

Guide to Cybersecurity

Accessible version

**Cybersicherheitsagentur Baden-Württemberg
(CSBW)**

Your security. Our mission.

Content

- Guide to Cybersecurity**..... 0
- Cybersecurity. In cooperation with you.** 3
- PASSWORD:** The secret to good passwords. Unique, long, and complex 4
- SECURITY INCIDENT:** Security incident at the office? Every minute counts!..... 6
- WORK FROM HOME:** Working securely from home. Recognising and addressing risk factors 8
- MOBILE WORKING:** Far from security? What to pay attention to when working on the go 10
- EMAIL:** Unknown sender? Proper handling of phishing emails..... 12
- WORKPLACE:** Office risks: Password notes, unknown persons, untidy desks 14
- INTERNET:** Internet and cloud. Blessing and curse at the same time?..... 16
- SOCIAL ENGINEERING:** Manipulation, deception, and fraud 18
- VIDEOCONFERENCES:** “...starting to share my screen” 20
- Glossary** 22
 - A** 22
 - B** 22
 - C** 23
 - D** 24
 - F** 24
 - G** 25
 - H** 25
 - I** 26
 - M** 26
 - N** 27
 - P** 27
 - R** 29
 - S** 29
 - T** 31
 - U** 31
 - V** 32
 - W** 33

Contact..... 34
Cybersecurity emergency response card 35

Cybersecurity. In cooperation with you.

Cyberattacks are constantly on the rise, and the resulting damage is often devastating, potentially threatening the very existence of organisations. Due to this development, the question is not whether you will fall victim to a cyberattack, but when will it happen and how well prepared you are.

In addition to targeted attacks, which are strategically planned and initiated through methods such as phishing emails, there are also less targeted fraud attempts sent indiscriminately to a large group of people, potentially affecting anyone. It is absolutely essential that IT systems are fundamentally secured in both the professional and the employee's personal environments.

But even a cutting-edge technical protection can be ineffective against the largest attack surface: people.

Information security therefore requires a combination of technical measures as well as security-oriented actions and must be approached holistically.

To achieve an appropriate level of protection, users must continuously be trained in security-conscious behaviour and be made aware of threats from cyberspace.

Cybersicherheitsagentur Baden-Württemberg supports the federal state and its citizens on the path to increased cybersecurity and provides them with the necessary knowledge to be prepared for an emergency.

Prevention is the best protection against cyberattacks.

Your security. Our mission.

CSBW Cybersicherheitsagentur Baden-Württemberg

PASSWORD: The secret to good passwords. Unique, long, and complex

Passwords are the key to our data and to our digital lives. Protect your professional and personal data reliably from unwanted access by using a unique and complex password for each of your accounts.

General principles:

- The longer and more complex a password is, the harder it is to crack.
- Never share your passwords with anyone, do not write them down, and always enter them unobserved.
- Immediately replace duplicate, weak, leaked, or default passwords with new, strong passwords.

Recommendations:

- **Combination of different character types:**

Use a mix of uppercase and lowercase letters, numbers, and special characters when creating a password to make it as complex as possible.

- **Use a password manager:**

A password manager is a software tool that helps you generate and manage complex passwords. You only need to remember one complex master password, which gives you access to all your other passwords.

- **Enable two-factor authentication:**

By combining two different components, such as a PIN and a payment card, two-factor authentication provides additional protection against potential attacks.

Useful tips

Use the initial letters of a sentence to create a memorable password:

CSBW: Prevention is the best protection against cyber attackers!

Password: CSBW:Pitbpaca!

Additionally, replace letters with special characters or numbers, e.g., S=\$, b=6:

C\$BW:Pit6paca!

Password manager:

Using a password manager simplifies the process of generating secure passwords and storing them in a database.

SECURITY INCIDENT: Security incident at the office? Every minute counts!

A suspicious incident at the workplace must be reported as quickly as possible to prevent further damage. Immediately inform the designated information security officer, the IT department, or management. Often, there are IT emergency plans set up for exactly these kinds of situations which specify who needs to be informed and when.

