Modul 231 Data Security and Data Protection

Nasrin Jafari
2024
TBZ

Table of Contents

Data Protection(Reading article)

What is Data Protection?

This section covers the importance of data protection in the digital age. It emphasizes the vast amounts of personal data that can be collected and interconnected through information technology, such as Big Data, artificial intelligence, and the Internet of Things. It highlights the gap between technological advancements and the awareness of data handlers regarding security measures. Furthermore, it points out the lack of sensitivity among individuals, both data handlers and data subjects, towards issues of personal privacy

Modern Information Technology and its Risks from Internet to Video Telephony:

This part delves into the risks associated with modern information technologies, focusing on the Internet and computers. It discusses the evolution of the Internet towards Web 2.0, where users are not just consumers but also content creators. The rise of social networking sites is highlighted, where users share personal information through profiles that can be accessed by others based on privacy settings. It warns about the potential dangers of digital storage media, like USB sticks, which can transmit viruses and compromise the security of personal data if lost

.

Modern Information Technology and its Risks - from Images to Image Rights and including page

This section continues to explore the risks posed by modern digital technologies, particularly focusing on images and image rights. It addresses the concerns of companies seeking advertising revenue through personalized offers to users. The discussion extends to the risks associated with data transfer via digital storage media, emphasizing the underestimated dangers posed by mobile data storage devices like USB sticks. While these devices can transmit viruses and jeopardize the security of personal data if lost, following specific guidelines can significantly reduce these risks. Reports indicate that numerous organizations have been infected with malicious programs through storage media in recent months

What does Data security and Data Protection mean?

What is Data Protection?

Data protection is the process of safeguarding sensitive data against loss, manipulation, and damage. Data protection is becoming more crucial as data production and storage have expanded at an unparalleled rate. Additionally, as data is used more and more in organizational processes, even a brief period of downtime or a small quantity of data loss can significantly impact a company. The protection of data requires both administrative and technical solutions. Legal considerations are part of administrative measures (privacy policies, terms, conditions, etc.).

Principles of Data Protection

The fundamental concept of data protection is to assure that data is always safe and accessible to its users. Data management and data accessibility are the two main pillars of data protection.

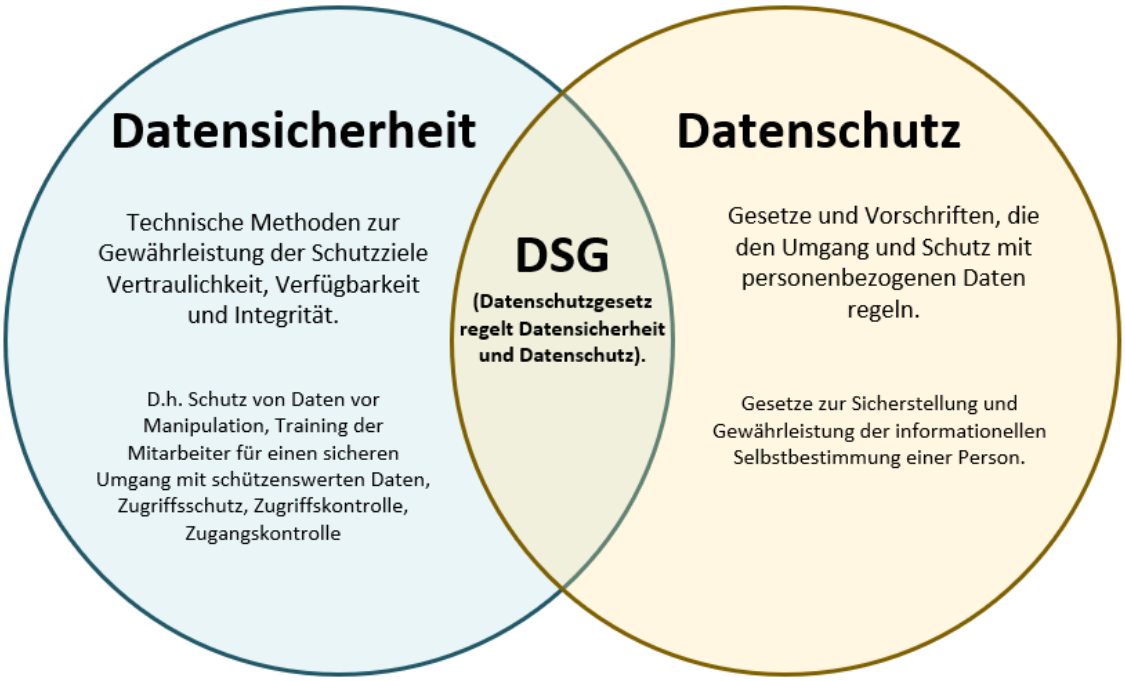
- **Data availability** ensures that clients can access the data they require for operations, even if it is damaged or deleted.
- **Data management** involves two major aspects of data protection: Data lifecycle management, Information lifecycle management

What is Data Security?

Data security protects digital information from internal and external, malevolent, and unintentional dangers. Although data security is concerned with keeping data secure, it also includes infrastructure security; it is difficult to secure data if the supporting architecture is not secure appropriately. Organizations have implemented numerous security procedures and data security solutions to ensure data security. Multi Factor Authentication (MFA) is one example, which uses at least two separate processes to validate a user's identity before giving access to data.

