How to Cyber-Secure Your Business 2026

A digital guidebook packed with practical tips and advice for small and medium-sized tech companies, tailored for both employees and management.

Funded by the European Union

Initiative by

Sweden Secure Tech Hub

SSF

CYBERCAMPUS SVERIGE

Participating partner:

BOSCH

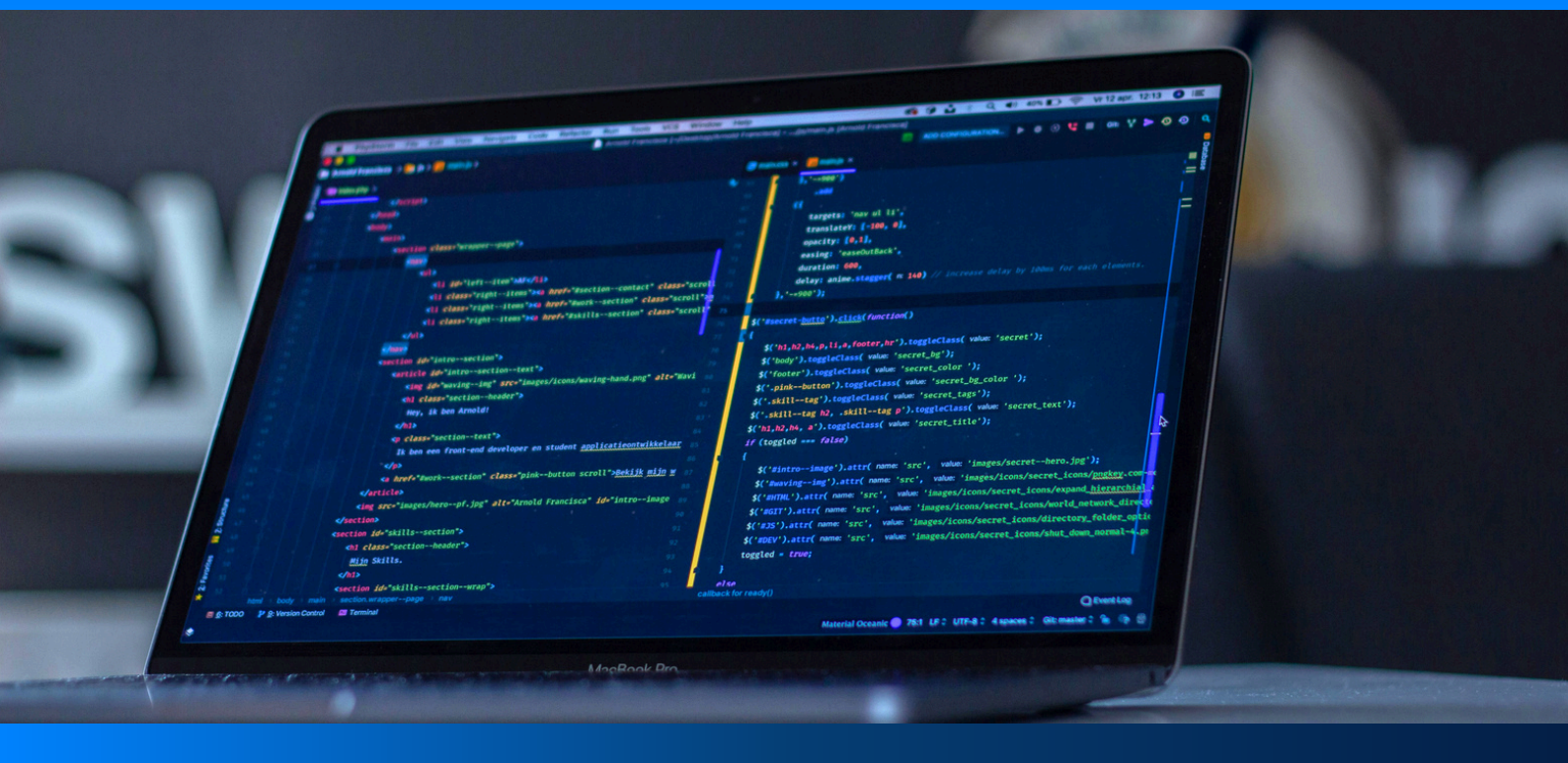


Table of Contents

Background

Cybersecurity has become a critical issue for small and medium-sized businesses. Cyberattacks are becoming increasingly common, and all types of companies are at risk. At the same time, many find it difficult to know where to start, what knowledge is required, and what support is available.