Protection objectives of information security:

The most important protection objectives of information security are **confidentiality**, **integrity**, and **availability** of information. Information security is meant to adequately protect all data and systems.

There is a security incident if at least one of the following situations has occurred:

- **Confidentiality** of data is compromised, for example, unauthorised persons gain access.
- **Integrity** of data is compromised, for example, data has been altered without authorisation and unnoticed.
- **Availability** of data is compromised, for example, a system has failed.

General principles:

- **Immediately report** to the IT department if devices such as computers or phones behave in an unusual manner.
- **The earlier an incident is reported, the higher the chance** of preventing serious damage.

- **In case of suspicion, it is better to report too often than too little:** Do not hesitate!

Cyber-Ersthilfe BW of Cybersicherheitsagentur is the central and free contact and reporting point for cybersecurity incidents in Baden-Württemberg.

Call 0711-137-99999 to receive a first assessment and individual action options for your suspected case, available 24/7.

Possible signs of a cyberattack

- Programmes start and close without your intervention.
- Files can no longer be modified or saved.
- The appearance of programme icons has changed.
- The homepage in the web browser has changed.
- The webcam light is on, even though the camera is off.
- The computer shuts down by itself.

Note: Not every symptom listed above is necessarily due to a cyberattack.

WORK FROM HOME: Working securely from home. Recognising and addressing risk factors

Working from home has become normal for many people. Unlike the protected office environment, at home we are responsible for ensuring the security of information.

The following recommendations can help mitigate potential risks:

- Close windows and doors and avoid using loudspeakers for phone calls, as business conversations are not meant for unauthorised ears.
- Always store paper documents locked away.
- Inform those around you that any overheard business information must be treated confidentially.
- Turn off and remove any voice assistant devices from the room while working.
- Do not connect personal devices to your work computer, and do not connect your work phone to your personal computer.
- Lock your screen when leaving your workspace with these shortcuts:

For Windows devices: Windows key + L

For Apple devices: Ctrl + Command key + Q

This prevents unauthorised persons from viewing your screen and stops pets from accidentally deleting or sending data through contact with the keyboard.

- Dispose confidential documents at the office, not in your household rubbish.
- Return outdated IT equipment such as USB sticks to the IT department.

Useful tips

Optimising the configuration of your home router significantly increases the security of your home workspace, for example by setting up a guest network.

A **VPN (Virtual Private Network)** helps you stay anonymous on the internet, maintain privacy, and access networks securely.

Software and virus scanner updates should be installed promptly, and the system should be regularly subjected to a virus scan.

MOBILE WORKING: Far from security? What to pay attention to when working on the go

On business trips or when working remotely, special caution is required with work devices and confidential information. Curious onlookers, thieves, public Wi-Fi access, and lost devices – the dangers are many and ever-present.

When on the move, consider the following:

In public

- Use a privacy screen or sit with your back to a wall to prevent unwanted glances at the screen.
- Use a headset, avoid speaking sensitive information out loud, or postpone the conversation to a later time.
- Paper documents are particularly critical as they contain unencrypted information and can easily be read.
- In some situations, it is better to postpone working. Whether the situation allows for risk-free work is up to your personal judgement.

Public Wi-Fi networks

- Third parties can gain access to transmitted data or inject malware over public Wi-Fi networks. To avoid this, refrain from using public Wi-Fi and disable the automatic connection to Wi-Fi networks on your devices. Only visit SSL-encrypted websites. These start with **https://**
Example: **https://cybersicherheit-bw.de**
- Access work data only through a VPN connection.

Useful tips

Activate all possible security measures to prevent unauthorised access, such as securing your laptop and mobile phone with a password or biometric feature.

If your device is lost, immediately inform the IT department and your supervisor so that access to media and devices can be deactivated remotely.

Before travelling, ensure that software updates are installed and the operating system is up to date.

