A Review and Guide

Cyber Threats in European Healthcare:

Combating Phishing and Fraud Through Awareness Training

Executive Summary

Healthcare systems across the DACH region (Germany, Austria, Switzerland) are facing a surge in cyberattacks, with phishing and social engineering among the most prevalent and damaging threats. As medical organizations continue to digitize sensitive patient services and records, cybercriminals are increasingly exploiting human error as the weakest link in the security chain.

Phishing attacks, in particular, continue to bypass technical defenses, targeting frontline healthcare workers with sophisticated, multilingual lures. Despite increased investments in cybersecurity tools, the majority of data breaches in healthcare are still caused by staff clicking on malicious links or unwittingly disclosing credentials [1][2].

Awareness training has emerged as one of the most effective and scalable ways to mitigate this risk. Programs that include role-based education, real-world phishing simulations, and behavior-focused modules can reduce phishing success rates by up to 70% [3]. Given the strict compliance landscape (e.g., GDPR, national data protection laws) and the high cost of cyber incidents, healthcare leaders must prioritize the human element of cybersecurity.

Structured, ongoing awareness training—adapted to local languages and healthcare roles—offers an immediate opportunity to reduce risk, meet regulatory expectations, and improve organizational resilience.

Healthcare providers in the DACH region should adopt a continuous, localized security awareness strategy as a core pillar of their cyber risk management.

Train your people.
Strengthen your frontline.

Hospital under threat
Human error as the "gap" in security
Training reduces phishing success

[1] **ENISA Threat Landscape for Healthcare, 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector

[2] **BSI "Die Lage der IT-Sicherheit in Deutschland 2023"** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf

[3] **Lucy Security Benchmarking Report, 2024** – https://lucysecurity.com (internal customer performance data)

Introduction:

Healthcare as a High-Value, High-Risk Sector

Healthcare institutions in the DACH region occupy a uniquely vulnerable position in the cybersecurity landscape. Hospitals, clinics, insurers, and service providers manage vast amounts of **highly sensitive data**—ranging from electronic patient records (ePA) and insurance numbers to clinical trial data and medication histories. This makes them attractive targets for cybercriminals seeking financial gain, patient identity theft, or access to infrastructure for broader attacks [1].

At the same time, the sector is undergoing rapid digital transformation. In Germany, for example, the Krankenhauszukunftsgesetz (Hospital Future Act) is driving the modernization of clinical IT systems with **over €4.3 billion** in funding for digitization projects [2]. Austria and Switzerland are following similar trajectories, with increasing reliance on telemedicine, cloud-based platforms, and electronic documentation.

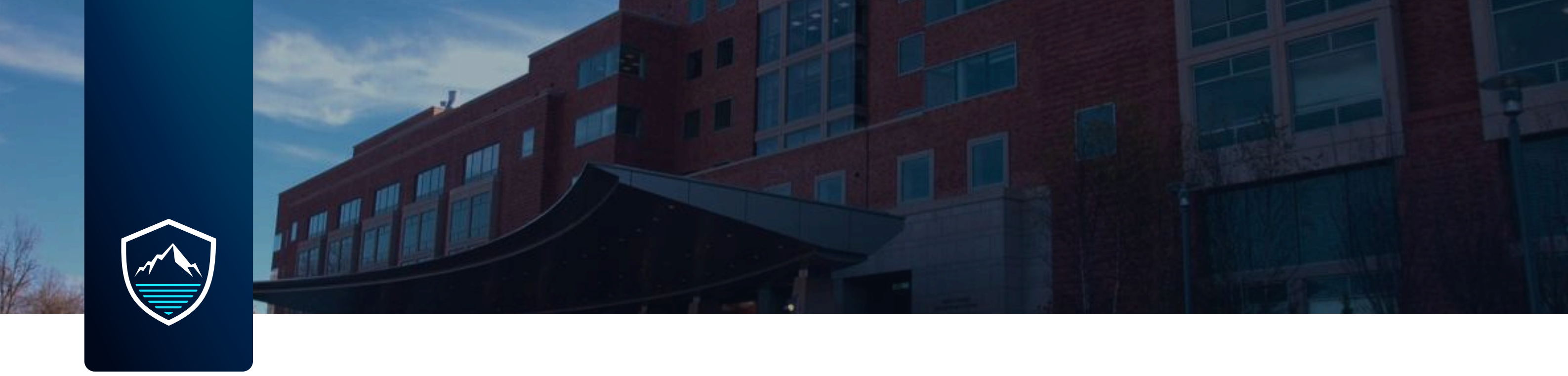
However, this digital expansion often outpaces the implementation of strong cybersecurity protocols. Many healthcare environments still operate with **legacy systems, outdated email infrastructure, and limited IT staffing**. Email remains the dominant communication tool in clinical workflows, increasing the likelihood of successful phishing attacks [3].

A key, often underestimated factor is **time pressure**. Medical professionals work in high-stress, fast-paced environments where rapid response is not optional—it's critical. Clinicians may check email between patients or respond to messages mid-shift, creating ideal conditions for impulsive clicks and reduced scrutiny of suspicious content [4]. Attackers exploit this urgency by crafting phishing messages that mimic internal communications, lab results, or urgent administrative requests.

Additionally, healthcare providers must navigate strict regulatory requirements, including the **EU's General Data Protection Regulation (GDPR) and national laws** such as the German Bundesdatenschutzgesetz (BDSG), Austria's Datenschutzgesetz, and Switzerland's revised Data Protection Act (revDSG). These frameworks demand not only technical safeguards, but also demonstrable steps to educate and protect staff.

In this high-value, high-pressure environment, awareness training emerges as a strategic necessity—not just a compliance checkbox.