Data Protection	Data Security
• Data protection is the method of preventing crucial data from being lost, corrupted, or compromised while also giving users the option to restore the data to a usable condition if something were to happen that prevented them from accessing or using it.	• The protection of a database against any acts or forces that could be harmful to the database is what data security is all about. In essence, it protects the data from being accessed by unauthorized individuals.
• Data security and data protection are equivalent in terms of technique. It performs data replication, data archiving, data recovery, and backups.	• Data security employs disc encryption, hardware-based measures to prevent data theft, data masking, data erasure, firewall deployment, and the ACLs (access control lists) technique.
• In general, data protection is implemented at the core data and level.	• Data Level – by employing techniques such as encryption Level of Access Control – using strategies such as role-based access control, etc.,

• Data protection keeps data safe and secure.	• Data security keeps data secure.

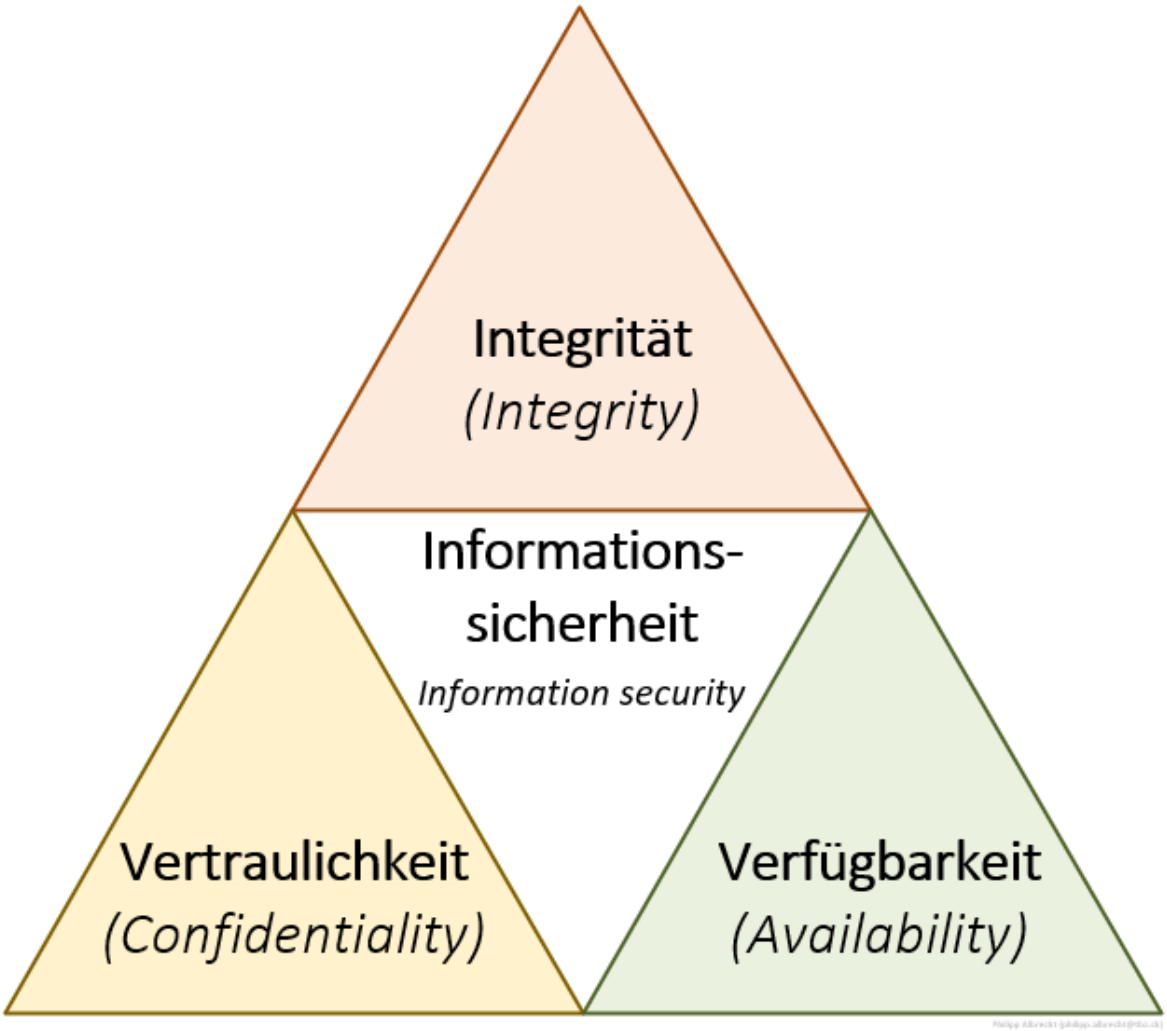


https://gitlab.com/klassenunterlagen_gg/

1. Availability: Prevention of system failures; access to data must be ensured within an agreed-upon timeframe.

2. Confidentiality: Data may only be read or modified by authorized users. This applies to both accessing stored data and during data transmission.