EMAIL: Unknown sender? Proper handling of phishing emails

Emails are a popular medium for attackers to target systems with malware. It is estimated that more than 80 percent of successful attacks are initiated via email. Phishing emails, which entice recipients to click on links or open attachments, pose a significant security risk.

The following tips can help identify and successfully repel attacks:

- Be particularly cautious with emails from unknown senders. Do not open links or attachments without verification.
- Even emails from known senders should be checked if the content seems unusual or requests sensitive information.
- Often, such emails contain threats of consequences or create a sense of urgency. Do not let yourself be pressured into quick actions.
- Report the email to the appropriate authority at the slightest suspicion and follow their instructions. This could be the designated information security officer or the IT department.
- The contact details provided in the email are often fake and should not be used to contact the sender. Instead, research the official contact details online and inform the supposed sender about the phishing attempt.
- Do not follow instructions to enter login credentials. Instead, open the relevant website through your usual access link to check if any action is genuinely required.

Very important!

Skim through emails in the preview pane before opening them.

Phishing emails are now largely error-free and difficult to distinguish from authentic ones.

Artificial intelligence (AI) is increasingly being used to generate authentic texts in the creation of phishing emails.

Phishing occurs across all text-based messaging channels. Therefore, attacks can also be expected via messenger services and SMS.

WORKPLACE: Office risks: Password notes, unknown persons, untidy desks

Even within the office, we are not completely secure from attacks. These can either occur digitally or through individuals attempting to gain physical access to the office building. Always be aware of your surroundings, identify unfamiliar persons, and actively help to protect your workplace from attacks.

Recommended protective measures:

- Position your screen to protect it from unwanted viewing or use a privacy screen.
- Always lock your screen when leaving your workstation.
- Do not leave documents in the printer and, if possible, print only with a transponder or access credentials.
- Do not connect unknown storage devices like USB sticks or external hard drives to your work computer.
- Cover your computer's webcam when not in use, for example with a webcam cover.
- Completely erase any information from whiteboards, flipcharts, or notice boards before leaving the room.

Clean desk principles

Untidy desks pose a security risk. Therefore:

- Always lock away confidential information.
- Do not write down passwords and do not leave personal data exposed.
- Store data carriers in a secure location.

Incidentally, the clean desk principles can easily be applied to your computer desktop as well.

Visitors

- Do not allow anyone into the building who cannot identify himself as authorised.
- Escort unfamiliar persons to the reception.
- Always accompany your visitors.

Very important!

Personal information is extremely valuable to criminals for planning and executing targeted attacks. Therefore, be cautious with details about internal structures as well as holiday or absence schedules.

Do not leave seemingly insignificant information such as phone numbers or network details on your desk.

Through social media posts, unauthorised persons can easily access confidential information. Therefore, never post photos of your workplace or surroundings on social networks.

INTERNET: Internet and cloud. Blessing and curse at the same time?

The internet serves as a gateway to the world offering unprecedented opportunities. This also applies to cybercriminals who do their mischief online. Hidden malware, Trojans, or ransomware represent a vast range of attack vectors. Caution is also advised when using cloud services, as sensitive data on the web is particularly vulnerable.

Internet

- Regular updates of the operating system, browser, and antivirus software protect against attacks and close potential entry points.
- An SSL certificate, indicated by a padlock symbol in the address bar and the “https” designation, confirms an encrypted and secure connection.
Example: <https://cybersicherheit-bw.de>
- Unusual website endings, such as .ru or .to, or poor spelling and grammar, can be signs of a fake website.
- Using a VPN (Virtual Private Network) helps to maintain anonymity on the internet and protect privacy.
- To prevent online activity tracking, delete cookies, clear browser histories, and disable tracking settings in your browser.

Cloud

- Only use the cloud services approved by your institution.
- Do not share work-related data through free sharing providers. The IT department can inform you which platforms are approved for data transfer.
- It is recommended to encrypt private data before storing it in the cloud.

Good to know

Language translation services are a great help and facilitate many tasks. However, before using them, you should check with your supervisors whether these services are permitted. Additionally, no confidential information should be included in the translations, and every piece of content to be translated should be anonymised.