This guidebook has been developed to lower that barrier. The three national organisations Sweden Secure Tech Hub, Stöldskyddsföreningen, and Cybercampus Sverige have jointly taken the initiative to make cybersecurity more accessible and concrete for Swedish companies. Together, they represent research, competence development, and practical security work – a broad and stable foundation to build upon.

The goal is to provide a clear first step. The guide contains practical advice, expert perspectives, and guidance to help companies move forward in their security work. The content is designed to be easy to absorb and possible to put into practice, regardless of where you are today.

The initiative is led by Sweden Secure Tech Hub, Stöldskyddsföreningen, and Cybercampus Sverige, with Bosch as a participating partner. Through their respective experience and expertise in cybersecurity, they have together created content that is both relevant and useful.

When knowledge is shared and organisations collaborate, the conditions for real change are strengthened. The hope is that this guide will inspire more companies to take the next step – and thereby contribute to a safer and more resilient Swedish business community

Sweden Secure Tech Hub

Sweden Secure Tech Hub is a national innovation hub that strengthens the cybersecurity capabilities of small and medium-sized companies in Sweden. The initiative operates in collaboration with Kista Science City, Ideon Science Park, Linköping Science Park, Lindholmen Science Park, Blue Science Park, and Luleå Science Park.

The project is co-funded by the European Union, Region Blekinge, Utveckla Norrbotten, and Västra Götalandsregionen.

Through Sweden Secure Tech Hub, companies gain access to needs analyses, expert advice, testing opportunities, and strong networks. The support is designed to be practical and tailored to each company's needs.

The goal is to make cybersecurity a natural part of the development of products and services. By combining expertise from research, industry, and the public sector, better conditions are created for innovation, growth, and long-term sustainable digital solutions.

BOSCH

BBosch is a global technology and services company with extensive experience developing solutions in areas including industry, mobility, and connected products. The company works broadly with digitalisation and has built strong expertise in cybersecurity over many years.

For small and medium-sized tech companies, this means Bosch can contribute both knowledge and practical support in how security is integrated into products and systems from the outset. This includes identifying risks during the development phase, building security features into the design, and ensuring that solutions meet relevant requirements and standards.

Through its experience with complex systems and international markets, Bosch can also provide guidance on how companies can work systematically with cybersecurity over time. For the target audience, this means reducing vulnerabilities, strengthening customer trust, and creating more robust and competitive products.

Four Steps to Cyber-Secure Your Business

Tips and Expertise

Sweden Secure Tech Hub, in collaboration with Bosch

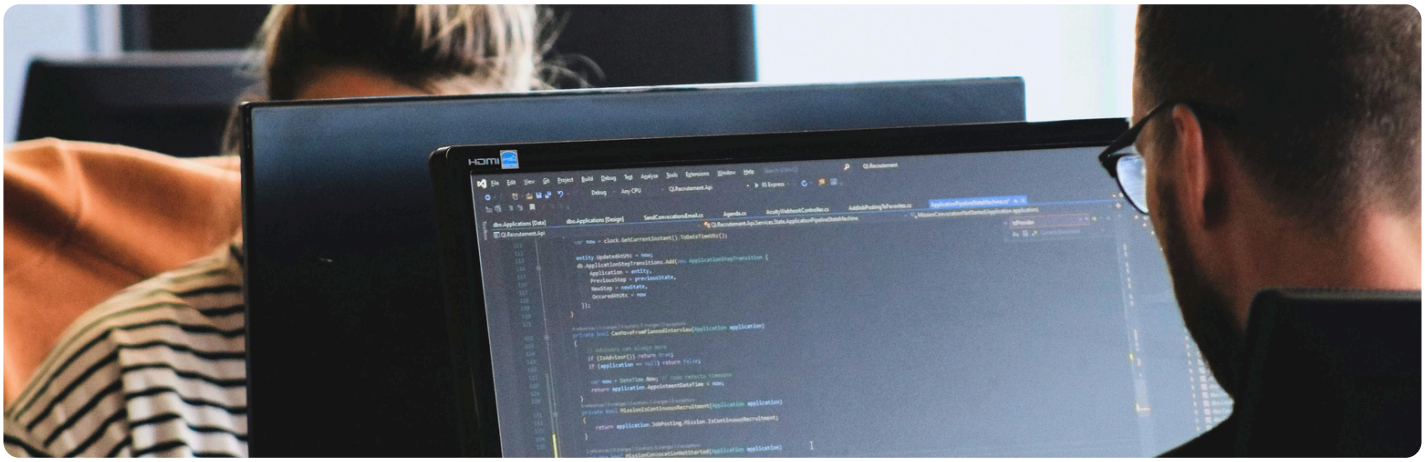
01 Integrate Security Early in the Development Process (Security by Design)