3. Integrity: Data must not be altered unnoticed. All changes must be traceable.



https://gitlab.com/klassenunterlagen_gg/

Right to information (Auskunftsrecht)

We as human have rights to have access to our personal inforamtion, delete or block the access of others to our information.

We have the right to access Our personal data and to check what data a public body collects. We do not have to provide any reasons for a request for access. Public bodies are obliged to provide information about the data.

Rights to Information according to EDÖB

Under the Data Protection Act (DSG), individuals have the right to request information from responsible parties about whether their personal data is being processed. They can also request data deletion or correction if necessary. This right allows individuals to control the data collected about them. The DSG outlines information that must be provided to individuals upon request, including the identity of the responsible party, details about the processed data, purpose of processing, data retention period, data origin, and recipients of the data. Individuals can exercise their right without providing justification, and responses are typically provided free of charge within 30 days. However, fees may apply for requests that cause undue burden. Responsible parties may refuse or restrict information provision in certain cases, but they must justify their decision. The process for requesting information can be facilitated by using a template letter provided by the Federal Data Protection and Information Commissioner. Requests and disclosures can be made electronically or via mail, with appropriate measures to ensure data security and identification. If no response is received within 30 days, individuals can follow up with a registered letter.

Duty to provide information(As Service Provider like Application developer):

The importance of transparency and individual rights regarding the processing of personal data under the Federal Act on Data Protection (FADP). It outlines the duty of organizations, as data controllers, to provide clear and accessible information to individuals about how their data is being used:

I. Data controllers must inform individuals in advance and adequately whenever their personal data is collected.
II. Information provided should be concise, transparent, and cover details such as the purpose of data processing and the identity of the data controller.
III. Exceptions exist, but efforts should be made to fulfill the duty to provide information.
IV. Specific requirements apply to automated individual decisions, ensuring individuals are informed and have the right to challenge decisions.
V. Federal bodies must clearly indicate when individual decisions are automated.
VI. The criminal aspects related to breaches of data protection obligations and individuals' right to request information about their personal data processing.

What should I do when I ask about my information (As a Normal Person)?

Imagin we want to know about my information which the Salt my Mobile Provider has collected (Case 1):

I. Ask about it per email or any electronic chanel like webform which the company provided.

II. if within 30 days no answer received, in switzerland as mentioned in the EDÖB we can proceed with the registered letters for each request, there are different kind of registered letter like for just asking about the collected personal inforamtion or asking for changing or deleting

III. Download the Regitered Letters from this website: Auskunftsrecht or from this EDÖB and fill it with your request

Checklists of the Data Protection Officer of Zurich

How to secure my smart phone in 10 Steps (Secure smartphone)

Step 01) Activate device lock:

- I have Auto locked enabled and my phone after 30 seconds inactiveness gets locked.

Step 02) Lock and erase the device immediately in case of loss:

- I have activated Find My app on my mac and smart Phone and all my apple products are connected and “Erase this device” option is also visible

Step 03) Install apps only from trusted sources:

- I alsways install apps from app store and other apps which are not available on app store only from trusted sources.

Step 04) Use public Wi-Fi with caution:

- On My Samrt Phone I never connect to public Wi-Fi unless to the school Wi-Fi or Offic.

Step 05) Install updates:

- On My Samrt Phone all Apps which are installed from App Store are on auto update and the Phone itself is also auto update only for alpha versions.

Step 06) Safely delete data:

- Yes, I have deleted all my data from my pervious smart phone before I give it away.

Step 07) Follow general precautionary measures:

- Yes, I never open suspicious links, emails, or call back to an unfamiliar telephone number.

Step 08) Disable wireless interfaces:

- Yes, I always turn bluetooth, wifi, airdropp off when I don’t use them.

Step 09) Limit synchronization:

- Yes, I have already limited sychronization to iCloud for more security also because of lack of space.

Step 10) Use a second factor for login:

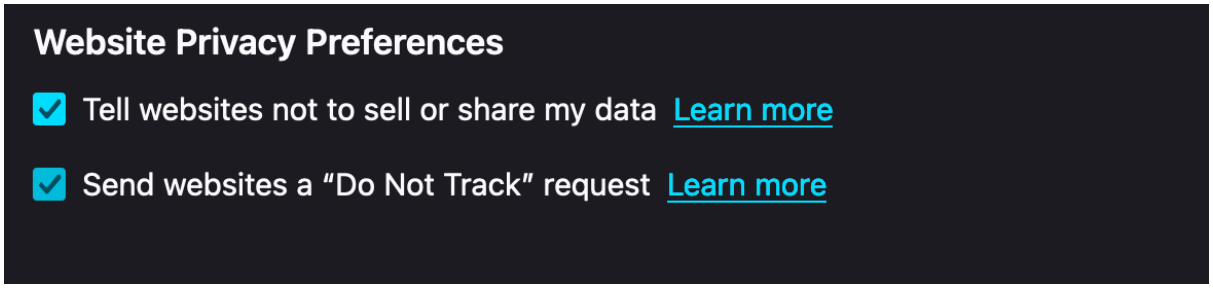
- Yes, I have already enabled the two FA since beginning.