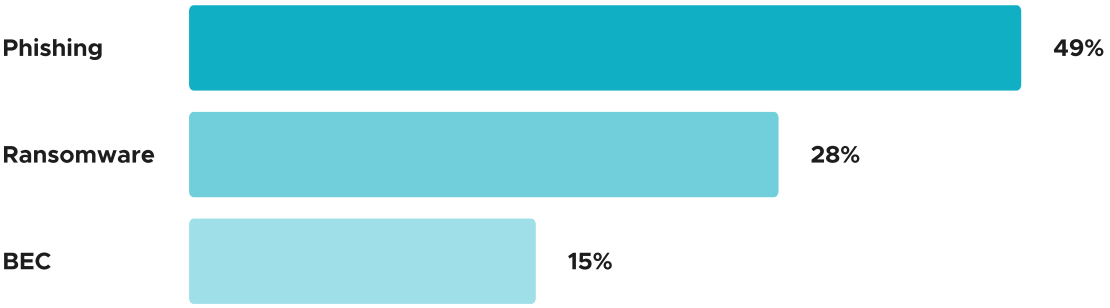
1. **ENISA Threat Landscape for Healthcare, 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **German Federal Ministry of Health** – Krankenhauszukunftsgesetz (KHZG) – https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz
3. **BSI Annual Report 2023** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
4. **Ponemon Institute: The Impact of Cyber Insecurity on Healthcare Delivery, 2022** – https://www.proofpoint.com/sites/default/files/pfpt-us-tr-report-ponemon-impact-cyber-insecurity-healthcare.pdf



Threat Landscape in DACH Healthcare

Healthcare providers across Germany, Austria, and Switzerland face an increasingly hostile cyber threat environment. Public and private medical institutions, insurers, and health IT platforms are targeted not only for financial gain, but also for their critical role in national infrastructure. In recent years, cyberattacks have escalated in both frequency and sophistication, with phishing and ransomware topping the list of threats [1].

Top Attack Vectors in the Sector



1. **Phishing & Credential Theft:**
   Email-based attacks are the most common entry point. Medical and administrative staff are frequently targeted with phishing emails impersonating labs, HR departments, insurers, or even internal IT. Many of these lures are tailored to local languages (German, French, Italian), increasing their effectiveness.

2. **Ransomware Attacks:**
   Hospitals and clinics have been hit hard by ransomware. Attackers exploit unpatched systems or use stolen credentials to deploy malware that encrypts critical files and demands payment. These attacks can shut down entire hospital operations, delay surgeries, or force rerouting of emergency services [2].

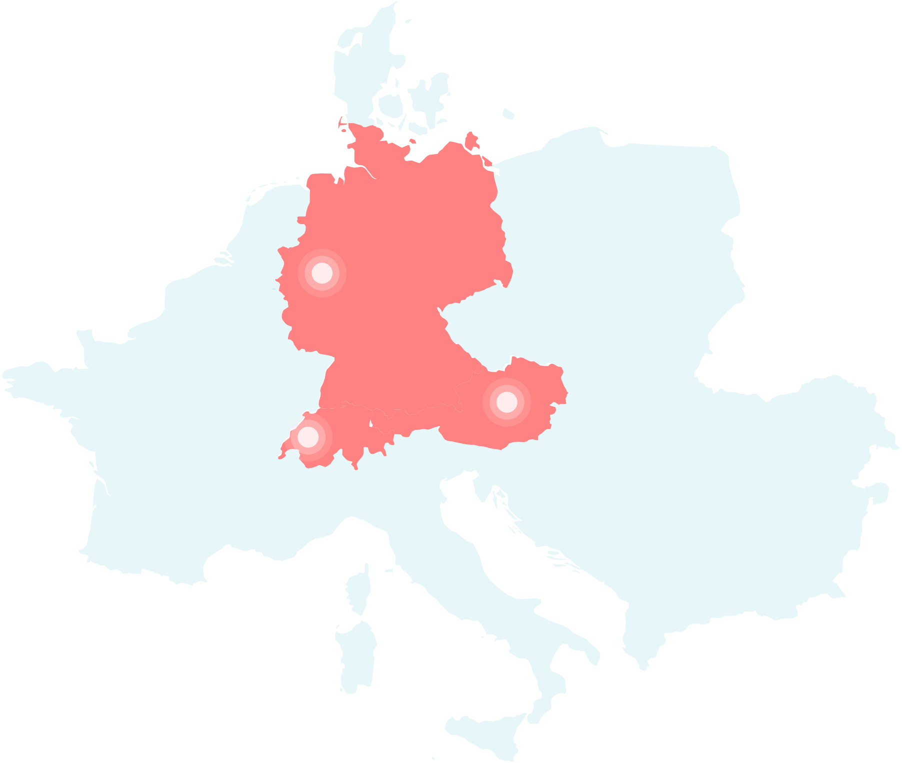
3. **Email Fraud & Business Email Compromise (BEC):**
   Cybercriminals increasingly use social engineering to impersonate executives, vendors, or public institutions. In 2023, several German clinics reported payroll redirection scams—where attackers tricked HR departments into sending salaries to fraudulent accounts [3].

Real-World Incidents in the DACH Region

🇩🇪 **Düsseldorf University Hospital (Germany, 2020):** A ransomware attack forced the hospital to shut down emergency care systems. One patient died after being redirected to another facility—an incident that drew global attention to the physical dangers of cyberattacks [4].

🇦🇹 **Healthcare Insurer Attack (Austria, 2023):** Multiple Austrian health insurers were targeted in a phishing campaign impersonating government COVID information. Thousands of credentials were stolen, some leading to attempted billing fraud [5].

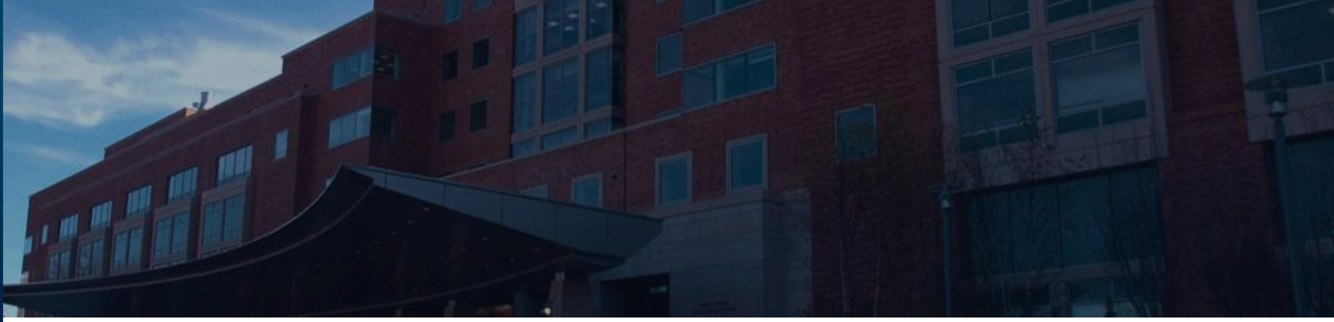
🇨🇭 **Swiss Medical Center Disruption (Switzerland, 2022):** A small clinic in Vaud suffered a data breach that exposed patient treatment files, prompting a full data protection audit and patient notification round [6].