a. Shift Left: Think about security from the start. It is significantly cheaper and more effective to address vulnerabilities during the design and coding phase than once the product is already on the market.

b. Threat Modeling: As early as the design stage, analyse potential threats and vulnerabilities in the product. Identify which attacks are possible and what consequences they may have. This helps you design in security controls from the beginning.

c. Secure Coding Standards: Train your developers in secure coding practices and standards. Ensure that security requirements are part of the specifications for new features.

d. Traceability: Ensure traceability from requirements all the way to test cases and incident management. This helps you resolve deficiencies that emerge late in the process.



02 Implement Robust Testing and Review Routines for Your Products

a. Automated Security Tests: Use tools such as static code analysis in your CI/CD pipeline.

b. Penetration Tests (Pentests): Have external, independent cybersecurity companies perform penetration tests on your products. They simulate attacks from real hackers to find vulnerabilities that your internal tests may miss. This is especially important before launch and at major updates.

c. Secure Coding Standards: Train your developers in secure coding practices and standards. Ensure that security requirements are part of the specifications for new features.

Magnus Alinder, Bosch
Head of Cybersecurity Management and Software Security Engineering

03 Proactively Manage Vulnerabilities and Updates Throughout the Product Lifecycle

a. Vulnerability Management: Establish a process for receiving, validating, and addressing security flaws discovered in your products, whether found internally or reported by customers.

b. SBOM (Software Bill of Materials): If you use third-party libraries and components, ensure you have an SBOM. It lists all components and their versions, making it easier to track vulnerabilities discovered in those components.

c. Secure Update Mechanisms: Ensure your products have a robust and secure mechanism for distributing security updates.

04 Clear Incident Management Processes

a. Incident Response Plan for Products: Have a plan for how you act if a critical vulnerability is discovered in a product already on the market. Key questions: Who is responsible? How is it addressed? How quickly must it be resolved?

Who is responsible? How is it resolved? How quickly must it be done?

Why Should You Seek Support via Sweden Secure Tech Hub?

We interviewed representatives from Innotech Sverige, InnoviGuard, and FixedIT Consulting to hear their perspectives.

What support have you received from Sweden Secure Tech Hub?

Innotech Sverige: SSTH has offered us expert advice and support in our needs analysis. We have also received assistance with testing and validation of our product, particularly regarding cybersecurity aspects.

What challenges did you face?

FixedIT Consulting: Large customers want proof of IT security, often via certifications such as ISO 27001 and SOC2. For startups, these are often too expensive and time-consuming – but simpler documentation such as white papers, gap analyses, or penetration tests are often sufficient.

How do you think support from SSTH will help your development as a company?

Innotech Sverige: Above all, we have high hopes for the cybersecurity report from Orange Cyberdefense, which SSTH helped us get in contact with. The results will be very valuable for us in the future, both at customer meetings and in connection with potential certifications such as ISO 27001.

Why should others seek support?

InnoviGuard: For us, it was a smooth opportunity to get an ISO 27001-style review and gain credibility as a supplier to our customers.

Innotech Sverige: The support provides a fantastic opportunity for a growing company to make a major leap forward in its development, free of charge.