Secure My PC in 5 steps (How to increase pc security)

Step 01) Protect personal information:

- I have already done this step, for example each time when I close the Firefox all casched data will be removed and I need to re-login to each website.

Step a) How do I prevent webtracking?
- I don't accept cookies from websites and always decline them.
- I enabled Do Not Track option in all my browsers.
- I enabled to delete all cookies, histories and caches when I close the browsers



Step 02) Angriffe abwehren:

Step a) Rugular securityupdate on your PC
- Yes I do it regularly

Step b) Activate the Firewall
- Yes it is activated

Step c) Choose secure browsing
- Yes I have enabled strict browsing in all my browsers

Step 03) Block unauthorized access:

Step a) Use Strong Password

- Yes, I use always strong passwords, minimum 8 length and combination of upper and lowercases, numbers and special chars.

Step b) Use unauthorized wireless networks weisely

- I never connect to random wireless networks only networks in school or my office building or sbb if I don't have another option.

Step c) Encrypt your wireless network

- I use my Personal hotspot and on iPhone there isnt a direct security encryption option.

Step c) Use the Screen Lock

- I use Screen Lock after 1 minutes and it always required password immediately when pc is inactive.

Step 04) Encrypt sensitive data:

Step a) Encrypt Drives

- I have secured my drives and they are encrypted by enabling FileVault on mac

Step b) Encrypt Emails with sensitive content

- No I hadnt encrypted my emails but now sensitive emails are encrypted

Step 05) Secure information and delete data completely:

Step a) Perform regular backups Instructions for Windows and MacOS.
Keep backups safe from fire and theft. Completely erase information before disposing of or selling the PC, for example, using specialized software. DBAN or PartedMagic can help with this

I hadnt done backup on my mac but I am going to do it on section related to Backup

what are Cookies on the internet?

Cookies are bits of data that are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website. This data usually appears as strings of numbers and letters in a text file. Every time you access a new website, a cookie is created and placed in a temporary folder on your device. From here, cookies try to match your preferences for what you want to read, see, or purchase.

A common analogy for a cookie is a coat check ticket at a concert or event: It's something you receive from a service, has no intrinsic value outside of the event, and is tailored exactly to you. However, you'll need it if you want to get your coat back.

What types of cookies are there?

In general, cookies can be classified based on their purpose, duration, and provenance.

Duration:

I. Session cookies: These are temporary cookies that expire once you close your browser or end your session.
II. Persistent cookies: These cookies remain on your hard drive until you delete them or until their expiration date. While they should not last longer than 12 months according to the ePrivacy Directive, they can remain on your device for much longer if no action is taken.

Provenance:

I. First-party cookies: These cookies are placed on your device directly by the website you are visiting.
II. Third-party cookies: Placed on your device by a third party, such as advertisers or analytic systems, rather than the website you are visiting.

Purpose:

I. Strictly necessary cookies: Essential for browsing the website and using its features, such as accessing secure areas. Consent is not required for these cookies, but their necessity should be explained to the user.
II. Preferences cookies: Also known as "functionality cookies," they remember past choices made on the website, like language preferences or login information.

I. Statistics cookies: Also called "performance cookies," they collect anonymized data about website usage to improve its functionality. This includes cookies from third-party analytics services used exclusively by the website owner.
II. Marketing cookies: Track online activity to deliver targeted advertising or limit ad exposure frequency. These are usually persistent cookies of third-party origin.

How can we protect our data against cookies?

I. Browse always in “Private ” mode (for Safari or Firefox) or “Incognito” (for Chrome). Browsing this way doesn't keep your internet service provider or a web server from knowing what you're doing online, but it does keep cookies from working.
II. Make sure you have a record of all the passwords for sites that require a login. (Password Manager)
III. clearing all your cookies.

Here's how to clear cookies in three popular browsers:

Chrome: Under the Chrome tab at the top left of your screen, click “Clear browsing data.” Check the box: “Cookies and other site data.” Then click the bar at the bottom right of the window that says “Clear browsing data.”

Firefox: Under the Firefox tab at the upper left of your screen, go to Preferences > Privacy & Security > Show Cookies > Remove All.

Safari: Under the Safari tab at the upper right of your screen, go to Preferences > Privacy > Manage Website Data > Remove All.

The final step is to instruct your browser to allow first-party cookies while blocking third-party cookies:

Chrome: Go to Preferences > Privacy > Content settings. Open the Cookies tab and select “Block third-party cookies.”

