, and formal breach response protocols. While these measures are crucial for improving patient data protection, smaller clinics and rural healthcare providers frequently report difficulties achieving compliance. Many lack the financial resources, trained personnel, or infrastructure to implement advanced cybersecurity controls, leaving them disproportionately vulnerable to phishing campaigns [Rundle, 2024].

These trends highlight a shifting threat environment. Healthcare organizations must adapt by enhancing phishing defenses to counter AI exploitation, vendor-related risks, escalating breach volumes, and compliance constraints, all while managing limited operational resources.

Table 5.2: Key Trends in Healthcare Cybersecurity (2018–2025)

Trend	Description	Evidence / Source
AI-powered phishing	Use of generative AI and deepfakes to enhance deception	Hoxhunt: 4,151% increase in phishing since 2022 [Hoxhunt, 2025]
Third-party breaches	Attacks through vendor or supply-chain access	80% of breaches via outsourced support services [Chan, 2025]
Increasing breach volume	More incidents and more affected records	239% rise in hacks (2018–2023); 168 million records breached [HIPAA Journal, 2024]
Regulatory tightening	New rules require MFA and logging for HIPAA-covered entities	Updated rules impose MFA and audit requirements [Rundle, 2024]

5.6.3 Bridging the Gap Between Theory and Practice

Although theoretical frameworks for cybersecurity, such as NIST, CSF and ISO 27001, offer comprehensive guidance, many healthcare organizations struggle with practical implementation. Common barriers include limited resources, fragmented IT systems, and competing priorities between clinical care and security [U.S. Dept. of Health and Human Services, 2023; National Institute of Standards and Technology, 2024].

Figure 5.4 illustrates how healthcare entities can map a theoretical target profile to their current profile and plan tiered implementations. This visual demonstrates the structured progression from risk assessment toward tailored cybersecurity operations.

Key implementation challenges include:

- **Resource constraints**: Smaller hospitals often lack dedicated cybersecurity staff and must make trade-offs between clinical and security budgets [U.S. Dept. of Health and Human Services, 2023].
- **Integration issues**: Diverse systems (EHR, IoMT, tele-health) often lack interoperability, making centralized logging and automated monitoring difficult to apply.
- **Cultural resistance**: Clinical teams may perceive security protocols as obstacles, particularly when workflows aren't well integrated with clinical processes [National Institute of Standards and Technology, 2024].

Closing this gap demands:

- Phase-graded implementation, beginning with core functions like "Identify" and "Protect", then adding "Detect", "Respond" and "Recover".

