



RSM Switzerland

A partner at your side



CYBERSHIELD ACADEMY



CyberShield Academy

1. Who We Are

We deliver comprehensive cybersecurity solutions designed to help organizations build robust defences against ever-evolving threats. Our approach emphasizes education, preparedness, and policy standardization—helping you safeguard your digital assets while enhancing your team's security awareness.

Did You Know?

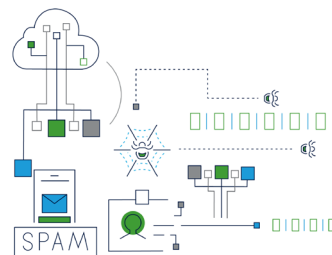
- 82% of data breaches involve a human element—such as errors, misuse, or social engineering tactics—according to the Verizon 2022 Data Breach Investigations Report.¹
- Organizations that implement regular cybersecurity awareness training can reduce phishing susceptibility by up to 75%, as shown in a study by KnowBe4.²
- A 2024 survey by Hornet security revealed that 78.5% of organizations believe IT security awareness training directly prevented cybersecurity incidents.³
- Research published in the ISACA Journal indicates that companies can achieve a return on investment (ROI) of up to 500% from implementing cybersecurity awareness programs—especially in large organizations.⁴

2. Our Core Services

We offer a centralized platform to elevate cybersecurity awareness across your organization. Our system tracks employee engagement and progress in key areas of IT security.

Platform Features

- ✓ Cybersecurity Awareness Training
- ✓ Phishing Simulations
- ✓ Dark Web Breach Monitoring
- ✓ Policy Management & Tracking



¹ Keepnet Labs. (2024, January 23). *2025 Security awareness training statistics*. <https://keepnetlabs.com/blog/security-awareness-training-statistics>

² KnowBe4. (2011, July 11). *New KnowBe4 statistics reveal security awareness training reduces phishing susceptibility by 75%*. <https://www.knowbe4.com/press/security-awareness-training-reduces-phishing-susceptibility-by-75>

³ Hornetsecurity. (2024, June 3). *Security awareness survey: 1 in 4 (25.7%) organizations do not provide I.T. security awareness training*. <https://www.hornetsecurity.com/en/blog/security-awareness-survey-2024/>

⁴ Bhaskar, R. (2022, May 18). *Better cybersecurity awareness through research*. ISACA Journal, 2022(3). <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research>

CyberShield Academy

3. Our Packages

We provide these services through three tailored packages, with optional add-ons to fit your specific industry or business needs (Appendix 1).

01

Starter – Cost Upon Request

- ✓ Platform Setup
- ✓ Standard Phishing Campaign
- ✓ Standard Training Modules
- ✓ Basic Breach Monitoring
- ✓ Policy Storage & Tracking
- ✓ Monthly Automated Reports

Annual License Fee Applies (less than 2 CHF per user per month)

02

Standard – Cost Upon Request

- ✓ Includes all Starter features, plus:
 - 2 Personalized Phishing Simulations based on your company's sector and employee roles

Annual License Fee Applies

03

Premium – Cost Upon Request

- ✓ Includes all Standard features, plus:
 - Advanced Breach Monitoring (Breach Pro)
 - 1-Hour Quarterly Report Debrief with an Expert

Annual License Fee Applies

4. Optional Add-Ons (EXTRAS) – Cost Upon Request

In-Person Training (4-Hour Session) (Appendix 2)

- ✓ Tailored Programs: Customized to your industry and team needs.
- ✓ Expert Instructors: Led by seasoned cybersecurity professionals.
- ✓ Topics Include:
 - ✓ Cyber Hygiene Best Practices
 - ✓ Social Engineering Awareness
 - ✓ Secure Password Management
 - ✓ Incident Response Procedures

CyberShield Academy

Custom Phishing Simulations

- ✓ Designed around your business sector and employee workflows.
- ✓ Includes targeted emails, landing pages, tracking, and analysis.

Policy Writing & Deployment

- ✓ Identify policy needs based on best practices and standards (e.g., ISO 27001).
- ✓ Co-develop and validate policies with leadership.
- ✓ Distribute policies and track employee acknowledgment.

SSO Integration Support

- ✓ Coordinate with your IT team or third-party providers to implement Single Sign-On (SSO) across platforms.

5. Why Choose Us?

- ✓ 20+ Years of Expertise in Cybersecurity
- ✓ End-to-End Services from Prevention to Response
- ✓ Scalable Solutions for SMBs to Enterprises
- ✓ Proven Impact: Reduced phishing incidents, improved compliance, and lower insurance premiums

CONTACT US!

Scan this QR code and contact us directly on our website.



About RSM

RSM Network

Global strength that reinforces our Swiss delivery

From Switzerland, RSM operates locally while leveraging the reach and capabilities of the RSM international network. This allows our teams to apply international standards and access specialised expertise whenever needed, without losing proximity or local leadership.

- Firms in **120 countries** with presence in each of the **top 40 major business centres** worldwide
- **56,000+** professionals globally
- **500+** offices across the Americas, Europe, MENA, Africa and Asia Pacific



56,000
People worldwide



500
Offices



120
Countries

RSM Switzerland

Swiss expertise, rooted in the local economic fabric

Operating across Switzerland, RSM supports Swiss SMEs, mid-sized companies and large organisations with audit & assurance, tax and consulting services. Our teams have a strong understanding of the Swiss regulatory, economic and entrepreneurial environment, bringing clarity and reliability to every engagement.