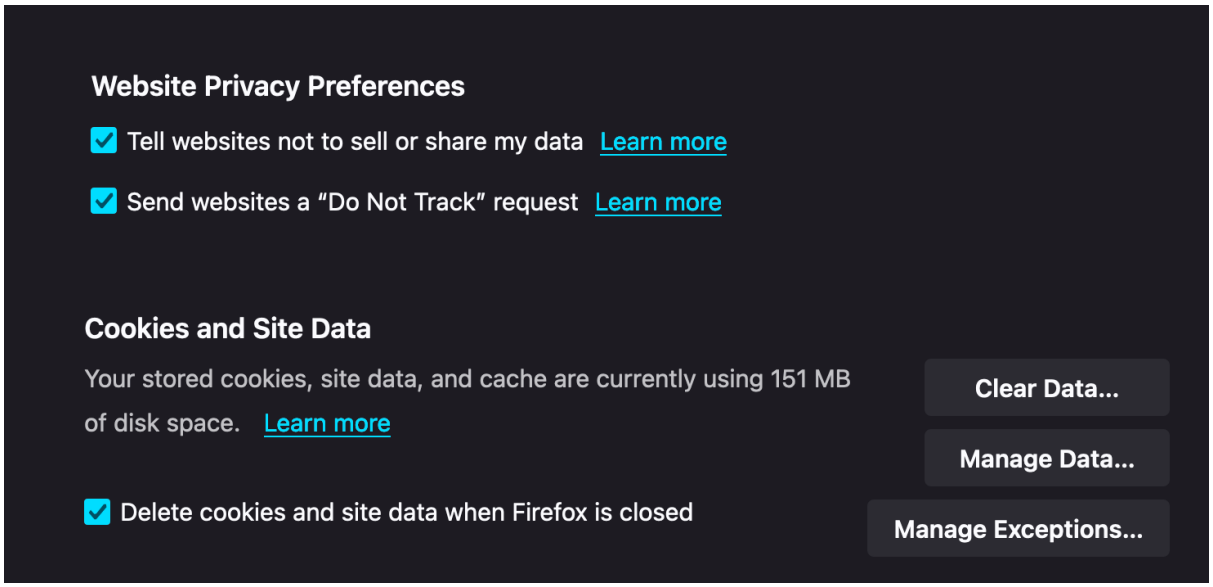
Firefox: Go to Preferences > Privacy > History. The default setting is “Remember history.” Change it to “Use custom settings for history” to reveal your cookies options.

For third-party cookies, you have three options: “Always,” “Never,” and “From visited.”

Safari: Apple's browser features the same cookie compromise–“Allow [cookies] from websites I visit”—which can be found at Preferences > Privacy.

How I Protect my Privacy in relation to Cookies?

- I use mostly the Firefox Browser and what I did I set the setting of the Firefox to delete all the cookies each time when I close the browser.
- The Problem is here that each time I need to pass my log in credentials to the websites I use



What I will do differently?

- I would save my passwords in a password manager to make the browsing experience better.

Permissive passwords

Introduction

While usernames are often public email addresses or derived from names, passwords are typically randomly generated sequences. Notably, commonly used passwords like "123456" or "password" suggest a tendency towards simple combinations.

To grasp the necessity of passwords, it's crucial to understand the concept of identification. A digital identity starts with an entity, where attributes are determined, mapped into a digital record, and associated with the entity. This process facilitates identification and verification, continuing until the entity's use concludes.

Illustratively, consider a package sent through postal services: its characteristics are recorded, a unique identifier (e.g., barcode) is affixed, and its journey is tracked until delivery. However, vulnerabilities exist, as a package could attempt to pose as another, leading to potential system alerts.

Human entities present unique challenges. While they possess distinct abilities like biometrics and secure storage methods (e.g., passwords), they also entail misuse risks. Authentication options include knowledge-based (e.g., passwords), possession-based (e.g., smart cards), and biometric methods.

Multi-factor authentication enhances security by utilizing different authentication options, such as sending verification codes to mobile phones. In Module 231, the focus will be on understanding secure passwords and effective password management techniques.

Why passwords? Reason for using passwords: Why are passwords used?

Passwords are used for authentication, security, and privacy, ensuring that only authorized individuals can access sensitive information or resources. They protect data, control access, and help comply with security regulations.

What is protected? What is protected with passwords?

Passwords are used to protect various types of sensitive information and resources, including:

I. **Personal Accounts**: Passwords protect personal accounts such as email, social media, online banking, and shopping websites, safeguarding private communications, financial details, and purchase histories.
II. **Corporate Systems**: Passwords secure access to corporate networks, servers, databases, and applications, preventing unauthorized individuals from gaining entry to sensitive company data, intellectual property, and proprietary software.
III. **Devices**: Passwords are used to lock smartphones, tablets, laptops, and other devices, safeguarding personal and professional data stored on these devices from unauthorized access.
IV. **Online Services**: Passwords protect access to a wide range of online services, including cloud storage, productivity tools, entertainment platforms, and communication services, ensuring the privacy and security of user accounts and data.
V. **Sensitive Information**: Passwords encrypt sensitive information stored on devices, in files, or transmitted over networks, preventing unauthorized individuals from viewing or tampering with confidential data such as medical records, financial records, and personal documents.

What types of information are protected with passwords, which are freely available?

Passwords protect personal, financial, and health information, along with intellectual property and corporate data. They serve as a barrier to unauthorized access to accounts, devices, and sensitive information. Despite their role in safeguarding data, passwords can be compromised through various means, including phishing attacks and data breaches. Therefore, it's crucial to use strong, unique passwords and implement additional security measures like multi-factor authentication. Breaches of password-protected systems can lead to financial losses, identity theft, and reputational damage for individuals and organizations. Regular password updates and awareness of security best practices are essential for maintaining data security. Overall, passwords play a vital role in protecting sensitive information but require diligence and caution to be effective in the face of evolving cyber threats.

