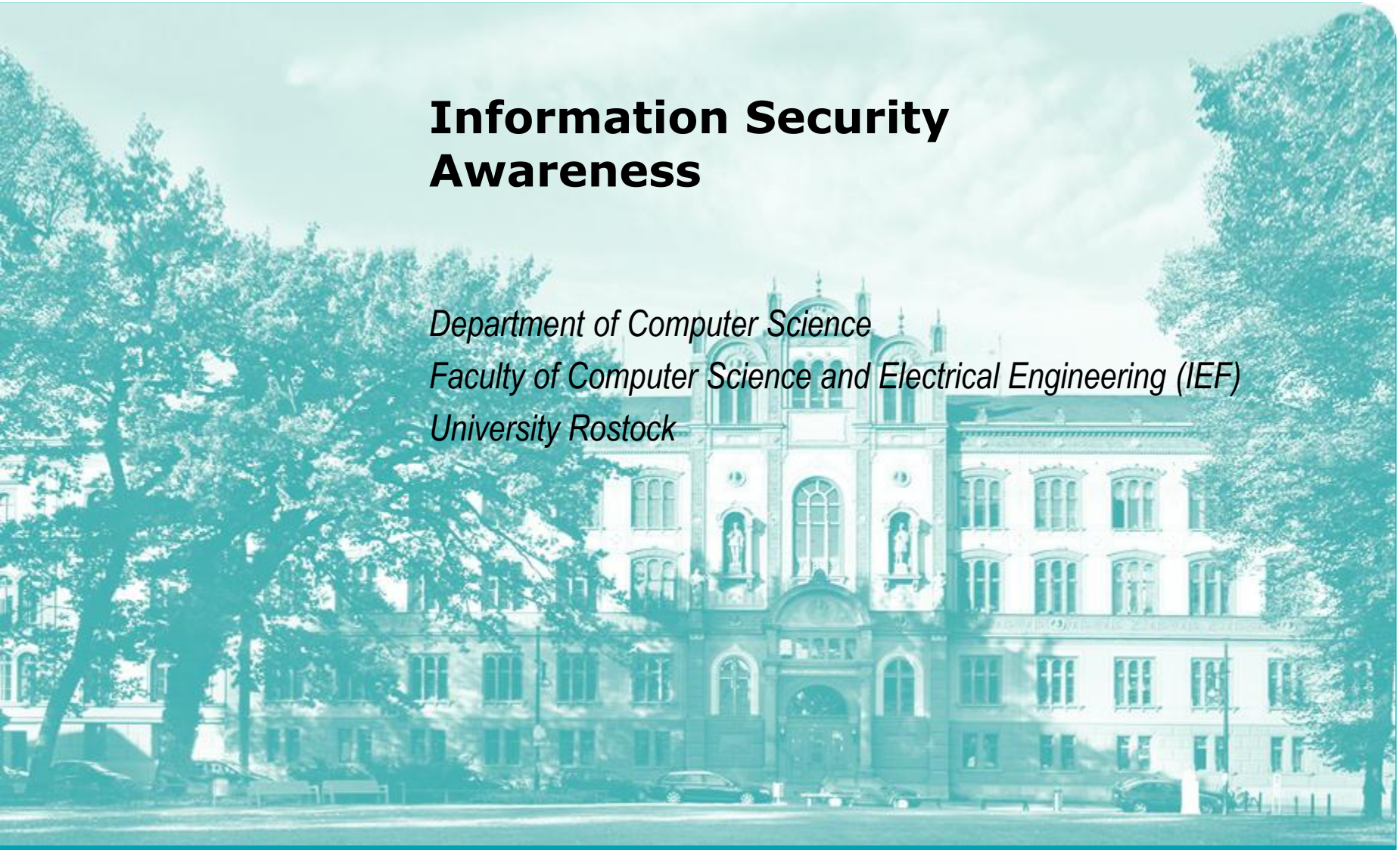
Universität Rostock

Traditio et Innovatio



Information Security Awareness

Department of Computer Science
Faculty of Computer Science and Electrical Engineering (IEF)
University Rostock

Content

Date: 03/27/2025

1. General information
2. Secure workplace and secure IT infrastructure
3. Safety for mobile devices
4. Passwords
5. Confidential data
6. Handling of security incidents