Many search engines store and analyse user information, such as personal data and IP addresses. To reduce data traces on the internet, it is advisable to switch to a search engine that respects your privacy.

SOCIAL ENGINEERING: Manipulation, deception, and fraud

Social engineers pose as trustworthy individuals who are supposedly authorised to request information from you. The victims act in good faith, believing they are doing the right thing. This is why this tactic remains highly effective in committing fraud.

Social engineering can occur through various channels: in person, over the phone, via messenger services, or on social networks.

Tactics and strategies:

- Helpfulness, sympathy, or fear: Attackers use social manipulation techniques to elicit specific emotions in the target person or to prompt them to take rash actions.
- Individuals who are unknown or not clearly identifiable may request confidential information, internal processes, or access credentials and often threaten consequences if the requested information is not provided.
- Even seemingly insignificant information such as phone numbers, addresses, names, or absence times can help a social engineer plan and execute an attack.

Appropriate responses:

- If the person is not clearly identifiable, do not provide any information.
- In case of doubt, politely end the conversation and consult with your supervisor.

Useful tips

Attackers often stage extraordinary scenarios that demand the disclosure of a password or the installation of software. In such cases, do not act hastily; always clarify software installations with the IT department.

Especially in social networks and messenger services, attackers often pose as friends or family members. Personal questions that only the real person can answer can help verify their identity.

VIDEOCONFERENCES: “...starting to share my screen”

Videoconferences allow us to collaborate together as a team over distances, share data, and present content. When sharing your screen, it is particularly important to ensure that no sensitive information is visible. Not all videoconference systems have equal security levels and may not be approved for internal use. Your supervisor can usually inform you about the conference systems that are permitted and how to handle invitations to unauthorised conference systems.

General principles:

- Use a virtual background or blur effect whenever possible to protect your privacy.
- Voice assistant systems can listen in and should, therefore, be turned off and removed from the workspace during work.
- Participants without an active camera and those joining by phone must identify themselves at the beginning.

When screen sharing:

- Others could view or capture sensitive information via screenshots.
- Do not enter passwords while sharing your screen.
- Close unnecessary tabs and the password manager before screen sharing.
- Disable pop-up notifications from email programmes, conferencing systems, and messaging services.

Useful tips

Many videoconferencing systems offer the option to record conversations. Before recording, obtain consent from all participants, who should also be informed about

the recording's purpose. Additionally, ensure that the recordings are securely stored and properly deleted once their purpose has been fulfilled.

Disable all unnecessary tracking, logging, and recording functions, as well as the "use data to improve services" feature.

Glossary

A

Access link

By clicking on an access link, users are forwarded to the target address and granted access to a website, file, or platform (e.g., a videoconference).

AI

AI stands for Artificial Intelligence and refers to machines and systems capable of showing human-like intelligence. This includes abilities such as perceiving sensory inputs and responding to them or gathering information and autonomously solving problems based on it.

Antivirus software

Computer software that detects, blocks, and removes malicious programmes such as viruses, trojans, and malware to ensure the security of a computer and the data stored on it.

B

Blur filter

A filter used in videoconferences to blur or fade the background of your video image, thereby protecting your privacy.

Browser

A software application that allows you to display and interact with websites and web content on the internet.

Browser history

A chronological list of visited websites and search queries that are automatically recorded in the background by a web browser.

C

Clean desk policy

The principle of maintaining a tidy workplace where confidential documents and items are always secured to prevent unauthorised access.

Cloud/cloud computing

Cloud computing, often simply called 'the cloud', is a model that allows the retrieval of computing resources (e.g., databases, servers, storage) over the internet. From a user perspective, this makes it possible to store and access photos or files in a cloud.

Cloud/cloud service

An internet service that allows data and applications to be stored, managed, and accessed on remote servers instead of being stored locally on the user's computer.

Cookies

Cookies are small text files stored on a computer or device by a website, which contain information about user interactions with this website. There are different types of cookies serving various purposes: technical cookies ensure website functionality, while advertising and analytics cookies analyse user behaviour to tailor advertisements and offers.