What is a strong password?

A strong password is long (12 characters or more), complex (mixing uppercase and lowercase letters, numbers, and special characters), and unpredictable (avoiding easily guessable information like personal details or common words). It should be unique for each account and regularly updated for added security. Avoid using dictionary words or common phrases, opting instead for random combinations or passphrases. Utilizing a password manager can help generate and manage strong passwords securely.

what is authentication and authorization?

Authentication verifies the identity of users, devices, or systems trying to access a resource, ensuring they are who they claim to be through credentials like passwords or biometrics. Authorization, on the other hand, determines the permissions and privileges granted to authenticated entities, dictating what actions they can perform or what resources they can access. While authentication focuses on identity verification, authorization focuses on granting appropriate access levels based on authenticated identities. In essence, authentication confirms identity, while authorization governs access rights.

What do you do if you forget your master password?

I. I should check for password recovery options or account recovery methods provided by the password manager.
II. I should consider using backups if available to restore my password data.
III. If all else fails, I can create a new master password and manually recreate my password database

How do you back up your password database?

I use keychain password and there is an option: Export Password and it will generate a csv file.

If you use a cloud service: What do you do if you no longer have access to your account?

I. Attempt account recovery through password reset or account recovery forms provided by the service.
II. Contact customer support for assistance in regaining access.
III. Check for backup email accounts or phone numbers linked to the account.
IV. Provide proof of ownership, such as payment receipts, if necessary.
V. Consider seeking legal assistance as a last resort.
VI. Ensure to act promptly and follow the service's specific procedures for account recovery.

How do I manage my Password?

I. I use Keychain Access to view and manage my saved passwords.
II. I have the option to edit or delete passwords as necessary.
III. I also enabled iCloud Keychain for syncing passwords across devices.

What will I do Differently in the future to protect my passwords?

I don’t update my password regularly, I would update them for more protection.

Filing systems

what is Filing Systems?

A filing system is a method used to organize and store documents, papers, or digital files in a systematic manner to facilitate efficient retrieval and management. Filing systems can vary widely depending on the needs and preferences of individuals or organizations. They can be physical, involving paper documents stored in cabinets or folders, or digital, involving electronic files stored on computers or servers.

Common types of filing systems include:

1. Alphabetical: Documents are arranged in alphabetical order based on the name of the file or the subject.
2. Numerical: Documents are assigned numbers and arranged sequentially based on those numbers.
3. Chronological: Documents are organized based on the date of creation or receipt, with the most recent documents placed on top or at the front.
4. Subject-based: Documents are grouped together based on their subject matter or category.
5. Geographical: This type of filing system is used to organize documents based on their geographical location or relevance.
6. Hierarchical: Documents are organized in a hierarchical structure, with broader categories containing subcategories, and so on.

How do I differentiate between my personal and general data?

1. **File Naming Convention**: I adopt a consistent file naming convention that includes identifiers to distinguish my personal files from general ones. For example, I prefix personal files with my name or initials.
2. **Folder Structure**: I create separate folders or directories for my personal and general data. I organize my personal files under a designated folder specific to me, while general files are stored in common directories accessible to all users.
3. **Access Control**: I implement access control mechanisms to restrict access to my personal data only to authorized individuals. I utilize user authentication and permissions to ensure that only relevant personnel can access my personal files.

4. **Metadata Tags**: I assign metadata tags or labels to my files indicating whether they contain personal or general data. This allows for easy filtering and searching based on data type.
5. **Encryption**: I encrypt my personal data to add an extra layer of security, ensuring that only authorized users with decryption keys can access and view my sensitive information.
6. **Document Classification**: I classify my documents based on their content and sensitivity level. Personal documents are classified as confidential or private, while general documents may be labeled as public or for internal use only.

Backup

what does Backup means?

A backup refers to the process of copying and storing data from a primary source to a secondary location, typically for the purpose of protecting against data loss. Backups are crucial for ensuring the availability and integrity of important data in case of accidental deletion, hardware failure, data corruption, or other unforeseen events. The secondary copy of the data, known as the backup, serves as a safeguard that can be used to restore the original data if needed.

The Purpose of the Backup

- **Data Protection**: Backups are essential for safeguarding your important files and data against various risks such as hardware failures, software errors, accidental deletion, or cyber-attacks like ransomware.
- **Recovery**: They provide a means to recover lost or corrupted data, allowing you to restore your files to a previous state before the loss occurred.
- **Continuity**: Backups ensure business continuity by minimizing downtime in case of data loss incidents, allowing operations to resume swiftly.

Limitations of a Backup:

- **Time Lag**: Backups capture data at specific points in time, meaning any changes made after the backup may not be included. This can result in some data loss between backup intervals.

- **Incomplete Restoration**: While backups aim to restore data comprehensively, there might be limitations in recovering certain types of data or system configurations, leading to partial restoration.
- **Dependency on Backup Integrity**: The effectiveness of backups relies on their integrity and accessibility. If backups are not properly maintained, corrupted, or inaccessible when needed, they cannot fulfill their purpose.
- **Not a Substitute for Security**: Backups protect against data loss but do not prevent unauthorized access or data breaches. Additional security measures such as encryption and access controls are necessary to safeguard data from theft or unauthorized access.