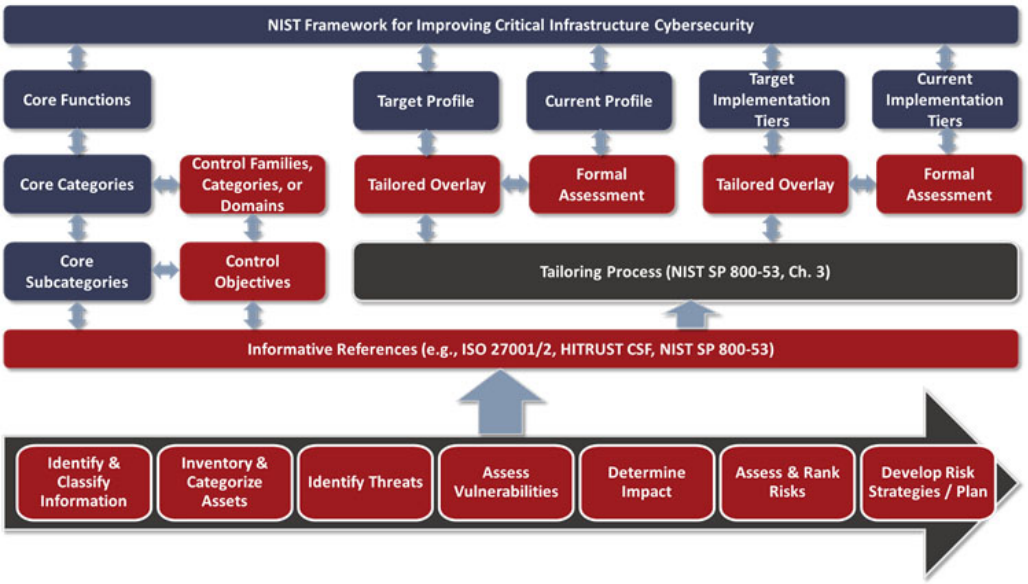

Figure 5.4: NIST-Based Framework Implementation Tiers in Healthcare [U.S. Dept. of Health and Human Services, 2023]

- Use of tailored overlays and enterprise maturity assessments to align implementation with organizational context, size, and risk appetite [U.S. Dept. of Health and Human Services, 2023].

Embedding technical controls is insufficient unless supported by policies, training, and leadership buy-in. Effective bridging requires attention to governance, customization, and ongoing evaluation.

5.6.4 From Analysis to Action

Throughout my thesis, I have examined the complex landscape of phishing in healthcare, tracing systemic vulnerabilities, evolving attack methods, and the multi-layered defenses needed to counter them. The key challenge is not merely recognizing these threats but converting my findings into lasting, practical improvements.

My review of risk factors and countermeasure gaps showed that, even with established frameworks like NIST CSF and ISO 27001, many healthcare organizations encounter implementation difficulties. Limited budgets, legacy IT systems, and gaps in cybersecurity expertise continue to impede progress [National Institute of Standards and Technology, 2024; European Union Agency for Cybersecurity, 2023]. Technical solutions such as Zero Trust architectures and AI-driven anomaly detection offer strong protection, but their

effectiveness relies on coherent strategy, clear governance, and executive support [Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido, 2022].

I also found that human-centered weaknesses persist. Even the most advanced tools fail when staff lack awareness or when reporting processes are unclear. My analysis highlighted that insufficient training frequency, reporting fatigue, and a punitive culture significantly increase phishing success rates [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017; U.S. Department of Health and Human Services, 2023].

Moreover, the threat landscape continues to evolve. Adversaries are leveraging third-party vendor credentials, AI-generated content, and regulatory gaps to bypass static defenses. This dynamic environment demands an adaptive security culture, one that combines automated controls, ongoing education, and shared accountability across all organizational levels.

Chapter 6 will build on these insights by presenting targeted recommendations, spanning policy updates, technology roadmaps, and cultural initiatives, designed to help healthcare providers bridge the gap between theoretical frameworks and real-world resilience against phishing attacks.

Chapter 6

Conclusion and Outlook

6.1 Summary of Key Findings

Healthcare is a prime phishing target. Legacy systems, weak segmentation, and thin security teams widen attack surfaces [Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K., 2017; European Union Agency for Cybersecurity, 2023; Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona, 2024]. The biggest gap is human, because of stress, fatigue, and limited role-based training leave staff open to spear-phishing, AI-generated e-mails, and QR-code scams [Waddell, 2024; Cloudflare, 2024]. The literature shows that layered defense, robust e-mail filters, MFA, Zero-Trust access, and regularly tested incident-response playbooks, offers the best protection as attackers evolve [National Institute of Standards and Technology, 2020; U.S. Department of Health and Human Services, 2023].
Figure 6.1 shows a seven-layer cybersecurity defense model that can be adapted for protection against phishing in healthcare.