Sources:

- University of Rostock, IT security concept for the ITMZ: https://www.itmz.uni-rostock.de/it-sicherheit/dokumente-und-links/it-sicherheitskonzept-fuer-das-itmz/
- Technical University of Munich, information and tips on IT security for employees: https://www.it.tum.de/it/it-sicherheit/fuer-mitarbeiterinnen/
- security.org – How Secure Is My Password? https://www.security.org/how-secure-is-my-password/

General Information

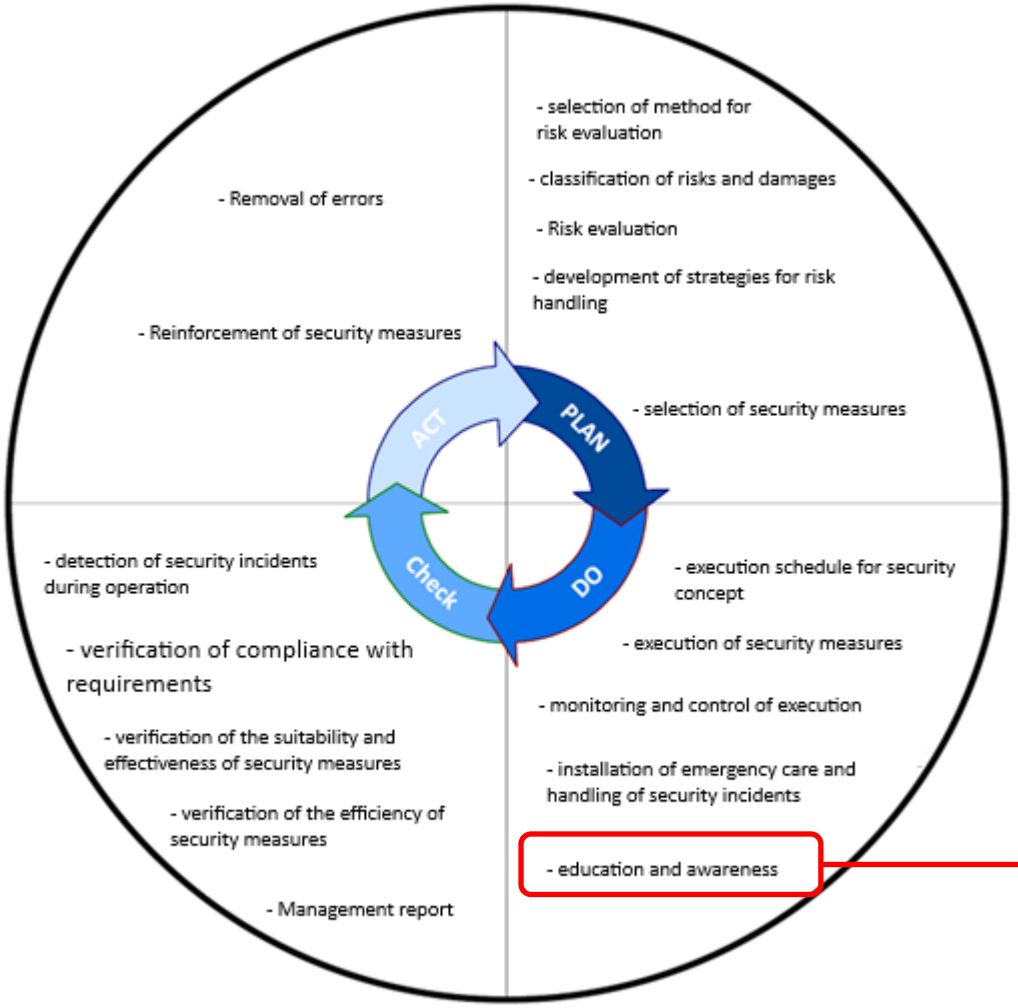
Information security is indispensable

- Systematic management of information security to protect data, information and IT-systems is necessary regarding:
  - **Confidentiality:** secure sensible or confidential information for unauthorised disclosure.
  - **Integrity**: all data stays complete and unmodified during and after processing.
  - **Availability**: all information and functionalities can be accessed by the user when needed.