The Growing Threat

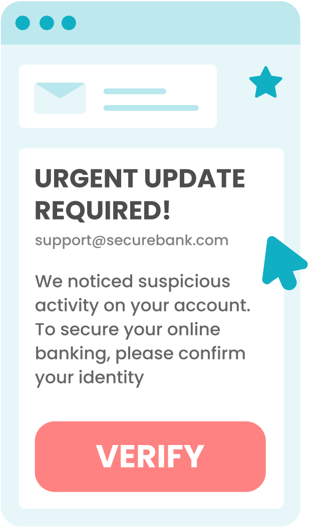
According to ENISA, the healthcare sector was the second-most targeted industry in Europe in 2023. **The German BSI noted a 92% increase in reported cyber incidents in healthcare between 2021 and 2023** [1][7]. The rise in connected medical devices and remote access solutions—accelerated by COVID-era digitization—has further expanded the attack surface.

1. **ENISA Threat Landscape 2023** – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
2. **BSI IT Security Situation Report 2023** – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
3. **CERT.at Annual Report 2023** – https://www.cert.at/assets/files/docs/report_2023.pdf
4. **BBC News: "German hospital cyber-attack led to patient death"** – https://www.bbc.com/news/technology-54204356
5. **Der Standard (Austria): "Phishing-Welle trifft Gesundheitskassen"** – https://www.derstandard.at/story/2000133703346/phishing-welle-trifft-oesterreichische-gesundheitskassen
6. **RTS Info (Switzerland): "Cyberattaque contre un centre médical vaudois"** – https://www.rts.ch/info/regions/vaud/13224936-cyberattaque-contre-un-centre-medical-vaudois.html
7. **BSI: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung** – https://www.bsi.bund.de/DE/Themen/Kritische-Infrastrukturen/Gesundheitsversorgung



Phishing: Still the Top Entry Point

Despite advances in cybersecurity technology, phishing remains the leading initial access vector in healthcare-related cyber incidents. Attackers understand that technical defenses—such as spam filters or endpoint protection—can be bypassed with well-crafted emails targeting human psychology. In high-pressure medical environments, where staff handle dozens of messages per day, this tactic continues to yield results.



URGENT UPDATE REQUIRED!

support@securebank.com

We noticed suspicious activity on your account. To secure your online banking, please confirm your identity

FAKE EMAIL

Social Engineering Cues

- **Urgency**
  pushes immediate action
- **Branding**
  masquerades as legitimate entity
- **Language**
  uses the recipient's native language
- **Name Match**
  contains familiar-looking email

Why Phishing Works in Healthcare

1. **Impersonation of Trust Sources**
   Phishing emails often mimic trusted senders—such as labs, HR, government agencies, or even internal IT departments. Attackers use real logos, local domain names, and urgent subject lines (e.g., "New COVID Protocol Update") to trigger compliance without scrutiny.

2. **Multilingual and Role-Based Targeting**
   The DACH region's multilingual nature (German, French, Italian, English) is frequently exploited in phishing lures. In 2023, Switzerland's NCSC reported phishing attacks that adapted to the recipient's preferred language—dramatically increasing click rates [1].

**Similarly, attackers tailor messages based on professional roles. Doctors may receive phony lab result alerts; administrative staff may get fake invoice requests; IT staff might see simulated security alerts.*

3. **Bypassing Technical Controls**
   Many phishing campaigns use techniques like:

- **Spoofed domains** that resemble legitimate healthcare senders;
- **No payload strategies** (e.g., pure credential harvesting);
- **QR code phishing**, increasingly used to bypass email filters.

**These methods easily slip past perimeter defenses and rely on human error for success* [2].

Example Techniques Observed

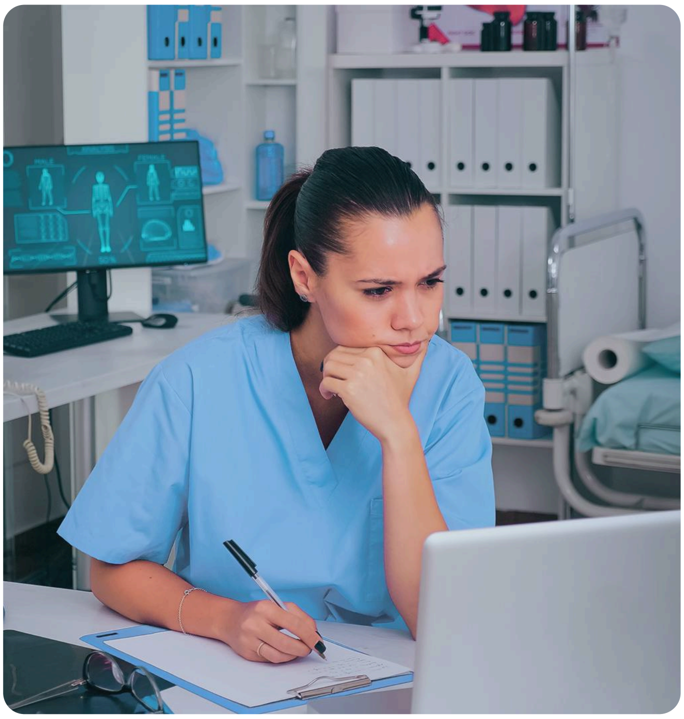
Fake Appointment Confirmations
Sent to nurses or administrative staff, requesting login to verify patient scheduling.

Credential Harvesting Pages
Redirected staff to fake login portals using real hospital branding.

QR Code Phishing
Phishing emails with QR codes claiming to link to secure patient portals or vaccination updates.

A Persistent Threat

According to the SANS 2023 Security Awareness Report, **32% of healthcare organizations rate phishing and credential theft as their most serious cybersecurity concern**—above ransomware and insider threats [3]. Meanwhile, the Verizon DBIR shows that **over 60% of phishing emails in healthcare bypass existing technical controls**, making human response the critical line of defense [4]. These findings reinforce the urgency for continuous, scenario-based training—especially in healthcare, where phishing can lead to both data loss and patient safety consequences.