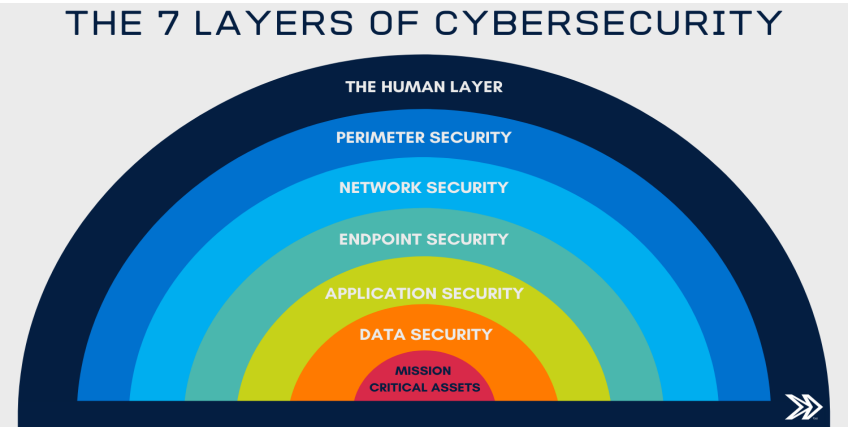

Figure 6.1: Seven-layer cybersecurity framework adapted for phishing defense in healthcare [51Sec, 2019]

- **Layer 7 (Human Layer):** Build resilience with role-based phishing simulations, targeted just-in-time training and a non-punitive reporting culture (Chapters 5.3 - 5.6).
- **Layer 6 (Perimeter Security):** Enforce SPF/DKIM/DMARC, spam filtering and gateway-level threat intelligence to block the bulk of phishing emails (Chapter 5.3).
- **Layer 5 (Network Security):** Segment clinical, guest, and administrative networks to contain lateral movement and use IDS/IPS to flag suspicious traffic patterns (Chapter 5.3).
- **Layer 4 (Endpoint Protection):** Deploy EDR, next-gen antivirus, and host-based firewalls on workstations and medical devices to stop malware payloads delivered by phishing (Chapter 5.3).
- **Layer 3 (Application Security):** Keep clinical and administrative applications patched, use secure coding practices, and harden interfaces (Chapter 5.4).
- **Layer 2 (Data Security):** Encrypt PHI at rest and in transit and apply data-loss prevention rules to block exfiltration even if upstream controls fail (Chapters 5.2 & 5.4).
- **Layer 1 (Mission Critical Assets):** Identify and classify the most sensitive systems (EHR databases, imaging archives) so all defenses focus on protecting what matters most (Chapters 2 & 4).

Finally, recurring issues such as poor implementation of authentication protocols, limited vendor oversight, and uncoordinated regulatory frameworks highlight the urgent need for systemic improvements. Chapter 5's strategic analysis laid the groundwork for actionable pathways, standardized policies, and culturally driven defense models that will be developed in the final chapter.

Together, these insights stress the importance of integrated, evidence-based cybersecurity programs in healthcare, programs that combine infrastructure modernization, workforce engagement, and continuous adaptation to outpace evolving phishing threats.

6.2 Answer to the Research Question

The central research question of this thesis was: *"What are the primary risks, consequences, and effective mitigation strategies associated with phishing attacks targeting healthcare systems?"*

My work shows that phishing risk in healthcare arises from a convergence of outdated digital infrastructure, human factors, and fragmented governance. These vulnerabilities are magnified by AI-generated attacks and supply-chain exploits, leading to data breaches, operational disruptions, and loss of trust [HIPAA Journal, 2024; Hoxhunt, 2025].

The consequences of successful phishing attacks are substantial. Beyond data breaches and financial loss, such incidents frequently disrupt clinical workflows, delay treatments, and damage institutional trust. Case studies and statistical evidence revealed a marked rise in both the scale and severity of healthcare data breaches over the past five years [HIPAA Journal, 2024; Hoxhunt, 2025].

The thesis also identified a range of technical and organizational mitigation strategies, including the implementation of Zero Trust Architectures, SIEM-SOAR integrations, targeted staff training, and board-level accountability frameworks. However, no single control is sufficient in isolation. The findings strongly suggest that a layered, interdisciplinary defense model, one that combines technological safeguards, human-centric awareness initiatives, and policy-driven governance, is the most resilient approach to counter phishing in healthcare settings.

