Information Security 101

Susan Rösner

Information Security Officer central services

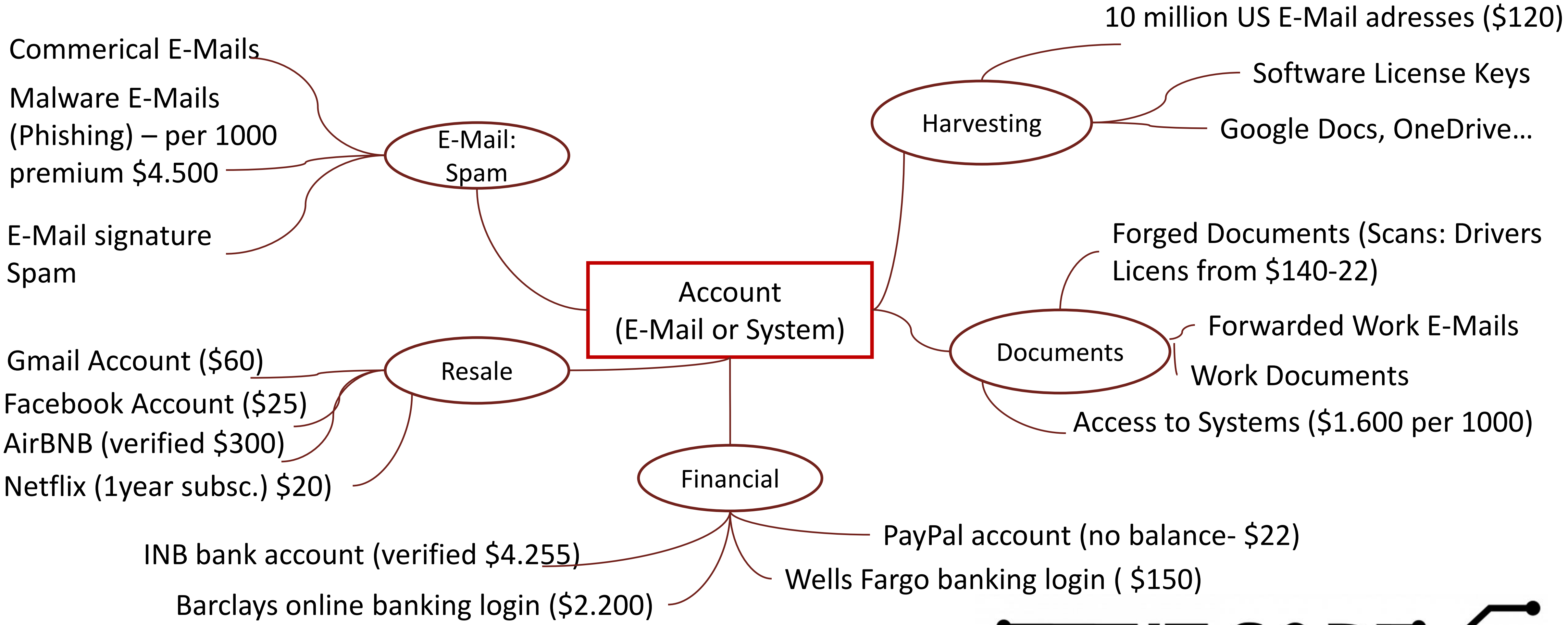
2024-11-07

Stiftung Universität Hildesheim 2003

IT-SAD

IT Security Awareness Days

Information Security 101



Account (E-Mail or System)

E-Mail: Spam

- Commerical E-Mails
- Malware E-Mails (Phishing) – per 1000 premium $4.500
- E-Mail signature Spam

Resale

- Gmail Account ($60)
- Facebook Account ($25)
- AirBNB (verified $300)
- Netflix (1year subsc.) $20)

Financial

- INB bank account (verified $4.255)
- Barclays online banking login ($2.200)
- PayPal account (no balance- $22)
- Wells Fargo banking login ($150)

