

Information Security Awareness



Daniel Hauswirth, CISO

Speaker notes

Welcome to VSHN's information security awareness education.

The employees of a company are an important link in the chain of information security. Therefore it is important, that VSHNeers are aware of possible threats and risks using IT.

In this presentation I would like to give some insights about information security with the goal to make you aware of security risks.

Agenda

1. General
2. Your Device
3. Cloud / IT Tools
4. Human
5. Physical
6. Summary

Speaker notes

In today's education we are going to show general Information Security awareness topics.

I don't assume it is complete and if you have additions, feel free to add them at the end or contact me later.

This is the first education concentrating fully on awareness, so it is intended to grow over time.

Today we are going to dive in to five areas.

Firstly, there will be a general overview.

Second, I show you some risks on your device.

Then some information about IT tools in VSHN are shown.

And with point 4 and 5 we dive into the human and physical side.



And in the end a summary as usual in a presentation.

1 - General

Speaker notes

In this section I'm going to talk about general threats in information security. I will quickly explain some common terms and general threats to the information security.

Viruses / Malware / etc

- Malware (Malicious Software)
 - Harmful software
 - Includes viruses, spyware, adware, and more.
- Spyware 
 - Gathers information from users without their knowledge
- Virus 
 - Often attaches to legitimate programs
 - Can replicate itself
- Worm
 - Standalone, replicates itself

Speaker notes

I'd like to explain some terminology regarding viruses and malware.

Malware (Malicious Software): Malware is a broad term for any software designed to harm or exploit computers, networks, or users. This includes viruses, spyware, adware, and other harmful programs intended to steal sensitive information, damage systems, or gain unauthorized access.

Spyware: Spyware is a type of malware that secretly gathers information about a person or organization without their knowledge. It can capture keystrokes, monitor online activities, and collect sensitive data, posing a significant threat to privacy and security.

Virus: A computer virus is a malicious software program that can replicate itself and spread to other computers. It often attaches itself to legitimate programs, causing damage to files and disrupting normal computer operations.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers

Worms/Viruses Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Ransomware

- Malicious software
- encrypts files, demanding a ransom for their release.
- How It Works:
 - Infection: phishing emails, malicious downloads, or software vulnerabilities (e.g. your NAS in WWW)
 - Encryption: Locks files, making them inaccessible to the user.
 - Ransom Demand: Displays a message demanding payment (usually in cryptocurrency) for a decryption key.
- Prevention Tips:
 - Backup
 - Updates
 - Don't get phished
 - Don't let your NAS unprotected in the WWW

Speaker notes

Ransomware is a special type of malware. It is a malicious software that encrypts files, demanding payment for their release. So if you manage to get infected by ransomware, it will encrypt your files, so you cannot access them. The attacker helps you to decrypt the file if you pay them some money, a ransom. Usually that's paid in bitcoin or similar currencies.

How It Works:

Spoofing

- A technique used by attackers to falsify information, creating a false sense of trust or authenticity.
- Types of Spoofing
 - Email Spoofing
 - Website Spoofing
 - E.g. www.atlassian.com (note the **L** is actually an **I**)
 - Caller ID Spoofing

Speaker notes

Spoofing can be, somebody trying to impersonate somebody you trust. Like you know all the mails you get from a fake Markus in your inbox ;-)

- Some types of Spoofing:
 - Email Spoofing: Attackers send emails with falsified sender addresses, often used in phishing attacks.
This is probably the most seen in user scope, e.g. daily a mail is coming pretending to be someone else
 - Website Spoofing: Creating fake websites to trick users into disclosing sensitive information. E.g. banking sites that looks similar and the domain name use characters that looks similar to others. Example www.atlassian.com (note the L is actually an I)
 - Caller ID Spoofing: Falsifying phone numbers to appear as trusted entities in phone scams.
- Implications:
 - Spoofing can result to unauthorized access or financial losses. Meaning, that if you are tricked into a wrong banking page and enter your credentials, then the attacker gets your passwords and could login and lock you out.
 - Reputation's damage for VSHN, e.g. if somebody acts as VSHN and sends mails with our vshn.ch addresses outside to external parties.
 - In case of website spoofing a password manager already helps, as it does not autofill in spoofed web sites.

(source chat GPT, wikipedia, Daniel's historical knowledge)

Phishing

Attempts to trick people into revealing sensitive information such as usernames, passwords or financial details.

Speaker notes

Phishing are attempts to trick people into revealing sensitive information such as usernames, passwords or financial details. Called phishing, because they try broadly like with fishing nets and hope that some single fishes are taking the hook.