InnoviGuard innotech FIXEDIT

SSF

Stöldsyddsföreningen

By offering relevant and free information, practical support, and tools in the area of cybersecurity, we help small and medium-sized businesses strengthen their cybersecurity. As part of our work, we offer the platform säkerhetskollen.se, aimed at providing guidance and tools for increased security, preventing risks, and standing stronger in a digital reality.

We also conduct webinars with current knowledge and insights. Via our website stoldskyddsforeningen.se, we offer a practical cybersecurity programme in 6 steps, designed to provide a clear structure and support for taking the next step towards a safer and more resilient business.

A Standard for Basic Cyber Hygiene

Businesses that have their cybersecurity under control protect not only their own operations but also create business advantages. At the same time, they contribute to increased security for both customers and suppliers. All businesses should therefore achieve a basic level of cyber hygiene.

At stoldskyddsforeningen.se, you can download our free cybersecurity standard, which contains concrete controls to help businesses of all sizes ensure they meet basic cybersecurity requirements.

A Self-Test That Helps You Get Started

It can be difficult to know how to prioritise and which measures provide the greatest possible effect with the least possible effort. At säkerhetskollen.se, you will find a simple test that helps you “take the temperature” of your business. You immediately get an overview of which measures should be prioritised.

Ongoing News That Keeps You Updated

Some threats are constantly relevant, while others are acute for the moment. Säkerhetskollen.se helps you keep your ear to the ground. There you will find news that both warns of ongoing attacks and provides tips on new measures that help you strengthen your business’s cybersecurity.

Guides That Show How You and Your Colleagues Strengthen Cybersecurity

Many measures are not as complicated as they sound. At säkerhetskollen.se, there are guides that explain how and why you should take simple measures that have a major impact on your business’s cybersecurity. The guides are aimed at both IT staff and other employees.

Webinars That Make You More Cybersecure

SSF also conducts a number of webinars announced on stoldskyddsforeningen.se. The webinars cover topics such as management responsibility and business consequences, getting started without your own cybersecurity expert, and structure and tools for the way forward.

Practical Cybersecurity Programme in 6 Steps

Available through stoldskyddsforeningen.se

01 Getting Started with Structured Cybersecurity Work

Strengthen your ability to prioritise the right measures, distribute responsibility, and create follow-up in your cybersecurity work. The goal is to give you a clear structure that strengthens both security and business.

02 Practical Application of the SSF Cybersecurity Baseline Standard

We provide concrete support in how you translate the requirements of the SSF Cybersecurity Baseline standard (SSF 1101) into practical measures in your business. You begin with a current-state analysis showing where you stand and what you need to prioritise.

03 When Something Happens: Act Correctly

Develop your competence in incident management, data breaches, and business disruptions. Focus is on continuity, responsibility, and how you prepare through simple and effective exercises.

04 Employees: An Important Resource

Technology is one part of security work and people are another. Improve your capacity for making your staff an active part of cybersecurity work and building behaviours that last over time.

05 Safe AI Use in the Business

AI is already used in many businesses but often without governance. Here you strengthen your ability to identify risks, set boundaries, and use AI in a safe and controlled way.

06 Supplier Requirements and Business Value

Do you deliver to a business or municipality covered by the cybersecurity law? Here you gain insights into how cybersecurity can become a business advantage through reduced risk and increased trust – for example through certification.

"Cybersecurity is not a cost but a business advantage. Certification shows that you take security seriously."