Harvesting

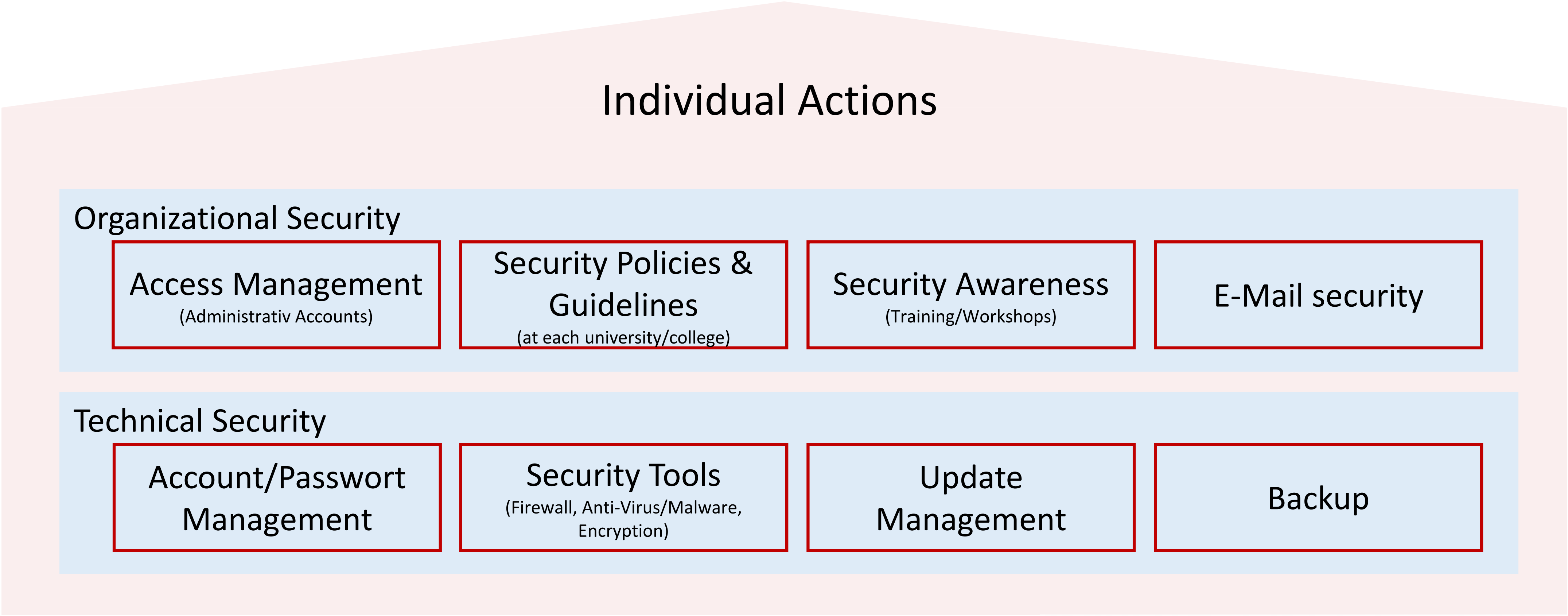
- 10 million US E-Mail adresses ($120)
- Software License Keys
- Google Docs, OneDrive…

Documents

- Forged Documents (Scans: Drivers Licens from $140-22)
- Forwarded Work E-Mails
- Work Documents
- Access to Systems ($1.600 per 1000)

Source: https://www.privacyaffairs.com/
Source: https://krebsonsecurity.com

Information Security 101



Individual Actions

Organizational Security

Access Management
(Administrativ Accounts)

Security Policies & Guidelines
(at each university/college)

Security Awareness
(Training/Workshops)

E-Mail security

Technical Security

Account/Passwort Management

Security Tools
(Firewall, Anti-Virus/Malware, Encryption)

Update Management

Backup

IT-SAD
IT Security Awareness Days

Information Security 101

Stiftung Universität Hildesheim 2003

IT-SAD

IT Security Awareness Days

Agenda

Dos and don‘ts of information security

+ Technical Security
+ Organizational Security
+ Individual Actions

Password Management

- Passwords are the doors to your information - use individual & secure Passwords

  Risk: knowing your passwords allows attacker to take over your identity

  What do do:

  - Lenghts beats complexity (absolut minimum: 12 characters – full complexity)
  - Hackers are human too! Do not use substitation rules
    - f.ex. o=0 | i or l =1 | ! at end of password | pattern in numbers/letters like 2580 or edcgz
    - Not secure: Fireb1rd123! | R0esner-397!
  - Check your password/email: https://haveibeenpwned.com/Passwords
  - Use Password-Manager like Keepass2 (not Browser)

IT-SAD

IT Security Awareness Days

Password Management

- Passwords are the doors to your information - use individual & secure Passwords

  Risk: knowing your passwords allows attacker to take over your identity

  Examples to create passwords:

  - Use Password generators
    - Like in Keepass or https://www.tu-braunschweig.de/it-sicherheit/pwsec
  - Create sentence – take 1st character to create password:
    - Sentence: Today I am holding a session on Information Security 101. It starts at 2:00pm
    - Password: TiahasoIS101.Isa2:00p
  - Create long sentence – longer the better
    - 3birds-1forrest-1city-1desserts

Update management

- Updates are essential!