A single Swiss point of contact, connected globally

We know that time is precious. Your dedicated Swiss contact coordinates your needs locally and acts as your central interface, ensuring smooth collaboration and efficient delivery, while remaining close to your business realities.

Tailored solutions for Swiss businesses

Through close client relationships and strong sector knowledge, we deliver practical and tailored solutions.

Our approach helps organisations improve efficiency, manage risks and support sustainable growth in Switzerland and beyond.

Our presence in Switzerland



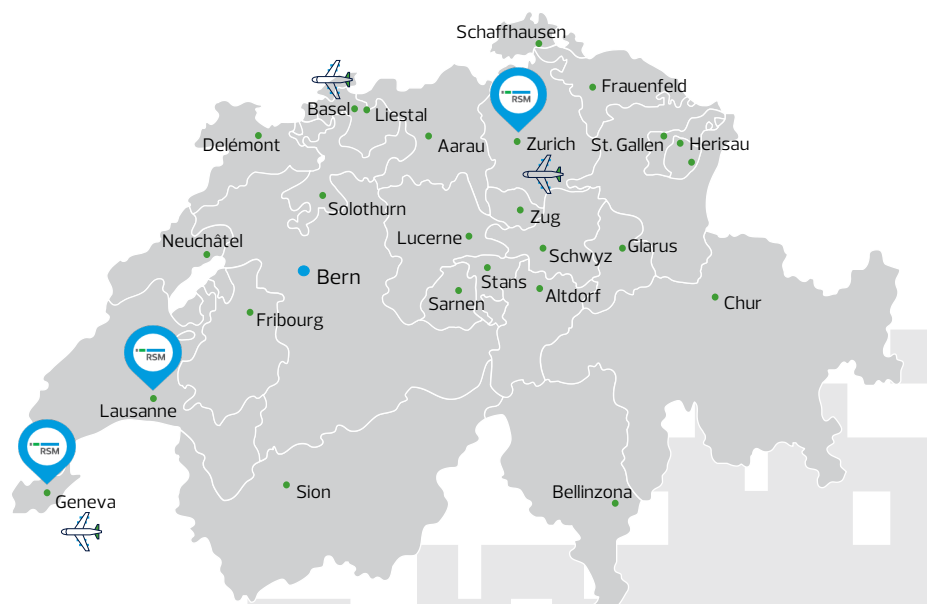
3
Offices



13
Partners



140+
People





LIST OF THE AVAILABLE PACKAGES AND FEES (APPENDIX 1)

	Offer			
	Starter	Standard	Premium	Extra
Set-up	x	x	x	-
Phishing	x	x	x	-
Training	x	x	x	-
Breach Check	x	x	x	-
Policy Storage	x	x	x	-
Monthly Automated Report	x	x	x	-
Annual Licenses Follow-up	x	x	x	-
2 Personalized Phishing related to employee activities/company sector	-	x	x	-
Breach Pro Insight	-	-	x	-
1h report debrief per quarter	-	-	x	-
In person training Half day	-	-	-	Upon request
Personalized Phishing relate to employee activities/company sector	-	-	-	Upon request
Policy writing	-	-	-	Upon request
SSO connexion	-	-	-	Upon request
TOTAL	Upon request	Upon request	Upon request	

CYBERAWARENESS TRAINING PLAN (APPENDIX 2)

	Start Time	End Time	Period
Welcoming	8:30	9:00	0:30
Introduction <ul style="list-style-type: none"> • Trainer introduction and icebreaker • Training goals & expectations • Agenda walkthrough 	9:00	9:15	0:15
Cyber Threat Landscape <ul style="list-style-type: none"> • Why cybersecurity matters (real-world impact) • Common cyber threats: <ul style="list-style-type: none"> ○ Phishing ○ Malware & ransomware ○ Social engineering ○ Insider threats • Threat trends and evolving risks 	9:15	9:45	0:30
Phishing & Social Engineering <ul style="list-style-type: none"> • How phishing works (email, SMS, voice) • Social engineering tactics and examples • How to detect and report phishing 	9:45	10:15	0:30
Break 1	10:15	10:30	0:15
Passwords, MFA & Account Security <ul style="list-style-type: none"> • Secure password practices • Password managers: how and why • Importance of MFA and how it works • Account recovery traps 	10:30	11:00	0:30
Data Privacy & Protection <ul style="list-style-type: none"> • What is sensitive data? • Data classification & labelling • Legal overview (GDPR, local laws) • How to protect data at work and on the go 	11:00	11:30	0:30
Break 2	11:30	11:45	0:15
Secure Remote Work & Device Security <ul style="list-style-type: none"> • Working from home securely • Using public Wi-Fi safely • Device encryption, USBs, mobile phones • BYOD policies 	11:45	12:15	0:30
Incident Reporting, Q&A, Wrap-up <ul style="list-style-type: none"> • How to report suspicious activity • Incident response overview 	12:15	12:30	0:15
Recap of Takeaways	12:30	12:40	0:10
Final quiz	12:40	13:00	0:20
Q&A + Conclusion	13:00	13:15	0:15
TOTAL			4:45