How do I do my Backups?

Laptop	For My Laptop I only use the iCloud and save all my importatn documents there
Smart phone	For My Samrt phone I only use the iCloud and save all my importatn documents there
Documnets	Documents are seperated in categories, personal ones are in iCloud or google Drive, the Documents related to school or working projects are mostly on Gitlab or Github
Projects	The Projects are all hosted on Gitlab or Github

Licensing models

what is License?

The word "license" refers to a legal permission or authorization granted by one party (the licensor) to another party (the licensee) to perform certain actions, use specific property, or access particular rights. In essence, a license grants the licensee the right to do something that they would not otherwise have the legal authority to do.

For example, in the context of software, a software license grants the licensee the right to use the software according to certain terms and conditions set by the licensor. These terms and conditions may include restrictions on usage, redistribution, modification, and other actions related to the software.

In broader contexts, licenses can apply to various things such as intellectual property rights (e.g., patents, trademarks, copyrights), driving privileges, operating businesses, practicing professions, and many others.

Overall, a license is a legal instrument that regulates the use of certain rights or properties by granting permission under specified conditions.

Why do people come up with the idea of creating licenses?

Licenses are created to provide legal protection, monetize creations or assets, control and manage their usage, promote distribution, and ensure compliance with terms and conditions. They serve as a framework for regulating the use, distribution, and protection of intellectual property and other assets, benefiting both licensors and licensees.

What types of licenses exist besides software?

1. **Patents:** These grant exclusive rights to inventors for their inventions, allowing them to prevent others from making, using, selling, or importing the patented invention without permission.
2. **Trademarks:** Trademark licenses allow others to use symbols, logos, names, or other identifiers to distinguish goods or services under specified conditions.
3. **Copyrights:** Copyright licenses permit the reproduction, distribution, display, or performance of original works of authorship such as literary, artistic, musical, or other creative works.
4. **Franchises:** Franchise licenses enable individuals or businesses (franchisees) to operate under a recognized brand name and business model (franchisor) in exchange for fees and compliance with franchisor standards.
5. **Real Estate:** Licenses are required for various real estate activities such as buying, selling, leasing, or managing property.
6. **Professional Licenses:** Professionals such as doctors, lawyers, engineers, and accountants require licenses to practice legally, ensuring they meet specific standards and qualifications.

Software License Model Overview

Understanding software license models is essential for IT decision-makers, given the increasing complexity of software procurement. Microsoft, for instance, predominantly offers licenses for download (ESD), including volume licensing programs like OEM or PKC, making physical disks largely obsolete.

Procuring software now involves navigating various license types, with sustainability considerations becoming increasingly important for businesses. Sustainable software procurement aligns with AVV Climate guidelines and is gaining traction across industries.

To help navigate this landscape, companies like LizenzDirekt provide comprehensive guidance on purchasing new or used software, ensuring transparency and compliance. Their expertise aids in managing ongoing software license contracts, IT agreements, and license optimization.

Common Software License Models

1. Perpetual Licensing:
    - Customers purchase the software once and retain it indefinitely.
    - Typically, customers pay the license fee upfront, with occasional annual maintenance fees.
    - Provides customers with a fixed cost without unexpected price changes.
2. Concurrent User Licenses:
    - Allows multiple users to share a single license code.
    - Facilitates easy management of software licenses for businesses.
3. Subscription-Based Licensing:
    - Popular among consumers, with successful models used by companies like Spotify and Netflix.
    - Offers self-service features, increasing customer satisfaction.
    - Customers know when usage fees are due (e.g., monthly or annually).
4. Proprietary Licensing Models:
    - Customers purchase the right to use the software while the provider retains ownership.
    - Users must agree to the provider's terms and conditions.
    - Can be used in conjunction with other software licensing models offered by Thales Sentinel.
5. Floating-Feature Licensing Model:
    - Customers purchase multiple licenses but restrict simultaneous use of specific features.
    - Provides flexibility in utilizing and selecting certain features, saving money for companies.
6. Feature-Based Licensing Model:
    - Offers high control over which features can be used with each license code.
    - Allows for customization based on individual user needs.
7. Network Licensing:
    - Ideal for situations where users need to access software without stable internet connections.
    - Allows monitoring of usage even without internet access.
8. Cloud-Based Licensing:
    - Provides on-demand access from anywhere, anytime.
    - Commonly associated with subscription licenses.
    - Best implemented on an existing on-premises licensing platform or as a new system.

Benefits of Software License Management and Volume Licensing

Volume licensing, such as Microsoft's Open Value program, streamlines software procurement for businesses, providing benefits like simplified deployment and cost savings. This approach, coupled with Software Assurance options, offers support and access to updates.

Moreover, understanding and implementing diverse software licensing models contribute to business growth, offering flexibility and catering to customer needs. By integrating cloud-based licenses, companies can enhance customer satisfaction, increase revenue, and improve operational efficiency.

Thales Sentinel aims to provide tailored software licensing models, empowering businesses to develop systems that align with their needs and those of their customers.