In summary, phishing attacks pose a persistent and evolving threat to healthcare organizations, but they can be effectively mitigated through integrated strategies that address technical, human, and organizational vulnerabilities simultaneously.

6.3 Practical Implications for Healthcare Providers

The findings of this thesis provide actionable insights for healthcare institutions seeking to strengthen their cybersecurity posture against phishing attacks. While theoretical frameworks such as Zero Trust and Defense-in-Depth offer conceptual guidance, their implementation requires tailored adaptations within the healthcare environment.

- **Modernize infrastructure**: Migrate off unsupported systems, enforce patch management, and roll out MFA in high-risk areas (email, EHR).

- **Embed training in culture**: Schedule frequent, role-specific phishing simulations with instant feedback and JIT (Just in time, context-aware prompt that appears exactly when a user is about to take a risky action) reminders.
- **Strengthen governance**: Assign a CISO, secure dedicated budgets, formalize incident response, and include cybersecurity clauses in vendor contracts.

By applying these insights in practice, healthcare organizations can build more resilient environments that proactively address both technological and human vulnerabilities.

6.4 Limitations of the Study

While this thesis provides a broad literature-based overview of phishing risks and mitigation strategies in healthcare, several limitations must be acknowledged.
This thesis relies solely on secondary sources; the absence of interviews or surveys limits insight into organization-specific realities. Because the review centers on U.S. and EU contexts, results may not translate to regions with different legal or technical baselines. Rapid changes in phishing tactics risk making some findings obsolete, and publication bias may skew the picture toward large, well-publicized breaches.
These limitations do not undermine the findings but highlight the need for cautious interpretation and further empirical validation in future work.

6.5 Future Research Directions

Despite progress mapped in this thesis, two questions remain critical as phishing tactics evolve:

1. **Clinical-workflow phishing simulations.** Hospitals need longitudinal, role-specific trials that measure how simulation formats (immersive scenarios vs. micro-lessons) affect click rates, reporting speed, and retention under real clinical pressure.
2. **AI-driven anomaly detection on legacy systems.** Most smaller providers run outdated infrastructure; research should test cost-balanced, hybrid deployment models that integrate machine-learning analytics without disrupting compliance or patient care.

Figure 6.2 visualizes broader research themes, AI adoption, IoT risk, deepfakes, user awareness, insider threats, that frame these priorities.

Figure 6.2: Emerging healthcare cybersecurity research themes [SelectHub, 2025]

Continued inquiry into these areas will help bridge technological advances with practical, resource-aware deployment models, ensuring sustainable resilience as healthcare digitizes further.

Bibliography

51Sec (2019). Layered phishing defense model. https://blog.51sec.org/2019/05/cyber-security-architecture-with-nist.html.

Akter, Shahriar and Uddin, Mohammad Rajib and Sajib, Shahriar and Lee, Wai Jin Thomas and Michael, Katina and Hossain, Mohammad Alamgir (2022). Reconceptualizing cybersecurity awareness capability in the data-centric era. *Annals of Operations Research*, 320:1–26. Publisher: Springer.

Alotaibi, Y. K. and Federico, F. (2017). The impact of health information technology on patient safety. *Saudi Medical Journal*, 38(12):1173–1180. Publisher: Saudi Medical Journal, Riyadh.

Amoroso, E. (2012). *Cyber Attacks: Protecting National Infrastructure*. Butterworth-Heinemann, Oxford.

Blackbaud (2025). Top cyber threats to educational institutions in 2025. https://blog.blackbaud.com/top-cyber-threats-to-educational-institutions/.

Blackkite (2025). Impact on industries and ecosystems – third-party breach report 2025 (logistics focus). https://content.blackkite.com/ebook/2025-third-party-breach-report/impact-on-industries-and-ecosystems.

Chan, B. (2025). Wall street worried it can't keep up with ai-powered cybercriminals. https://www.businessinsider.com/banks-ai-cybersecurity-threats-hackers-generative-ai-2025-3.