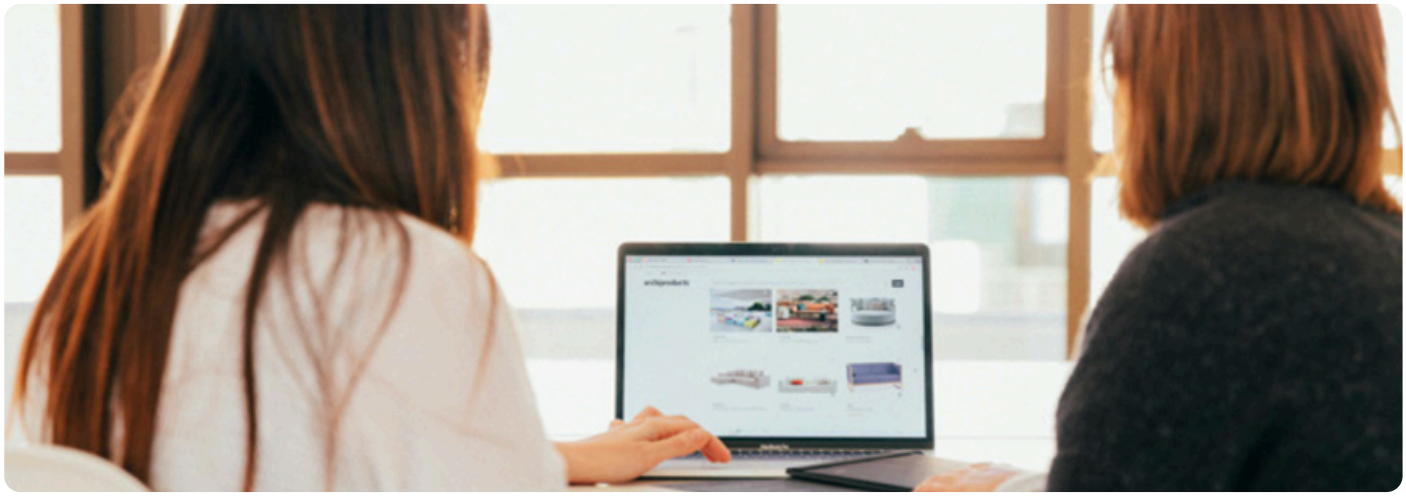
CYBERCAMPUS SVERIGE

Cybercampus Sverige is a Swedish national initiative and collaboration between universities, research institutes, government agencies, and companies.

Cybercampus enables education, research, and innovation in cybersecurity and cyber defence beyond what is possible for a single university, institute, agency, or company. The purpose is to increase the country's cybersecurity, strengthen society's defence capability, and Swedish competitiveness.

Among Cybercampus's partners and members are companies, government agencies, research institutes, and higher education institutions. Small and medium-sized companies are a primary target group for Cybercampus.

Since 97% of the country's companies have fewer than ten employees, it is incredibly important that there are good and tailored opportunities for competence development. New threats and needs require constant updating of skills.



Guide to Competence Development in Cybersecurity

With the right knowledge in cybersecurity, it becomes easier to detect risks in time, prevent incidents, and protect both the company and your customers. It doesn't have to be complicated – but it does require that you invest in the right competence development. Cybercampus Sverige has developed a guide for this.

When you invest in cybersecurity knowledge, you also show that you take security seriously. This strengthens trust among customers, business partners, and suppliers.

01 Define Your Needs

Start by finding out what your specific company needs. All companies have different risks and different conditions. It is therefore important not to start with training directly, but first to understand where the knowledge gaps are. At Cybercampus.se, there is a fillable template that helps you identify areas where you are vulnerable. The answers help you see what knowledge you need. If you want to identify what specialist roles may be needed, you can use EU agency ENISA's competence profiles.

02 Set the Right Level and Have Realistic Expectations

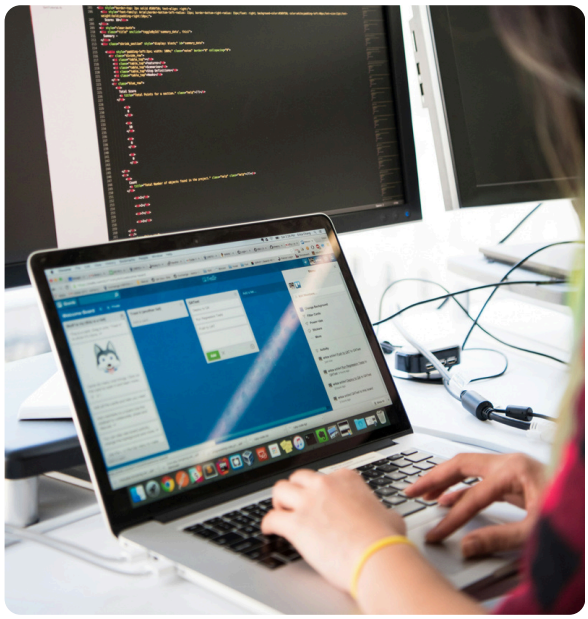
Not everyone in the company needs to become experts in cybersecurity. What matters is that the right people have the right knowledge for their tasks.