Cyber

The term 'cyber' pertains to all things related to computers, the internet, and digital technologies, particularly focusing on aspects like security and crime in the digital realm, such as cybersecurity and cybercrime.

Cyberattack

A criminal act involving the infiltration of a computer system or network to steal, manipulate, or damage data.

D

Data carrier

A physical medium for storing and transferring data. Examples of data carriers include hard drives, USB sticks, CD-ROMs, DVDs, Blu-ray discs, and memory cards.

Data traces

Digital information left by a user on the internet, such as search queries, visited websites, online purchases, or social media interactions.

Default password

A pre-set password that enables the initial access to an account or application. Users are usually prompted to change the default password after the first login.

F

Fake website

A fraudulent website that mimics the appearance of an original site aiming to capture login credentials or personal information or to collect money for products and services without delivering the promised goods or services.

G

Guest network

A separate Wi-Fi network set up parallel to the main network. Guests can access the internet via Wi-Fi while the main network is kept protected.

H

Hacker

The term 'hacker' (also computer hacker) usually refers to individuals or groups who infiltrate foreign IT systems in an unauthorised manner. Their goal is to attack, manipulate, or infiltrate systems to enrich themselves or cause chaos. However, there are also white hackers: they uncover vulnerabilities and report them to official authorities or conduct legal tests on systems to identify entry points.

Home router

A router is a hardware device that acts as a connection point between a local network and the internet. The router used at home is referred to as a home router.

https

HTTPS (Hypertext Transfer Protocol Secure) is a protocol for secure data transmission on the internet. Unlike HTTP (Hypertext Transfer Protocol), HTTPS connections are encrypted, and all communication between the user and the server is not visible from the outside. This is especially important when processing confidential information.

I

Information security

Information security aims to protect information from unauthorised access, alteration, or destruction while ensuring the availability, confidentiality, and integrity of information.

Information security officer

The information security officer is responsible for managing all aspects of information security within an organisation.

Internet

A worldwide network of interconnected computers through which information and data can be exchanged and accessed.

IP address

An IP address is a unique numerical identifier assigned to a device to facilitate communication and unique identification within a network.

IT

The abbreviation IT stands for Information Technology, encompassing all electronic data processing and the associated hardware and software infrastructure.

M

Malware

Malicious software designed to cause harm to a computer, network, or other devices. It can perform unauthorised activities and harmful actions, steal or destroy data, and impair system resources.

Master password

A complex password with a minimum length of 14 characters required to access the password manager's database. If the master password is lost, access to the passwords stored in the password manager is no longer possible.

Messenger service

An online service that allows users to exchange written messages as well as multimedia content (photos, videos, etc.) over the internet.

N

Network drive

A storage area on a remote computer or server that is accessible over a network appearing as a local drive on the user's computer.

P

Password

A password is a combination of characters, numbers, and symbols used to protect data, accounts, or devices.

Password manager

Software that allows users to generate, store, and securely manage passwords.

PC lock shortcut

For Windows devices: Windows key + L

For Apple devices: Ctrl + Command key + Q

Personal data

Information that relate to an individual, such as name, address, date of birth, email address, or IP address.

Phishing

Phishing combines the words 'password' and 'fishing' and is a form of internet fraud. Criminals pose as trustworthy persons or organisations via phone, email, and other text-based messaging channels. They use skillful manipulation to obtain confidential information such as passwords or credit card details.

PIN

Abbreviation for 'Personal Identification Number', a number required to access personal accounts or data.

Pop-up notification

Brief messages that appear on the screen edge, for example, to indicate the receipt of a message and provide a preview of its content.

Post (social media)

Messages or content published on a social media platform.

Preview pane

Since merely opening an email can result in system infection, the email programme offers a partial preview of the content without opening the actual email.

Privacy screen

A thin, transparent film applied to the screen of a device such as a computer or smartphone, preventing unwanted views from the side or above.