Cloudflare (2024). What is quishing? understanding qr-code phishing. https://www.cloudflare.com/learning/security/what-is-quishing/.

Consultia (2023). Ways to improve cybersecurity culture. https://www.consultia.co/ways-to-improve-cybersecurity-culture/.

Cyber Magazine (2024). How hackers are hitting healthcare via their supply chain. https://cybermagazine.com/articles/cyber-attacks-threaten-healthcare-supply-chains.

Damiani, J. (2019). A voice deepfake was used to scam a ceo out of $243,000. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/.

Deanna D. Caputo and Shari Lawrence Pfleeger and Jay D. Freeman and M. Elizabeth Johnson (2016). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1):28–38. Publisher: IEEE.

Do, Nguyet Quang and Selamat, Ali and Krejcar, Ondrej and Fujita, Hamido (2022). Phishing attack life cycle. https://www.researchgate.net/figure/Phishing-attack-life-cycle_fig2_358678073.

European Union Agency for Cybersecurity (2023). Enisa threat landscape: Health sector. Technical report, ENISA.

Europol (2022). Facing reality? law enforcement and the challenge of deepfakes. Technical report, European Union Agency for Law Enforcement Cooperation.

FRSecure (2021). Healthcare phishing: Examples, types and statistics. https://frsecure.com/blog/healthcare-types-of-phishing-attacks/.

Hartman Executive Advisors (2021). How data breaches impact the financial industry. https://hartmanadvisors.com/how-data-breaches-impact-financial-industry/.

Herzig, T. W. (2013). *Implementing Information Security in Healthcare: Building a Security Program*. CRC Press, Boca Raton.

HIMSS (2023). Healthcare cybersecurity survey 2023. https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf.

HIPAA Journal (2020a). Extent of magellan health ransomware becomes clear: More than 364,800 individuals affected. https://www.hipaajournal.com/extent-of-magellan-health-ransomware-becomes-clear-more-than-364000-individuals-affected/.

HIPAA Journal (2020b). Uvm health restores ehr system one month after ransomware attack. https://www.hipaajournal.com/uvm-health-restores-electronic-health-record-system-one-month-after-ransomware-attack/.

HIPAA Journal (2021a). Almost 190,000 patients affected by roper st. francis healthcare phishing attack. https://www.hipaajournal.com/almost-190000-patients-affected-by-roper-st-francis-healthcare-phishing-attack/.

HIPAA Journal (2021b). Phi of more than 100,000 elara caring patients potentially compromised in phishing attack. https://www.hipaajournal.com/phi-of-more-than-100000-elara-caring-patients-potentially-compromised-in-phishing-attack/.

HIPAA Journal (2024). Healthcare data breach statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

HIPAA Journal (2025). 41% of 2024 third party breaches affected healthcare organizations. https://www.hipaajournal.com/41pc-2024-third-party-breaches-affected-healthcare-organizations/.

Hoxhunt (2025). Phishing trends report 2025. https://hoxhunt.com/guide/phishing-trends-report.

IBM (2024a). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach.

IBM (2024b). Ibm report: Escalating data breach disruption pushes costs to new highs. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs.

IBM Security (2024). X-force threat intelligence index 2024. https://www.ibm.com/reports/threat-intelligence.

Imprivata (2023). Hackers, breaches, and the value of healthcare data. https://www.imprivata.com/blog/healthcare-data-new-prize-hackers.

International Organization for Standardization (2022). Iso/iec 27001:2022 – information security, cybersecurity and privacy protection – information security management systems – requirements. https://www.iso.org/standard/27001.

Jain, Ankit Kumar and Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks*, 2017(0):1–20. Publisher: Hindawi.

Kruse, C. S. and Frederick, B. and Jacobson, T. and Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1):1–10. Publisher: IOS Press, Amsterdam.