Think about what level is reasonable. What does management need, and what do all employees need? When is more in-depth specialist knowledge needed? Is your organisation directly or indirectly covered by the cybersecurity law?

Competence development takes time. Do not expect immediate results, but count on risks decreasing step by step.

03 Create the Right Conditions in the Company

Competence development needs to be prioritised to happen. Responsibility should not lie with the employee – instead, decide who should take which training, when it should take place, and how much time and money can be allocated. Start with the people and areas where the needs are greatest.



04 Match Skills Gaps and the Right Measures

Choose a training initiative that meets the competence needs you have identified. Find out what training is available and how much time it requires, so that it can be combined with your daily operations.

05 Invest in Continuous Training

Cybersecurity is not a one-time project. Threats change, technology evolves, and new ways of working are introduced. Therefore, knowledge needs to be updated on an ongoing basis.

Make competence development a natural part of the business, ideally with a simple training plan that is reviewed regularly. Current and relevant knowledge reduces the risk of incidents – and simultaneously strengthens the company's competitiveness.

06 Follow Up and See What You Have Achieved

It is important to find out what completed training initiatives have actually led to. Has understanding increased, have working methods changed, do employees find it easier to handle risks in everyday life? This follow-up becomes simpler if you set clear goals from the start.

”Många svenska företag befinner sig i dag i ett tidigt skede när det gäller strukturerat cybersäkerhetsarbete. Mognadsbedömningar visar att det ofta saknas tydliga roller, uppföljning och helhetsgrepp, samtidigt som allt fler företag berörs – direkt eller indirekt – av nya EU-regelverk som NIS2 och CRA.

Det handlar oftast inte om bristande vilja, utan snarare om att man inte alltid har full insyn i sitt eget nuläge, ansvar eller vilka krav som faktiskt gäller. Om cybersäkerhet inte är integrerad i affärs- och produktutveckling kan det uppstå gap mellan de risker företaget exponeras för och den organisatoriska beredskapen. Det ökar risken för exempelvis phishing eller ransomware-attacker, och kan leda till förlorad data, förtroendeförlust och ekonomiska bortfall.

När det gäller kompetensutveckling krävs det inte alltid stora eller drastiska insatser. För vissa företag kan expertkompetens vara nödvändig, men för många är det viktigaste att successivt höja den grundläggande kunskapen hos hela organisationen. I Sverige finns ett gott utbud av verksamhetsnära utbildningar.”

Mette Svensson,
Business Developer in Education,
Cybercampus Sverige

Sweden Secure Tech Hub

Your First Step to a Cyber-Secure Business

Are you a company that wants to take your cybersecurity to the next level? We guide you to the right support to drive your business forward and strengthen your security.

Sweden Secure Tech Hub is a national innovation hub that strengthens small and medium-sized companies' capacity in cybersecurity. We want to help your company grow safely and reach new heights. Apply for support via our website today!

Apply at:
swedensecuretechhub.se

Types of Support We Offer

01	Needs Analysis	Our digital quick test provides an overview and identifies development opportunities. We also look at your supply chains to strengthen security and identify areas for improvement.
02	Expert Advisory	Receive tailored guidance to strengthen both product and organisational security, with insights adapted to your industry. We also help you find financing for further measures.
03	Testing and Validation	We test and validate your systems in real time, reduce risks, and strengthen security with specialised training, threat simulations, and certification support.
04	Network	We support you in building strong networks within the cybersecurity ecosystem by mapping key players and facilitating targeted matchmaking with relevant partners.