1. **Swiss NCSC Annual Report 2023 –** https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/reports/annual-reports.html
2. **ENISA Threat Landscape 2023 –** https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. **SANS 2023 Security Awareness Report –** https://www.sans.org/blog/2023-security-awareness-report
4. **Verizon Data Breach Investigations Report 2023 – Healthcare Sector Insights –** https://www.verizon.com/business/resources/reports/dbir/

The Cost of Inaction

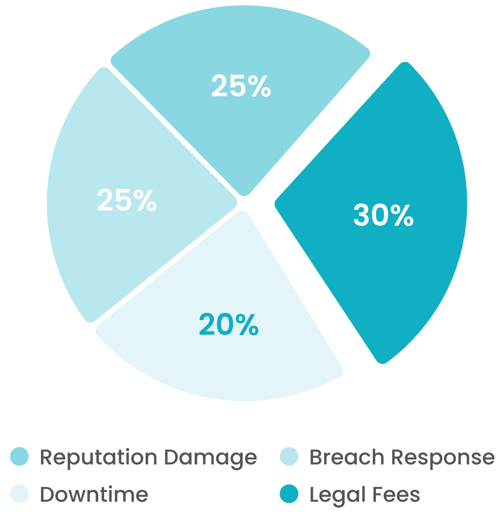
The consequences of a successful cyberattack in healthcare go far beyond financial loss. In the DACH region, the combination of regulatory pressure, public accountability, and patient safety risks makes the cost of doing nothing alarmingly high.

A Persistent Threat

The average cost of a data breach in the European healthcare sector is estimated at **€4–6 million per incident**, factoring in response efforts, downtime, legal expenses, and long-term reputational damage [1]. This figure can escalate in larger hospital groups or cross-border incidents, where coordination and recovery take longer.

In 2022, a ransomware attack on a mid-sized clinic in Bavaria resulted in a **€1.2 million recovery bill**, including emergency IT services, system rebuilds, and delayed patient operations [2]. Insurance covered only a portion of the damages, and premiums increased substantially afterward.

Cost Breakdown of a Healthcare Data Breach



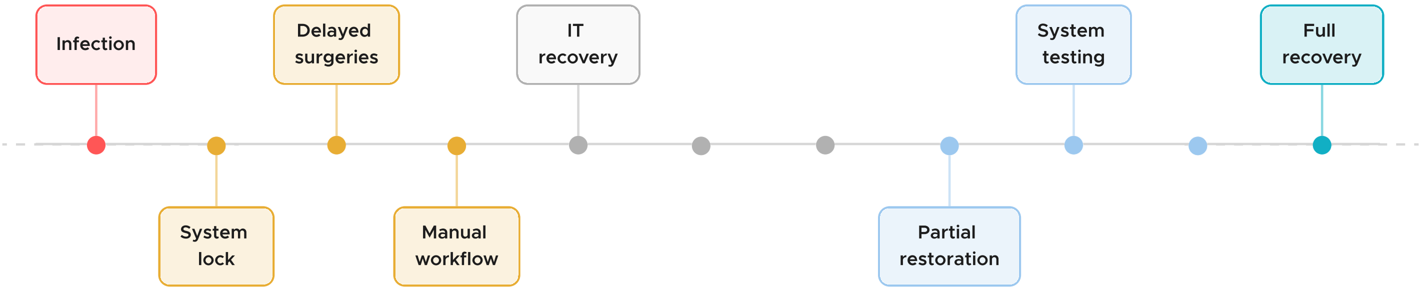
Regulatory Fines & Legal Exposure

Under the EU General Data Protection Regulation (GDPR) and national privacy laws (e.g., BDSG in Germany, DSG in Switzerland), healthcare providers are required to report breaches promptly and demonstrate adequate preventive measures—including staff training.

Failure to comply can lead to fines of **up to €20 million or 4% of global turnover**, whichever is higher [3]. Several German healthcare institutions have faced six-figure fines for insufficient breach handling or failure to train staff on data protection [4].

Operational Disruption & Patient Safety

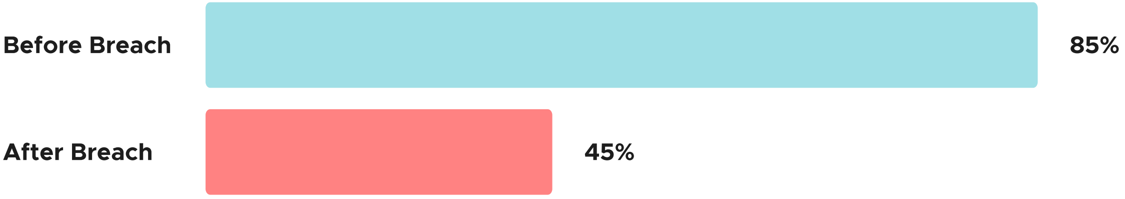
Cyberattacks often cause IT system outages that halt clinical operations. In one 2023 case in Austria, a ransomware infection forced a hospital to revert to paper-based workflows for 11 days, delaying surgeries, lab work, and patient intake [5]. In severe cases, these disruptions can endanger lives. The 2020 ransomware attack on Düsseldorf University Hospital led to the redirection of emergency patients—one of whom died in transit [6].



Hospital Outage Timeline (Day 1–11)

Reputational Damage & Insurance Fallout

Patients expect their medical records to be protected with the highest standard of care. Public reporting of breaches—now required in most cases—damages trust and can lead to patient loss, legal complaints, or negative press cycles. Insurers, meanwhile, are tightening cybersecurity requirements. Healthcare organizations without proper awareness training and incident response protocols may see reduced coverage or denied claims, especially in the wake of repeated incidents [7].



Trust Meter: Confidence Before vs. After a Breach

1. IBM Cost of a Data Breach Report 2023 – Healthcare Sector – https://www.ibm.com/reports/data-breach
2. Heise Online: "Ransomware-Angriff auf Klinik in Bayern" – https://www.heise.de/news/Ransomware-Angriff-auf-Klinik-in-Bayern
3. GDPR Text – Article 83 – https://gdpr-info.eu/art-83-gdpr/
4. BfDI Annual Report 2022 – https://www.bfdi.bund.de/DE/Service/Publikationen/Taetigkeitsberichte/
5. ORF.at: "Spitalsbetrieb nach Cyberangriff tagelang gestört" – https://orf.at/stories/3293602/
6. BBC News: "German hospital cyber-attack led to patient death" – https://www.bbc.com/news/technology-54204356
7. SwissRe Institute: Cyber Insurance in Healthcare: A Hardening Market, 2023 – https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html

Building a Human Firewall:
The Role of Awareness Training

While firewalls, endpoint protection, and email filters remain vital, they are no longer sufficient to stop sophisticated phishing attacks. In healthcare, where frontline staff make split-second decisions and interact daily with sensitive data, people are the new perimeter. Cybersecurity awareness training empowers these individuals to become proactive defenders—forming what experts call a **"human firewall."**

Key Components of an Effective Awareness Program

1. Simulated Phishing Campaigns

Realistic simulations help staff identify common phishing techniques—without exposing systems to real risk. Over time, this exposure trains instinctual caution and improves reporting behavior.