  Risk: No Updates = No Security. Updates close „doors“ into your system. For example: if you do not update your browser, it is enough to visit a webpage to become infected.

  Malicious code on a webpages tests your browser – finds the vulnerability (open door) and infects your system without you realizing it.

What to do:

- Be aware of End-of-Life (Smartphones, Routers, Wi-Fi stations…)
- Configure to „automatically“ install updates (where possible)
- install security updates at once
- be aware of software without „automatic updates“ –manual check required
- for ALL devices – Smartphones, Smartwatch, Tablets, Laptops, Workstation, Routers (!)…

IT-SAD
IT Security Awareness Days

Security Tools

- Be aware how they work and configure them!

  Risk: Application open door in your Firewall to internet making you vulnerable to attacks OR Anti-Virus (AV) signatures are old – leaving you vulnerable to infected documents…

  What to do:

  - Go to „advanced settings“ in your Firwall – check the applications in there – deactivate them
  - AV: always keep it up to date
    - only works in conjunction with updates !
    - be aware: older viruses might not be detected
    - for employees: Anti-Virus tools are offered (in most universities)
  - be aware of open WLANs - Use VPN for secure communication (ask your technical support for client/configuration)

IT-SAD
IT Security Awareness Days

Backup

- Backup is your insurance against risks

  Risk: through accident (fat finger syndrom), malware attack, or simple hardware error – data may be destroyed.

- What to do?
  - Secure data with backup (data on system, e-mails, key files, …)
  - Offline backup required (for example external harddrive – secure/encrypted!)
  - Be carefull of „Cloud backup“
    - Device or provider gone – Cloud access gone
    - serivce in US – different (privacy) laws apply
    - if it is „free“ – you pay with your data

Information Security 101

Agenda

Dos and don‘ts of information security

- + Technical Security
- + Organizational Security
- + Individual Actions

Access/Passwort Management

- User account vs. Administrative account

  Risk: Malware needs administrative rights to install in background

  What to do:

  - NEVER use an administrative account for daily work !
  - use „normal“ user accounts → privilges that do not exist, cannot be used against you

- Invidiual accounts and passwords

  Risk: Everywhere the same – 1 account/password compromised = everything compromised

  What do do:

  - 1 account per service (shops, support websites, zoom, adobe, newspapers…)
  - 1 account for work
  - use password manager (like KeePass 2) to manage

    - do not use Browser passwordmanager

IT-SAD

IT Security Awareness Days

Security Policies & Guidlines - Clean Desk Policy

- Secure your workspace!

  Risk: sensitive data might get in wrong hands – (malicious) actions using your name could happen, data lost (USB-Sticks)…

  What to do:

  - Check your university for guidelines of the dos and don‘ts
  - Lock your screen (Windows: Ctrl +Alt+Del | MAC: Command +Ctrl+Q)
    → even just to get coffee
  - at end of your work day: secure sensitive data (USB-Sticks, documents…)
  - be aware how to destroy sensitive data (Online – delete sth. is not deletion | sensitive papers do not belong in wastebin)
  - during travel: block your screen

IT-SAD
IT Security Awareness Days

Security Awarness

- Know current common attacks

Risk: without knowing what is going on (new Phishing wave, fraud at amazone through external sellers…) you cannot protect yourself adequately

What to do:

- read known security magazins | news site of your university or maybe mailing list offered by our university
- (Commerical) magazines - for example:

https://www.bsi.bund.de/EN/Service-Navi/service-navi_node.html (see newsletters and press)
https://heise.de/ (nur Deutsch) |
https://www.theregister.com/ (see menu: Patches for vulnerabilities) |
https://www.securityweek.com/ (see Cyber Security News) |
and many more are available

IT-SAD
IT Security Awareness Days

Security Awarness

- ➢ There are no „free“ services

  Risk: you pay with your (personal) data and may infect more people

  Risk: you pay with your compute ressource and may be involved in attack against others

What to do?

- ➢ Read what you accept – don‘t simply accept „OK“ Button
- ➢ check if requested information is relevant for your actions/situation.
- ➢ do you realy need this software? If yes: go to secure (!) webpage like the developer one or known download webpage
- ➢ check what privileges the app wants

E-Mail security 101

- E-Mail security 101

  Risk: Phishing tries to trick you in clicking on links to steal data or passwords or click on attached documents to install malware. Not unsusal that old mails are referenced and are in good english.