What does "open source" mean and what can you do with such software?

"Open source" refers to software that is released with a license allowing anyone to access, modify, and distribute its source code freely. This means that the inner workings of the software are transparent and accessible to users, enabling them to study, alter, and distribute it as they see fit.

With open-source software, users have the freedom to customize the software according to their specific needs, without being limited by proprietary restrictions. They can modify the code, add new features, fix bugs, and share their improvements with the community.

One of the key benefits of open-source software is its collaborative nature. Users from around the world can contribute to its development, leading to rapid innovation, improved functionality, and enhanced security.

Additionally, open-source software is often available at no cost, making it accessible to individuals, organizations, and communities regardless of their financial resources. This democratization of technology fosters creativity, empowers users, and promotes a culture of sharing and collaboration in the digital realm.

what is the difference between Copy right and Copy left?

I. Copyright:
   a. Copyright is a legal concept that grants the creator of an original work exclusive rights to its use and distribution.

b. It restricts others from copying, distributing, or modifying the work without permission from the copyright holder.
c. Copyright law is often used to protect proprietary software and other creative works.

II. Copyleft:
a. Copyleft is a strategy of utilizing copyright law to permit the free use, modification, and distribution of a work and its derivatives, as long as the same freedoms are preserved in the derivative works.
b. It is often associated with open-source software licenses, such as the GNU General Public License (GPL), which ensures that the software and its derivatives remain freely available to users.
c. Copyleft licenses aim to promote collaboration, sharing, and community-driven development by requiring that derivative works also be released under the same license terms.

Which licensing model is applied when you

download and install a paid app from the App Store?

If you don't know whether you paid extra, how and when do you pay?

When I download and install a paid app from the App Store, I am typically subject to a proprietary licensing model, where the developer retains the rights to the software, and I am granted permission to use it under certain conditions outlined in the End User License Agreement (EULA) provided by the developer.

download and install a free app from the App Store?

When I download and install a free app from the App Store, it can still be subject to various licensing models. Some free apps may use open-source licenses, allowing users to freely use, modify, and distribute the software's source code. Others may utilize proprietary licensing, similar to paid apps, but may be free to download and use with certain restrictions or limitations.

Did you pay for the software when you bought/received your current smartphone?

No I havent paid for any Software since I bought my smartphone

If you don't know whether you paid extra, how and when do you pay?

If I'm unsure whether I paid extra for the software, I can typically check my purchase receipt or invoice to see if any specific charges were associated with software licenses.

Hardware failure Laptop and Smart phone

Which datas are available?(Photos, Messages, Documents)

My Photos and Documents are not available in case of hardware failure I disabled them to be synched with the iCloud.

How do I access to which type of data?

Only I have access to datas which are syched with iCloud.

can I access to a new Computer without my smart phone?

I normally use another back up email or have another Authentication app on another iPad or iPhone.

Where do I have saved my Passwords?

Normally I save them on my keychain access app.

What asccess has the “Finder” of my PC?

Totally nothing.

Which damages can the “Finder” cause on my devices?

A finder could potentially cause various damages with the data they have access to, including:

I. **Identity Theft**: They could use personal information stored on the devices to steal your identity, open fraudulent accounts, or engage in other forms of identity theft.
II. **Financial Loss**: If financial information such as bank account details or credit card numbers is accessible, the finder could make unauthorized transactions or drain your accounts.
III. **Privacy Breaches**: Sensitive personal data, such as private photos or messages, could be leaked, compromising your privacy and potentially leading to embarrassment or harm.
IV. **Data Manipulation**: The finder could alter or delete important files or documents, leading to data loss or disruption of your work or personal life.
V. **Blackmail or Extortion**: If the finder discovers sensitive or embarrassing information, they could use it to blackmail or extort you for money or other favors.
VI. **Reputation Damage**: If the finder publicly exposes private or sensitive information, it could damage your reputation or relationships with others.

Can I delete data from abroad?

yes I can via Find my App on Apple products but location shoud be on.

Can I find My devices?

Yes again via Find My it will find my device but if they are still turn on.

Against which damages are my back ups secures secured?

I. Data Loss: If I accidentally delete, corrupt, or otherwise lose my original data, I can restore it from my backups to recover the lost information.
II. Hardware Failure: In case of hardware failure, such as a hard drive crash or device malfunction, my backups ensure that I can restore my data to a new device or repaired hardware.
III. Malware and Ransomware Attacks: If my device is infected with malware or targeted by ransomware, backups allow me to restore my data to a clean state without having to pay ransom or risk permanent loss of data.
IV. Accidental Changes or Deletions: If I accidentally change or delete important files, backups provide a means to revert to previous versions or restore the deleted files.
V. Theft or Loss: In the event that my device is lost or stolen, backups ensure that I still have access to my data and can restore it to a new device.

How do you assess your time investment?

I had all the required steps dones and it didn’t take me too mcch time

what is my Consequence from this experiment?

Ich have found that I wasn’t fully ready in case of Hardware death.

Resources

The Federal Council
Cookies, the GDPR, and the ePrivacy Directive
Cookies&Online Security