**Organizations that conduct phishing simulations every 4–6 weeks see up to 67% fewer real-world phishing clicks* [1].

2. Role-Based Microlearning Modules

Short, targeted training tailored to job roles (e.g., admin, clinicians, IT) improves relevance and retention.

**Healthcare staff who receive role-specific training are 45% more likely to recognize and report phishing attempts* [2].

3. Behavioral Analytics

Advanced platforms track training completion, click rates, and behavioral change over time. These insights can help organizations adapt programs to address high-risk groups or common mistakes.

4. Localized & Multilingual Content

DE FR IT EN

In multilingual environments like DACH, offering training in native languages (DE/FR/IT/EN) dramatically improves participation rates.

**Lucy Security reports a 60% higher completion rate in multilingual healthcare deployments* [3].

Culture Change Starts With Awareness

Technical controls may stop malware, but only people can stop manipulation. Building a culture where staff feel responsible for cyber hygiene and comfortable reporting suspicious activity is the foundation of long-term security.

This requires leadership buy-in, communication, and reinforcement—not just one-time training. Hospitals and insurers that integrate awareness into onboarding, compliance programs, and leadership briefings are better equipped to detect and respond to threats early.

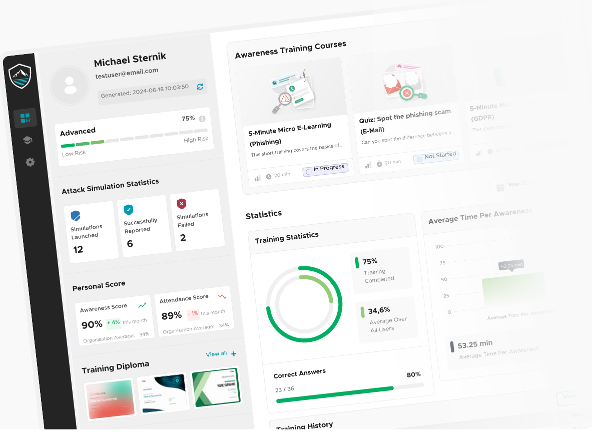
> “Security awareness is not a one-off campaign. It’s an ongoing effort to embed cyber hygiene into daily routines and decision-making at all levels of healthcare.”
>
> —ENISA Threat Landscape for Healthcare, 2023 [1].

Schedule a demo of LUCY Awareness today

enquiries@lucysecurity.com

www.lucysecurity.com

Schedule a Demo


Michael Sternik
testuser@email.com
Generated: 2024-06-18 10:03:50
Advanced
75%
Low Risk
High Risk
Attack Simulation Statistics
Simulations Launched 12
Successfully Reported 6
Simulations Failed 2
Personal Score
Awareness Score 90% + 4% this month
Organisation Average: 34%
Attendance Score 89% - 1% this month
Organisation Average: 34%
Training Diploma
View all
Awareness Training Courses
5-Minute Micro E-Learning (Phishing)
This short training covers the basics of...
20 min
In Progress
Quiz: Spot the phishing scam (E-Mail)
Can you spot the difference between a...
20 min
Not Started
5-Minute Mic (GDPR)
Statistics
Training Statistics
75% Training Completed
34,6% Average Over All Users
Correct Answers 80%
23 / 36
Average Time Per Awareness
100
75
50
25
0
53.25 min
53.25 min Average Time Per Awareness
Training History

[1] ENISA Threat Landscape for Healthcare, 2023 – https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
[2] SANS 2023 Security Awareness Report – https://www.sans.org/blog/2023-security-awareness-report
[3] Lucy Security Customer Deployment Data, 2024 – https://lucysecurity.com

Actionable Checklist:
10 Steps for DACH Healthcare Providers

With phishing, ransomware, credential theft, and social engineering targeting healthcare across the DACH region, security awareness must be practical, role-specific, and continuous. The following checklist outlines essential actions to reduce risk and strengthen staff as the first line of defense.

1. **Localize Training and Simulations in Native Languages**
   Tailor all content and simulated phishing messages to German, French, Italian, and English. Multilingual delivery ensures comprehension and supports inclusion across diverse healthcare teams.

2. **Tailor Content to Specific Roles (Admin, Clinical, IT, Executives)**
   Different job functions face different lures. Train based on real-world scenarios, such as fake discharge papers for nurses or fraudulent vendor messages to procurement teams.

3. **Establish a High-Frequency Training Cadence (Monthly Microlearning)**
   Deliver concise, monthly training modules to keep staff engaged and updated on emerging threats like social engineering, ransomware, and MFA manipulation. Frequent repetition builds long-term behavioral change.

4. **Run Phishing Simulations Every 4–6 Weeks**
   Expose staff to simulated attacks regularly. Use varied tactics such as spoofed logins, document lures, or reply-to phishing to reflect actual attack patterns.

   **Healthcare organizations that simulate phishing frequently experience up to 67% fewer real-world incidents* [1].

5. **Encourage Fear-Free Incident Reporting**
   Make it easy and culturally safe for staff to report suspicious activity. Reinforce that even mistaken clicks should be shared early—speed of response is key.

   **Positive reporting cultures see 3× higher incident detection rates* [2].

6. **Embed Awareness into Onboarding and Compliance**
   Integrate phishing awareness and data protection basics into onboarding. Reinforce topics through GDPR-aligned compliance training and periodic refresher requirements.

7. Use Simulations That Reflect Real-World Threats (e.g., QR Codes, BEC, Medical Lures)

Phishing simulations should mirror what attackers are actually using—**QR code phishing, business email compromise (BEC), fake appointment systems, and spoofed vaccination alerts**. The more familiar the context, the more effective the training.

8. Monitor Participation and Risk Trends Across Roles and Teams

Use dashboards to track simulation results, training completion, and phishing click rates by department. Identify outliers and reinforce targeted improvement.

9. Align Campaigns with Emerging Threats (Ransomware, Insider Risk, MFA Bypass)

Develop seasonal or thematic awareness campaigns on pressing threats like **ransomware, privileged access abuse, or social engineering against support staff.**

10. Ensure Executive Involvement and Visibility

Executives and department heads should participate in training, communicate its importance, and model secure behavior. Leadership engagement boosts program credibility and reach.