- Free online course: https://training.linuxfoundation.org/training/cybersecurity-essentials-lfc108/

IT security concept of Uni Rostock

Life cycle of ITMZ security concept



Oriented on the methodology of BSI-Grundschutz

Education and awareness

Secure Workplace and secure IT infrastructure

Clear responsibilities for operation systems and applications

- System engineer is responsible and liable for operation systems and applications of the IT infrastructure
- Subdivisions can be handed down to qualified employees

Secure workplace and secure IT infrastructure

Protection from unauthorised access and malware

- **Computer lock** (Screensaver with password or Win+L)
  - Even for short leaves from the workplace!
- Sparingly install software and deinstall unused software
  - Also for browser extensions
- Don’t use administrator account for daily use, only when necessary

- Keep software up to date: **Install updates**
  - For the operation system (Windows, MacOS, Linux, etc.)
  - For all used programs (i.e., browser)
- Keep virus protection and firewall of the operation system active

Secure workplace and secure IT infrastructure

Suspicious e-mails and USB sticks

- Be cautious of **suspicious e-mails**
  - Check Sender, mind external e-mail warning
  - Check plausibility of mail, especially for “urgent” requests
  - Open attachments only from trustworthy senders, check type of file

- Be cautious of **unknown USB sticks**
  - USB stick can hide malware and -hardware
    - i.e.: Device disguises as mouse/keyboard and imitates user
  - Don’t connect or use USB sticks of unknown origin

Secure workplace and secure IT infrastructure

Websites and adverticements

- Safe surfing
  - Prefer known and trustworthy websites
  - Check **authenticity** of websites
    (especially spelling of the address: unirostock.de instead of uni-rostock.de?)
  - Be mindful of **encryption** (https://... or lock-symbol)
  - Downloads exclusively from trustworthy sources

- Be careful of **advertisements** (banner ad, pop-ups etc. on websites)
  - Supposed ads can contain malware or phishing-attempts
  - Install Adblocker like *uBlock Origin*

Secure workplace and secure IT infrastructure

Backup and recovery

- Save no private data on work devices
- Protect your data from loss and destruction
  - Instead of saving data locally, safe it on the network drive of the University
  - For local data: create **backups** and **test** recovery!
- PC compromised (or there is a suspicion)?
  - **Warning:** Don't save data from compromised systems!
  - Data could be infected and compromise new/clean devices again

Safety for mobile devices

General safety instructions

- Publication of private mobile phone number only when necessary
- Verify unknown numbers bevor calling back
  (especially mind premium rate numbers like 0900… or foreign county calling codes)

- Install apps only through trustworthy sources
  (Apple App Store, Google Play Store)
- **Install updates:** for operation system and all apps
- If you lose your SIM card or a device with eSim profile: block card or device immediately!

Safety for mobile devices

Storage and transfer

- Don’t leave devices (mobile phone / tablets / laptops / etc.) unattended
  - Unattended devices can be quickly stolen
  - or: malware can be installed fast and unnoticed!
- Don't give devices out of hand
- Report loss / robbery of devices

- *Shoulder Surfing: reading displayed content “over the shoulder”*
  - Privacy filter limits the viewing angles of the display
  - Choose seat with back to the wall
- Confidential conversations only in quiet, private places, if necessary, call back

Safety for mobile devices

Protect devices from unauthorised access

- Activate screen lock and secure it with **PIN** or **password**
  - SIM PIN ≠ device PIN: SIM PIN only protects mobile connection, not the whole device
  - Further use biometry: Fingerprint / 3D face recognition

- Fully encrypt device storage
  - Standard on iOS and Android 6.0 and above with PIN or password
  - Windows: activate BitLocker, Linux: configure dm-crypt + LUKS
  - macOS: Standard with T2- or Apple-Chips, otherwise activate FileVault

Safety for mobile devices

Secure use of public Wi-Fi and devices

- Open (passwordless) WLANs are usually **unencrypted**
  - Traffic can be read without additional protection measures (e.g., HTTPS) , attackers can imitate and manipulate the network
  - Wi-Fi with publicly known passwords should also be treated as unencrypted
  - **Activate the Uni VPN** with profile Internet Access immediately after establishing the Wi-Fi connection (even with encrypted Wi-Fi)
  - **Remove** Wi-Fi from the list of known networks after use to prevent automatic connection
- When using public devices (even CleverTouch): Do not enter or save sensitive data (e.g., passwords), delete other stored data

Passwords

A long password is stronger than a short, complex password!