Programme icons

Small symbols that represent programmes, files, and folders on the desktop. A double-click executes the action associated with the icon.

R**Ransomware**

Malicious software that infects a system and encrypts data or the system itself. A ransom is demanded for decryption.

S**Screen sharing**

The ability to share your screen in real-time with others during a videoconference.

Screenshot

A captured image of the content displayed on a computer or mobile device screen.

Search engine

An application that searches the internet for websites and other digital content based on the entered search query and provides the most relevant results.

Sharing providers

Companies that provide platforms allowing users to access a variety of services, products, and resources, such as data transfer.

Shoulder surfing

A person attempts to steal sensitive information by looking over another person's shoulder at his screen (e.g., on a train) or observing what PIN is entered at an ATM.

Social engineering

Tactical interpersonal manipulation of individuals to use them for one's own purposes. People are influenced to disclose sensitive information. A social engineer is a person who executes such manipulations.

Spam

Unwanted and often mass-sent messages (usually via email) that typically contain advertising or fraudulent content.

SSL certificate

An SSL certificate (Secure Sockets Layer) is a digital file issued by a trusted certification authority. It confirms the identity of a website and enables encrypted data transmission between the server and the browser.

SSL encryption

SSL encryption (Secure Sockets Layer) encrypts the connection between a server and a client to ensure secure communication over the internet.

T

Tab

A tab is a section within a web browser that displays a webpage. Users can open several tabs (webpages) in a single browser window to navigate between them as needed.

Tracking function

Tracking functions enable monitoring and recording of a user's internet activities.

Transponder

An electronic device that can receive and send signals. An example is an access card used to operate printers and open doors.

Trojan

A malicious programme that masquerades as legitimate software stealthily infiltrating a computer system and manipulate it or steal data.

Two-factor authentication

A method of enhancing security by using two different identification factors to authorise access to an account. A typical example of two-factor authentication is using a bank card together with its corresponding 'PIN' to withdraw money from an ATM.

U

Update

The process of updating an operating system or software to fix bugs, close security gaps, or add new features.

USB stick

A small, portable storage device that can be connected to a computer to store and transfer data.

V

Videoconferencing system

A platform or application that enables video-based online communication with multiple people in real-time.

Virtual background

A digitally generated background used to protect privacy in videoconferences. It serves the same function as a blur effect but displays any chosen photo instead of a blurred background.

Virus scanner

Programme that protects electronic devices from malware by searching for and removing viruses. Since new virus variants emerge daily, even the most advanced virus scanners cannot guarantee complete security.

Voice assistance

Technology that allows interaction with a computer or digital device via voice commands to perform tasks or retrieve information.

VPN

A VPN (Virtual Private Network) is a virtual network that allows users to securely access the internet. It helps maintain anonymity online, protects privacy, and secures the use of public Wi-Fi networks.

W

Webcam cover

An integrated slider or sticker that covers a device's camera (webcam) preventing spying through the camera.

Webcam light

A small light next to the webcam that indicates whether the camera is currently active.

Wi-Fi access

Wi-Fi access (Wireless Fidelity) is a wireless connection to a network, such as the internet.

Contact

Cybersicherheitsagentur Baden-Württemberg (CSBW)

Internet: www.cybersicherheit-bw.de

Email: schulungen@cybersicherheit.bwl.de

Last update: April 2025

Cybersecurity emergency response card

IT emergency number:

Enter the emergency number here:

➔ **Stay calm!**

➔ **Stop working on the affected device/system.**

➔ **Report the cyberattack:**

Report to information security officer, IT department, or supervisor as outlined in your IT emergency plan.

1. **WHO is reporting? (name, position, etc.)**
2. **WHICH IT system is affected?**
3. **HOW and to what extent were you working on the affected system before the incident?**
4. **WHAT did you observe? Did you notice anything unusual about the system?**
5. **WHEN did the event occur?**
6. **WHERE is the affected device/system located? (building, floor, room, workstation)**

➔ **Only initiate further measures** in consultation with the responsible authority after having reported the incident.