  What to do?

  - never react to e-mails (directly) that you have not requested – included links/documents: go to original webpage| check contact details | do not open documents – if document might be relevant aks your HelpDesk
    - Please do not send SPAM Mails to HelpDesk
  - be aware: sender addresses can be faked – trust signed e-mails or check in e-mail header when in doubt (or ask HelpDesk)

Information Security 101

Agenda

Dos and don‘ts of information security

+ Technical Security
+ Organizational Security
+ Individual Actions

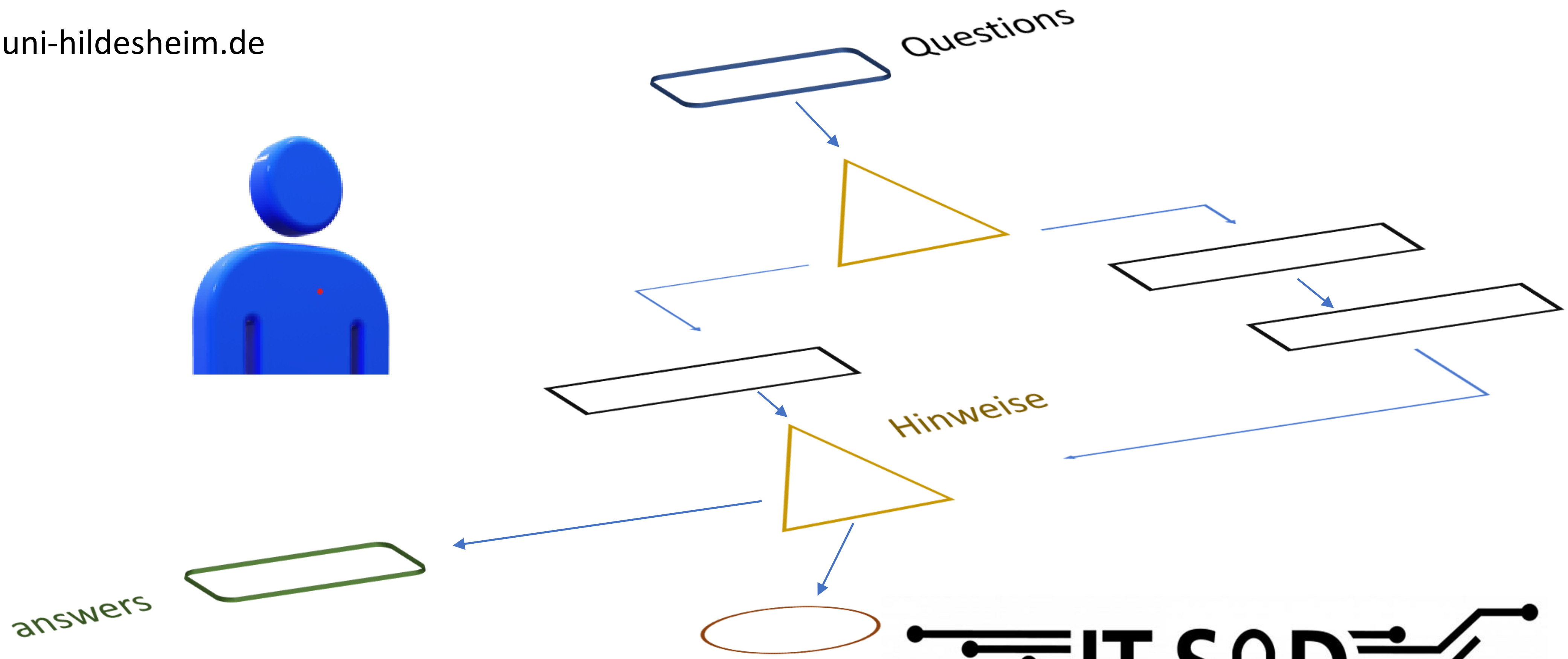
Individual Actions

- Know the price tag of your information
- Be aware what information you provide and where (Social media, Chat/support groups, cloud services)
- Be helpful to others – a co-worker does something that might compromise his system – tell them, they might not be aware of it.
- secure your system at home otherwise the same might happen: „kindergarden kid orderd electrical child car on amazon“

IT-SAD
IT Security Awareness Days

Fragen

Susan Roesner
it-sicherheit[@]uni-hildesheim.de



IT-SAD
IT Security Awareness Days