Malwarebytes (2024). Quishing: Qr-phishing explained and the rapid growth of code-based attacks. `https://www.malwarebytes.com/cybersecurity/basics/quishing`.

Microsoft (2023). 2023 identity security trends and solutions from microsoft. `https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/`.

Microsoft Corporation (2022). Cybersecurity awareness tips from microsoft to empower your team to #becybersmart. `https://www.microsoft.com/en-us/security/blog/2022/10/04/cybersecurity-awareness-tips-from-microsoft-to-empower-your-team-to-#becybersmart/`.

National Institute of Standards and Technology (2020). Zero trust architecture. Special publication 800-207, NIST.

National Institute of Standards and Technology (2024). The nist cybersecurity framework (csf) 2.0. Technical report, NIST.

Optimal Networks, Inc. (2020). Top 5 phishing red flags (infographic). `https://www.optimalnetworks.com/blog/top-5-phishing-red-flags-infographic`.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., and Moher, D. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372:n71. Publisher: BMJ Publishing Group.

Parliament, E. and of the European Union, C. (2016). Regulation (eu) 2016/679 (general data protection regulation). `https://eur-lex.europa.eu/eli/reg/2016/679/oj`.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. CRC Press, Boca Raton.

Pharmaceutical Technology (2021). Pharma cyber attacks: Five breaches that the industry must learn from. https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/.

PhishMe Inc. (2016). Enterprise phishing susceptibility and resiliency report. https://ca.insight.com/content/dam/insight-web/Canada/PDF/partner/phishme/PhishMe-EnterprisePhishingSusceptibility.pdf.

Resecurity (2025). Cyber threats against energy sector surge as global tensions mount. https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount.

Rundle, J. (2024). Healthcare providers face stiffer cyber rules even as they cry for help. https://www.wsj.com/articles/healthcare-providers-face-stiffer-cyber-rules-even-as-they-cry-for-help-b466197a.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company, New York.

SecurityScorecard (2024). 67% of energy sector breaches linked to software and it vendors. https://securityscorecard.com/company/press/67-of-energy-sector-breaches-linked-to-software-and-it-vendors-securityscorecard-reports.

SelectHub (2025). Top 13 cyber security trends for 2025. https://www.selecthub.com/endpoint-security/cyber-security-trends/.

Sharma, Dilli Prasad and Lashkari, Arash Habibi and Parizadeh, Mona (2024). *Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends*. Springer Nature Switzerland, Cham.

Supply Chain Magazine (2024). How are cyberattacks disrupting healthcare supply chains? https://supplychaindigital.com/supply-chain-risk-management/cyber-attacks-threaten-healthcare-supply-chains.

TechTarget (2024). How ai is making phishing attacks more dangerous. https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous.

U.S. Department of Health and Human Services (2022). Social engineering attacks targeting the hph sector. Technical report, U.S. Department of Health and Human Services.

U.S. Department of Health and Human Services (2023). Ai-augmented phishing and the threat to the health sector. Technical report, U.S. Department of Health and Human Services.

U.S. Dept. of Health and Human Services (2023). Health sector cybersecurity framework implementation. Technical report, HHS.

Verizon Communications Inc. (2023). 2023 data breach investigations report. Technical report, Verizon.

Waddell, M. (2024). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. *Healthcare Management Forum*, 37(1):24–29. Publisher: SAGE Publications, for the Canadian College of Health Leaders.

Wealth & Finance International (2024). The average cost of a data breach in the finance sector is $6.08 million. `https://wealthandfinance.digital/The-average-cost-of-a-data-breach-in-the-finance-sector-is-6.08-million-a-staggering-22-percent-higher-than-the-global-average-of-4.88-million/`.

Wired (2020). Hackers are targeting hospitals crippled by coronavirus. `https://www.wired.com/story/coronavirus-hackers-cybercrime-phishing/`.

Wired (2021). They told their therapists everything: Hackers leaked it all. `https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/`.