Co-funded by the European Union

IDEON SCIENCE PARK

LINKÖPING SCIENCE PARK

Swedish Agency for Economic and Regional Growth

BLUE SCIENCE PARK

SCIENCE PARK

Lindholmen Science Park

Kista Science City

REGION BLEKINGE

UTVECKLA NORRBOTTEN
EN DEL AV REGION NORRBOTTEN

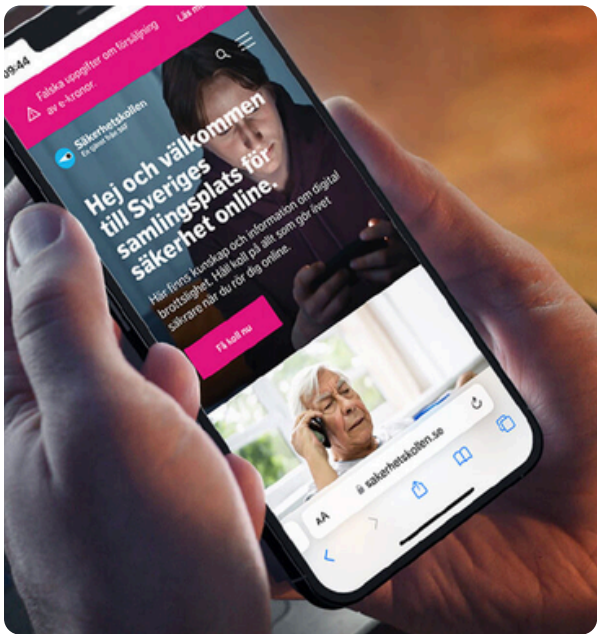
VÄSTRA GÖTALANDSREGIONEN

SSF roll i cybersäkerhetsarbetet

We are named in the government's national cybersecurity strategy and are an important piece in society's overall cybersecurity work. Together with the Police and the National Cybersecurity Centre (NCSC), we have a mandate to develop support in cybersecurity and reduce the number of cybercrimes affecting small and medium-sized businesses. The work is primarily driven by offering free information, advice, and tests on SSF's platform säkerhetskollen.se. The platform targets both IT staff and other employees.

SSF also offers business-adapted cybersecurity training via stoldskyddsforeningen.se, which reinforces and complements the free support at säkerhetskollen.se.

SSF is an independent, non-profit organisation working to prevent crime in support of the general public and private individuals. We do this through free advisory services, the development of security standards, and education.



Types of Support We Offer:

01

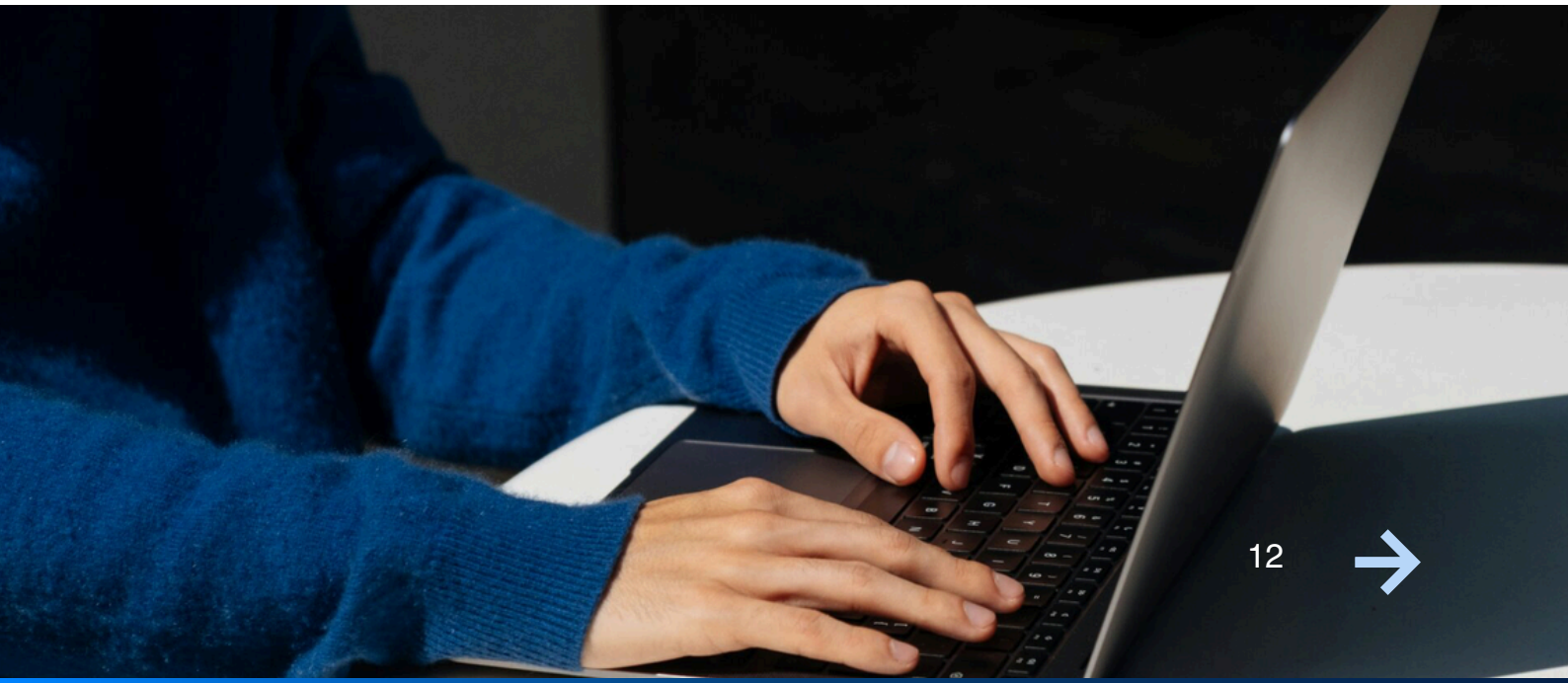
Go to säkerhetskollen.se and test your cybersecurity, and access guides and information.