- **Length of password:** at least 10 characters, better 16 characters
  - 8 Lowercase: Found out in 5 seconds
  - 10 Lowercase: Found out in 1 days
  - 16 Lowercase: Found out in 4.000 years
- **Complexity of password:** Upper- and Lowercase, numbers and special characters
  - 10 Upper- & Lowercase: Found out in 1 months
  - + numbers: Found out in 7 months
  - + special characters: Found out in 5 years
- **Combination:** long and complex passwords are practically impossible to guess
  - complex password with 16 characters: Found out in 10^{12} (1 trillion) years

Passwords

Long passwords aren't secure if they can be easily guessed

- The best passwords are random strings, so all possibilities must be tried to guess them (**Brute-force attack**)

- **Dictionary attacks** exploit the following vulnerabilities to detect passwords much faster than shown on the last slide:
  - *Personal data* like namen, birthdays, car number plate as password
  - *Whole words* which appear in normal dictionaries
    (also, backwards or with characters replaced by numbers such as „p4ssw0rd“)
  - *Keyboard patterns* like „qwerty“ or „asdf1234“ etc.
  - List if the most common or previously compromised passwords, e.g.:
    123456, password, hello, hello123, super123, daniel, michael, …

Passwords

Safe storage

- **Password manager** like *Bitwarden* or *KeePass securely* encrypt and protect passwords with a single, memorized **master password**
- **Never:** Save passwords unencrypted or attach notes to screen, desk, keyboard, etc.!

- **Change** passwords when prompted by system or administrators
- **But:** Never share passwords (admins will never need your password!)

Passwords

Finding and remembering good passwords

- Use **different passwords** for different services
  - In particular separation between private and official
- Password manager can **automatically generate** strong passwords for each service
- To manually generate strong passwords: Choose a long, easy-to-remember phrase and combine initial letters, numbers and special characters:
  - „I have only been buying T-Shirts online since early 2013“ → „IhobbT-Sose2013“
  - Don’t use popular quotes or lyrics! (Dictionary attack)

Confidential Data

All data that is not intended for the public.

- **(Sensitive) personal data:** master data of employees, students, applicants; access identifiers, passwords, usage logs
  - Special protection through data protection laws
- **Intellectual property:** Unpublished research material, copyrighted content in educational materials
  - Degree of protection determined by researchers or authors
- **Business-critical data:** strategic documents, accounting data, foundation data, etc.
  - Only a few selected people with access, otherwise strongly protected

Confidential Data

Handling of confidential data

- **Collection:** *Data minimization* – collect as little data as possible, only as much data as necessary. Data that has not been collected does not need to be protected.

- **Emails:** Send only to known recipients and addresses @uni-rostock.de
  - **As a recipient:** Do not have e-mails forwarded to private addresses
  - **Encryption:** For personal or business-critical data, emails must be encrypted!

- **Cloud:** Only use network and cloud storage and the University of Rostock, no storage on public or external cloud storage

Confidential Data

Signing and encrypting emails

- **Signing** emails protects against identity theft
  - Sender field in unsigned emails is easy to manipulate
  - Correct signature confirms sender and integrity of the message
- **Encrypting** emails protects confidential data from unauthorized access
  - Emails are unencrypted by default
  - Encryption by certificate restricts access to desired recipients

Confidential Data

Request a user certificate

➢ https://zertifikate.uni-rostock.de

- **Simple** certificates are suitable for encrypting and signing emails
- **Extended** certificates are also suitable for signing documents
  - Identity verification by ITMZ employees required (see website)

- Instructions from the ITMZ: https://www.itmz.uni-rostock.de/it-sicherheit/zertifikate-und-verschluesselung/zertifikate-fuer-nutzer/zertifikat-beantragen/