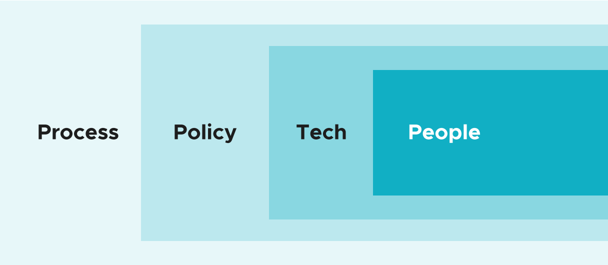
A strong awareness program doesn't just prevent phishing—it builds organizational resilience. By increasing training frequency, simulating realistic attacks (like QR code fraud or medical impersonation), and engaging staff across all roles and languages, DACH-region healthcare providers can proactively reduce their human risk factor.

> Awareness is no longer optional—it's operational defense.

1. **SANS 2023 Security Awareness Report –** https://www.sans.org/blog/2023-security-awareness-report
2. **Lucy Security Internal Benchmarking Data, 2024 –** https://lucysecurity.com

Complementary Measures for a Resilient Defence

While awareness training significantly reduces human risk, it is most effective when integrated into a broader cybersecurity ecosystem. For DACH-region healthcare providers, combining people-centric strategies with strong technical controls, governance, and policy integration creates a multilayered defence capable of withstanding modern threats.



1. Strengthen Technical Defences

Awareness must be supported by robust technical safeguards that reduce exposure and stop threats before they reach users.

Advanced Email Filtering & Threat Detection

Use AI-driven email security platforms that scan for malicious links, spoofing patterns, and attachments before delivery.

Multi-Factor Authentication (MFA)

Enforce MFA across all remote access and email systems to block credential-based attacks—even if passwords are compromised.

Endpoint Protection and Patch Management

Maintain real-time endpoint monitoring and regular patch cycles, especially on older clinical systems that may be vulnerable.

Network Segmentation

Isolate sensitive medical devices and patient data repositories from general-use systems to limit lateral movement in the event of a breach.

2. Align with Recognised Security Frameworks

Establish governance models based on widely accepted standards to ensure that awareness and technology measures are well-documented and auditable.

BSI IT-Grundschutz (Germany)

Incorporates security awareness as a requirement and emphasizes integrated, risk-based protection measures [1].

ISO/IEC 27001

Adopt controls related to awareness (Annex A.7) as part of your information security management system.

NIS2 Directive Preparation

For applicable entities, prepare to demonstrate both technical and organizational security measures under new EU regulations entering into force by 2025 [2].

Cybersecurity Requirements in DACH: ISO/IEC 27001, BSI IT-Grundschutz, NIS2

Control Area	ISO/IEC 27001:2022	BSI IT-Grundschutz	NIS2 Directive
Awareness Training	🟡 Staff must be aware of security responsibilities and consequences of breaches (Clause 7.3, A.6.3). [4]	🟡 Awareness training is a foundational measure (Standard 200-2). [5]	🔴 Article 21(2)(e): Training for employees and management. [6]
Risk Assessment	🟡 Must identify, analyze, and evaluate information security risks (Clause 6.1.2).	🟡 Core process for tailoring protection needs.	🔴 Entities must assess and manage cybersecurity risks.
Incident Response	🟡 Must plan, assess, respond, and learn from incidents (Annex A.5.24–A.5.28).	🟡 Defines roles and workflows for incident handling.	🔴 Article 21(2)(d): Response plans, drills, and reporting.
Management Role	🟡 Leadership must support, allocate resources, and ensure ISMS performance (Clauses 5.1–5.3).	🟡 Clear assignment of responsibilities required.	🔴 Article 20(2): Executives must oversee and approve measures.
Documentation	🟡 Maintain policies, procedures, risk assessments, and evidence (Clauses 7.5, 9.1).	🟡 ISMS requires structured and up-to-date documentation.	🔴 Must have documented cybersecurity policies and plans.
Continuous Improvement	🟡 ISMS must be continually improved through audits and reviews (Clause 10.2).	🟡 Ongoing review and optimization of controls is expected.	🟢 Encouraged to update measures regularly.

🔴 **Mandatory** – Legally enforced; non-compliance leads to legal or regulatory penalties.
🟡 **Required** – Essential for certification or compliance with the standard/framework.
🟢 **Optional** – Strongly advised but not strictly enforced; best practice.

3. Embed Security into Business Continuity Planning

Security awareness should be part of your **incident response and continuity planning**. Simulate phishing-driven incidents and ensure staff understand their roles in managing and escalating threats.

- Include security awareness checkpoints in disaster recovery playbooks.
- Train executive and clinical leadership on communication protocols post-breach.

4. Connect Policy with Culture

Having policies is not enough—they must be understood and enacted by staff.

- Communicate clearly written cybersecurity and reporting policies during onboarding and annual refreshers.
- Reinforce expectations through positive messaging and leadership participation.
- Build awareness into broader quality management and accreditation efforts (e.g., ISO 9001, hospital certifications).