02

Read more about our business-adapted cybersecurity training at stoldskyddsforeningen.se.

03

Sign up for our webinars via stoldskyddsforeningen.se and strengthen your cybersecurity.



CYBERCAMPUS SVERIGE

Cybercampus works within education, research, and innovation. In education, Cybercampus aims to help shape and offer training that meets the competence needs of different industries and sectors.

There is currently no comprehensive picture of the competence needs in cybersecurity in Sweden. Cybercampus, as the only national coordinating actor, addresses this challenge by acting as a hub – a first entry point for finding relevant cybersecurity training for professionals.

Work on training for professionals takes place in collaboration between Cybercampus's partners in higher education and connects existing offerings around Sweden. Cross-functional competence is often in demand, encompassing both deep technical knowledge and legal aspects and management issues.

AVocational colleges and universities have many opportunities to meet competence needs in the private and public sectors. Where existing training is lacking, new programmes can be created.

Approximately 80% of all Swedish companies request targeted training and business-oriented support, but fewer than 20% train their staff in cybersecurity. Through partner organisations KTH, Linköping University, and RISE, Cybercampus has reached out to Cybernode member companies to find out which subject areas are most important and which training formats are preferred – in order to offer and develop training that suits Swedish companies' needs.

Types of Support We Offer:

01

Help identifying what knowledge and competence your specific business needs.

02

We continuously gather relevant courses in cybersecurity from leading higher education institutions and create course packages and develop new courses.

03

Help matching your needs and maturity level with the right training initiative – if needed, we develop entirely new training programmes.

Contact

Mette Svensson, Business Developer in Education
mette@cybercampus.se
+46 737 652 341

How to Cyber-Secure Your Business 2026

How to Cyber-Secure Your Business 2026 is a practical and accessible guide packed with concrete tips, advice, and insights from cybersecurity experts.

The book has been developed to support small and medium-sized tech companies in strengthening their digital security. It provides guidance on how risks can be identified, managed, and prevented – and how long-term and sustainable protection can be built up.

The initiative is led by Sweden Secure Tech Hub, Stöldskyddsföreningen, and Cybercampus Sverige, with Bosch as a participating partner. Through their respective experience and expertise in cybersecurity, they have together created content that is both relevant and useful. Together they contribute broad experience from research, education, and practical security work.

The content is aimed at both employees and management, and serves as support in the daily work of creating understanding, engagement, and concrete measures throughout the organisation – with the goal of strengthening digital resilience in Swedish tech companies.

Funded by the European Union

Initiativtagare:

Sweden Secure Tech Hub · SSF · CYBERCAMPUS SVERIGE

Medverkande partner

BOSCH