Confidential Data

Setting up a user certificate in an e-mail program

- Instructions from ITMZ for Outlook, Apple Mail and Mozilla Thunderbird
- Outlook Web Client (https://email.uni-rostock.de) is not feasible

- For signing: https://www.itmz.uni-rostock.de/onlinedienste/e-mail-und-kollaboration/e-mail/e-mail-sicherheit/e-mails-signieren/
- To encrypt: https://www.itmz.uni-rostock.de/onlinedienste/e-mail-und-kollaboration/e-mail/e-mail-sicherheit/e-mails-verschluesseln/

Confidential Data

Mail programs to avoid

- Due to the storage of login and mailbox data in the Microsoft cloud, the following mail programs are not recommended for data protection reasons:
  1. The new Microsoft Outlook (2024)
  2. Outlook for Android
  3. Outlook for iOS

- Alternatives can be found on the ITMZ website

Confidential Data

Data protection in the collection of student data

- Central systems of the University of Rostock are centrally managed under data protection law, but self-procured or external systems are not

- Clarify the person(s) responsible for the operation of your own software and data processing and have them approved by data protection officers
- In the case of external systems, bind the provider to aspects relevant to data protection law by means of a **data processing agreement (DPA)**
  - If this is not possible, affected services may not be used!
  - Better to store data on central or own internal servers
- For your own public **web applications:** Imprint and privacy policy!

Confidential Data

Online Services

- **Scheduling:** DFN-Terminplaner – https://terminplaner6.dfn.de/
- **Chat:** Rocket.Chat of Uni Rostock – https://chat.uni-rostock.de/
- **Meetings:** Zoom X on the servers of dt. Telekom – https://uni-rostock-de.zoom.us/
- **LaTeX-Dokumente:** Overleaf of Uni Rostock – https://overleaf.uni-rostock.de/
- **Cloud:** Unibox of Uni Rostock – https://unibox.uni-rostock.de/

Confidential Data

Printer

- Many printed documents are confidential, and other documents often contain personal data: printers and printouts must be protected!

- **Printers can save:** Print jobs are often stored temporarily on internal storage in the printer for a longer period of time and are unencrypted!
- **Network printers are vulnerable:** Preventing access to printers from outside via firewall, often no authentication required to use printers
- **Pick up print jobs immediately:** Printouts that have been in printers for a longer period of time can in principle be taken by anyone. If possible: Restrict physical access to printers.

Handling of security incidents

Definition of "security incident"

- Includes any **breach** of the three confidential data protection objectives
  - *Confidentiality:* Data has been published or accessible to unauthorized persons
    - Email sent/forwarded to wrong person(s)
    - Passwords stolen, access to data with someone else's account
    - Access authorizations to rooms and buildings abused
  - *Integrity:* Data has been manipulated, deleted or (incorrect) data has been added
    - Exam data changed with stolen access data, logs deleted
  - *Availability:* Access to data impossible
    - System failure due to attack or error (not: planned maintenance)
    - Data, passwords or access authorizations lost

Handling of security incidents

Definition of "Major Security Incident"

- Examples of serious incidents:
  - Manual attack on university systems from internal or external
  - Access data for user accounts may be known to unauthorized persons
  - Attackers move through the university network via infected devices
  - Access authorizations have been stolen and/or misused

- Examples of non-serious incidents:
  - Unsuccessful social engineering attacks, infected emails
  - Unsuccessful login attempts from outside the university network

Handling of security incidents

Reporting chain

- Report all security incidents to the responsible system engineer!

- In the case of phishing e-mails or infected e-mails:
  Forwarding to postmasters of the university (postmaster@uni-rostock.de)
- In *potentially* serious cases: also inform the institute management and IT security officer by e-mail (it-sicherheit@uni-rostock.de)
- In *certain* serious cases: inform ITMZ by telephone (5301)
  - ITMZ only handles account / network blocks and log reviews

Handling of security incidents

Urgent measures

- **Prevent spread:** Disconnect compromised devices from the network
  - Remove network cable
  - Disable Wi-Fi, if possible
  - Do not use the device again until it has been approved by IT Security
- **Block access:** Change passwords
  - Especially if the same passwords are used for several services
  - Do not use a compromised device to change your password!
  - Account may be blocked by ITMZ to prevent misuse