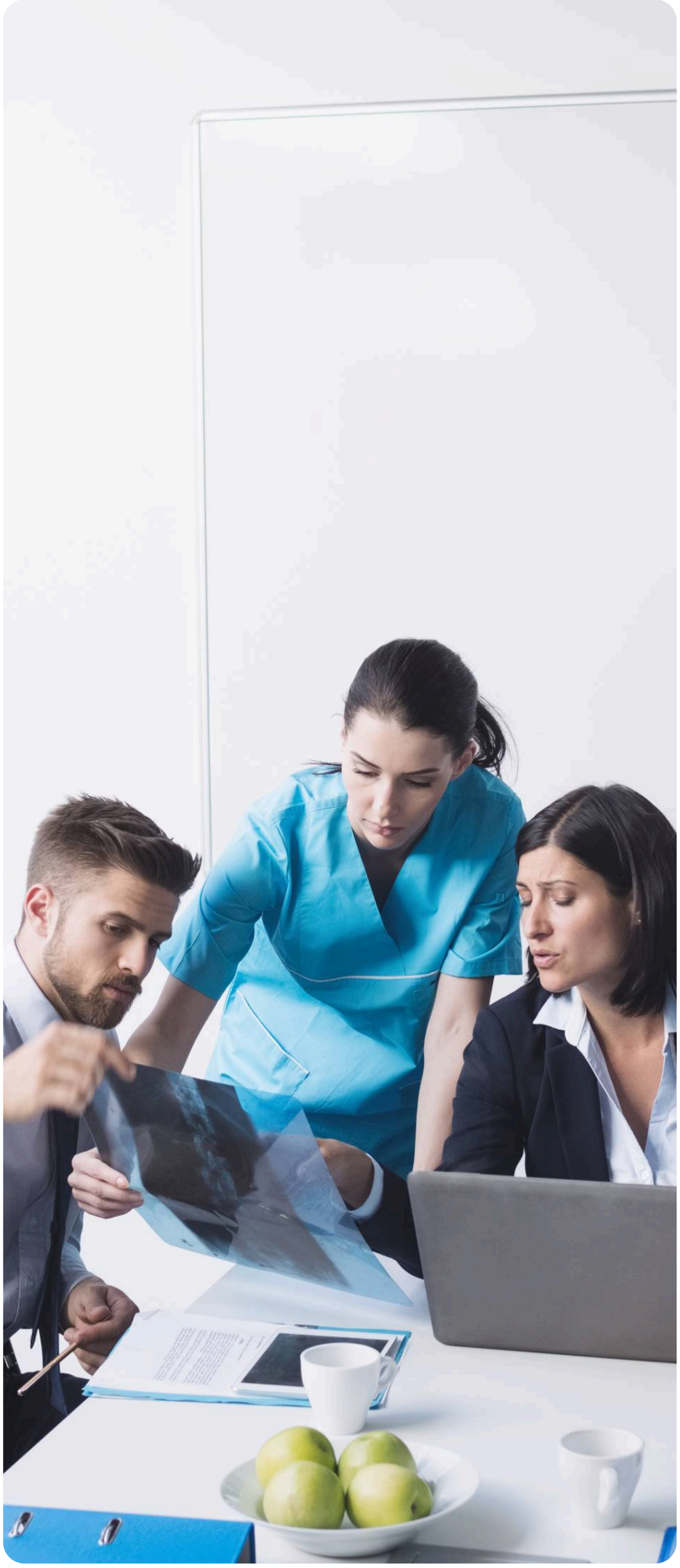
1. **BSI IT-Grundschutz Compendium, Edition 2023 –** https://www.bsi.bund.de/DE/Themen/ITGrundschutz
2. **EU NIS2 Directive Summary –** https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
3. **ISO/IEC 27001:2022 Standard –** https://www.iso.org/standard/27001
4. **ISO/IEC 27001 Clause 7.3 & Annex A.6.3** – ISMS.online
5. **BSI IT-Grundschutz Standard 200-2** – BSI Germany
6. **NIS2 Directive Article 21(2)(e**) – EUR-Lex

Conclusion

Healthcare providers in the DACH region are under increasing pressure—from cybercriminals, regulators, and patients alike. As digitization accelerates, so too does the attack surface. Phishing, email fraud, and social engineering continue to dominate as entry points for cyberattacks—exploiting the one variable that technology alone cannot fully control: human behavior.

Fortunately, this vulnerability is also an opportunity. By investing in structured, localized, and continuous awareness training, healthcare organizations can dramatically reduce their exposure to these threats. Awareness is not a checkbox—it's a strategic capability that builds internal resilience and helps protect patient data, clinical operations, and public trust.

With the average healthcare breach now costing millions of euros and threatening operational continuity, the case for proactive, people-focused cybersecurity has never been clearer. Combined with robust technical controls and leadership support, awareness programs form a scalable, compliant, and cost-effective defense.

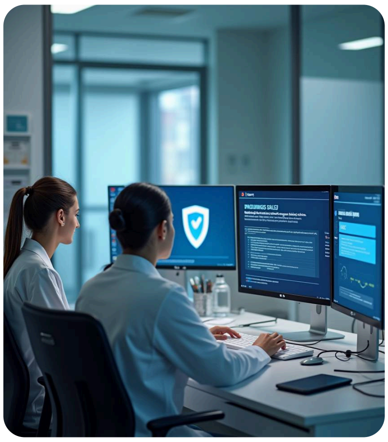


Cybersecurity in healthcare starts with people—and empowering those people starts with awareness.

Sourcing Guide

The Cost-Effectiveness of Awareness

Security awareness is not just a security measure—it's a business enabler. Consider the potential returns:



Lower Insurance Premiums:
Cyber insurers increasingly assess staff training and phishing simulation data when determining coverage levels and premium discounts [1].

Regulatory Readiness:
Proving that your staff is trained and regularly tested on cybersecurity is a defensible position in audits and during post-breach investigations under GDPR, revDSG, or NIS2.

Fewer and Less Severe Breaches:
Studies show that trained staff can reduce phishing success by 60–70%, potentially saving millions in breach costs, legal fees, and system recovery [2].

Improved Staff Confidence and Culture:
Beyond numbers, trained staff are more confident and capable in dealing with threats. This strengthens not only cybersecurity posture but also internal communication and incident response.

Sourcing Awareness Training: Product or Managed Service?

For many healthcare institutions, especially mid-sized hospitals or regional clinics, the choice of how to deliver awareness training is as important as deciding to do it in the first place. Organizations typically choose between two models:

Licensed product (Inhouse Model)

Purchasing your own product licence so you can run a totally personalised program of campaigns, under your own control. In most industries this is purchased in SaaS mode (Software as a Service), hosted by the supplier within the EU. You can also choose to install the product on your own IT infrastructure (On-Premise) and this option is popular in the Healthcare and Banking sectors.
Of course, your supplier may help you operate the system with some Managed Services support but you will often begin to operate it yourself which is becoming very achievable with Automated campaigns and user risk profiling. This approach is generally for larger organizations with their own IS resource, typically >1,000 employees.

Managed Awareness Service (Outsourced Model)

Smaller or resource-constrained organizations may opt for a **fully managed awareness service**—where phishing simulations, reporting, training updates, and even compliance tracking are handled by an external provider. This reduces internal burden while still meeting regulatory and audit expectations. This typically works best for organizations between 10 and 1,000 employees.
Lucy Security and her partners can support you with all three (SaaS, On-Premise and MSP) —giving healthcare providers flexibility based on their security maturity and team capacity.

Lucy Security, for example, offers both deployment options—giving healthcare providers flexibility based on their security maturity and team capacity.

[1] **Swiss Re Institute – Cyber Insurance and Healthcare Risk Models –** https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html
[2] **ENISA Threat Landscape for Healthcare, 2023 –** https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector

Next Step:
What to Look for in an Awareness Solution

Choosing the right awareness training platform or managed service is a strategic decision—especially for healthcare providers where time pressure, multilingual environments, and strict compliance come into play.

Below is an expert-curated checklist of must-have features, grouped by category, to help evaluate solutions that can effectively protect your human layer.

Phishing Simulation & Threat Replication

Support for varied delivery channels	• ✉️ Email • 📱 QR code phishing (scan-and-click attacks) • 💬 Messaging-based lures (WhatsApp, SMS phishing/"smishing") • 💽 Physical device (USB attacks)
Simulation of phishing attack types	• 🔐 Credential harvesting • 🏢 Business Email Compromise (BEC) • 💸 Fake payment/invoice requests • 🦠 Ransomware lures (attachment-based)
Advanced Simulation Features	• 🧪 Clone real phishing from threat intel or real-world inbox attacks into training simulations • 👥 Role-based attack templates (e.g., medical alerts, fake HR notices, IT ticket spoofing)otices, IT ticket spoofing) • © Ability to clone real landing sites to create realistic attacks • 🌍 Localized & multilingual templates (DE, FR, IT, EN) • 📈 Phishing difficulty scaling (beginner to advanced threat realism) • 📆 Automated campaign scheduling (weekly/monthly cadences) • 💣Attack randomization (auto vary the send frequency or choice of attack for realism) • 🚦Risk rating calculations and feedback into generation of subsequent campaigns

Awareness Training & Microlearning

Learning Formats	• ⏱️ Bite-sized modules (5–10 min) for busy clinical and administrative roles • 👩‍⚕️ Role-based learning paths (e.g., clinicians, finance, IT, executives) • 🌐 Multilingual course content tailored to regional healthcare systems
Compliance Alignment	• 📚 Content aligned with compliance frameworks (e.g. GDPR, ISO 27001) • 🧠 Adaptive learning engines based on prior performance or risk • 🧩 Interactive formats: quizzes, scenarios, gamification

Operational, Compliance & Reporting

Flexible deployment options	• 🏢 On-premise hosting for full data control • ☁️ Cloud-based options (EU-hosted) for scalability and ease of use
Analytics & Reporting	• 📋 Audit-ready reporting for GDPR compliance • 📊 Behavioral analytics dashboards to monitor user risk levels, campaign performance, and department trends
End-User Portal Capabilities	• 🔎 View their own risk score or progress • 🎯 Access assigned and optional training modules • 📜 Review simulation history and feedback
Advanced Capabilities	• Integration with identity platforms (e.g., Azure AD, Okta, LDAP) for user management and SSO • Customizable user risk scoring based on behavior, role, and simulation results • Managed service option for organizations without dedicated awareness or SOC teams • Data hosting within EU or on-premise options (for sensitive health data environments)

Culture & Incident Response Support

Support Options	• 🆘 “Report Phish” button integration with email clients (Outlook, Gmail, etc.) • 📄 Post-click education pages (explain what went wrong and why it matters) • 📢 Awareness campaign kits (posters, internal emails, digital signage) • 🧭 Leadership and executive awareness modules • 🕵️ Anonymous or low-friction reporting pathways to reinforce safe behavior

TIP 1:
Choose a provider with experience in regulated healthcare settings, multilingual support, and the ability to replicate real-world attack vectors as part of simulation campaigns.

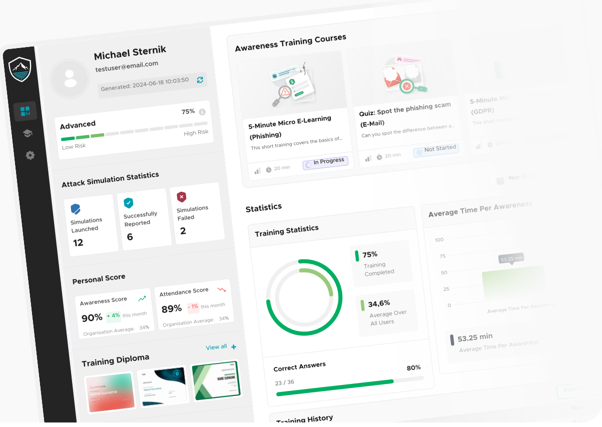
TIP 2:
What to avoid? Licences which bundle loosely associated services (such as Dark web monitoring) in with core Awareness, you will get better value by buying separately.

Schedule a demo of LUCY Awareness today

✉ enquiries@lucysecurity.com

🌐 www.lucysecurity.com

Schedule a Demo



References & Further Reading

Below is a curated list of authoritative sources that informed this report. These include regional cybersecurity agencies, academic studies, EU policy frameworks, and sector-specific threat analyses—all selected for their neutrality, relevance, and credibility in the European healthcare context.

Phishing Simulation & Threat Replication

1. **ENISA Threat Landscape for Healthcare (2023)**
   European Union Agency for Cybersecurity – Sector-specific analysis of evolving threats to healthcare.
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-healthcare-sector
2. **BSI – Die Lage der IT-Sicherheit in Deutschland (2023)**
   Annual cybersecurity report from the German Federal Office for Information Security.
   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
3. **CERT.at Annual Report (2023)**
   Overview of incident trends and response in Austria.
   https://www.cert.at/assets/files/docs/report_2023.pdf
4. **Swiss NCSC Annual Cybersecurity Report (2023)**
   National Cybersecurity Centre of Switzerland – incidents, phishing trends, and recommendations.
   https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/reports/annual-reports.html
5. **Verizon Data Breach Investigations Report – Healthcare Sector Insights (2023)**
   Global threat patterns and breach data focused on healthcare organizations.
   https://www.verizon.com/business/resources/reports/dbir/

Regulatory & Policy Frameworks

1. **General Data Protection Regulation (GDPR) – Article 83**
   Details on breach reporting obligations and administrative fines.
   https://gdpr-info.eu/art-83-gdpr/
2. **BSI IT-Grundschutz Compendium (2023)**
   Framework for implementing information security in public and private institutions.
   https://www.bsi.bund.de/DE/Themen/ITGrundschutz
3. **ISO/IEC 27001:2022 – Information Security Management**
   International standard for ISMS, including awareness and training requirements (Annex A.7).
   https://www.iso.org/standard/27001
4. **EU NIS2 Directive – Summary for Critical Entities**
   New obligations for digital and healthcare infrastructure providers in the EU.
   https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Awareness & Human Risk

1. **SANS Security Awareness Report (2023)**
   Survey and analysis of awareness program trends and human-centric security data.
   https://www.sans.org/blog/2023-security-awareness-report
2. **Lucy Security Benchmarking & Simulation Data (2024)**
   Aggregate performance metrics from healthcare-focused phishing simulations and training engagement.
   https://lucysecurity.com
3. **Swiss Re Institute – Cyber Insurance in Healthcare: Risk and Resilience Trends (2023)**
   Insight into how training and preparedness influence insurance coverage and premiums.
   https://www.swissre.com/institute/research/topics-and-risk-dialogues/technology/cyber-risk.html

LUCY
AWARENESS