- Introduction:
 - Phishing involves tricking attempts to obtain sensitive information through tricks and manipulation.
- Common Tactics:
 - Email Spoofing: Attackers falsify sender addresses to appear trustworthy.
 - Fake Websites: Phishers create convincing replicas of legitimate sites to deceive users. The one I already mentioned in Spoofing. Where www.atlassian.com is written with a capital I looking like a lowercase L.
 - Urgency and Threats: Creating a sense of urgency or fear to manipulate quick responses. That's also something you see in mails we get from a "fake CEO", where they say it is important and you need to act quickly.
- Indicators of Phishing:
 - Be careful with unusual sender addresses, spelling mistakes, and unsolicited requests for sensitive information.
 - Check the mail address you get the mail from
 - If they contain URLs, hover over the URL in the mail and check, where it will be redirected.
 - If you get an unexpected request, please be careful. Nobody in VSHN will ask you via mail to create a payment. And if so, please quickly call them or write via chat.
 - The spelling was often an indicator that it could be a phishing attempt. But with ChatGPT I doubt that the will make lot of spelling errors. Much

CEO Fraud

- Special form of Phishing → spear phishing 🎯
- Authorised employee is tricked into submitting a fraudulent invoice or an unauthorised transaction via the business account
- Signs:
 - Fraudsters pretend to be management persons
 - Unusual email, phone, fax, text message
 - Pressure (super urgent...), threats or unusual flattery
 - Request for confidentiality
 - Contradiction to internal procedures
 - Markus wants you to buy Apple gift cards

Speaker notes

Introduction: Already mentioned before. CEO Fraud is a specialized form of phishing, targeting individuals within an organization.

Modus Operandi: In CEO Fraud, an authorized employee is tricked into carrying out a fraudulent action, such as submitting a fake invoice or making an unauthorized transaction from the business account.

Signs of CEO Fraud:

- Impersonation of Management
 - Fraudsters often pretend to be executives or other high-ranking individuals to gain trust and authority.
- Unusual Communication Methods:
 - Be mindful for communications via email or text message that seem out of the ordinary.
 - If somebody ask you via mail to pay something but you usually communicate via chat with that person, you should verify, whether that's ok or not.
- Pressure Tactics:
 - Look out for urgent requests, threats, or unusual flattery designed to manipulate quick responses.
- Request for Confidentiality:
 - Fraudulent requests may stress the need for confidentiality to avoid detection.
 - So if they say you should pay something but do not tell anybody, that's a real sign something is fishy.
- Contradictions to Internal Procedures:
 - Be wary of instructions that go against established internal procedures or protocols.
- Unusual Requests (e.g., Gift Cards):
 - Markus want you to buy gift cards is a good example of that.

2 - Your Device

Speaker notes

Your device is really important for keeping information safe. It's like the first line of defense against bad stuff happening. Your personal choices on the device can either protect or risk important data. So, by being aware of that and ensure to keep your device safe, you're helping to make sure our organization stays secure.

Browser Tips

- Be careful with add-ons, some recommended ones:
 - uBlock Origin (ensure to choose the original)
 - Privacy Badger
- Use of Browser containers, e.g. in Firefox
 - e.g. for sysadmin work
 - e-Banking in a different container, browser, profile
- Have a different browser ready which is clean

Speaker notes

Add-ons for browsers are to be handled in the same way as other software, install it only after assessing if it's reliable.





I recommend two add-ons, namely uBlock origin and Privacy Badger.

- uBlock Origin is a free and open-source browser extension for content filtering, including ad blocking. It helps keep you safe online by stopping harmful ads and scripts, and by blocking known malicious websites. As a bonus, pages could load faster by blocking unnecessary elements and it increases privacy by preventing tracking.
- Privacy Badger is a browser extension that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web.

I further recommend to use different containers for different work. For your everyday browsing you could use your main browser container. For sys-admin tasks, e.g. being logged in as Administrator of Jira / Gitlab / Chat, you could use a different container. Like that, you are still logged in with your personal all day credentials in your main browser container and do admin task explicitly in a different one. Same for ebanking and other tasks that should not be in connection with your other browser work.

Instead of different containers also a different browser is possible or different profiles. My workflow here is, that I use brave browser for clean browsing, e.g. for private ebanking or if I have to test something on our Keycloak for someone with a VSHN Account. I use containers in Firefox for admin tasks. And as backup browser I have chromium.

Updates

- Ensure you update your system regularly 
- Ensure to update your tools regularly, such as Zoom 
- In VSHN every VSHNeer is responsible themselves to keep their machines up to date 
- Your browser must be always up to date
- To do for you today 
 - Check if your Zoom client has an available update
 - Check update settings of your OS

Speaker notes

Software is never bug free. If there are unclosed vulnerabilities e.g. in your browser, they could be exploited for example with a drive-by download on a malicious site.

Therefore it is very important that you always update to the latest fixes of all your used software.

Your duties: (see slide)

1. Update your system regularly
2. Update your tools regularly (such as Zoom)
3. You are responsible for your machine to be up to date. Corp IT does not have control over your device.
4. Your browser must be always up to date

To do for today:

- check if your zoom is up to date
 - Update it if it has update
- Check how your OS is updated. Do you have an automatically update configured?

Backup

- You're responsible for a backup
 - Store your data on Nextcloud
 - Local data backed-up in an encrypted way
- Backup for your Password manager

Speaker notes

You are responsible for backing up your local data.

I recommend to store your files on Nextcloud. You could use Nextcloud's sync program so you could store the data in your file system and it is synced automatically.

Most important part to have access to your password manager. Having all your data stored in Nextcloud, and you have access to your password manager, you are able to switch to a new machine if your current one is corrupt.

An example: In case of a ransomware infection the only solution is, to full clean the laptop and set it up freshly. In such a case if you have had local data, you need to restore a backup. If you don't have local data and everything is on Nextcloud or other VSHN infrastructure, then you could just use a fresh installed device and start using it. What would be important in this case is to have a backup of your password manager, with that you would be able to restore your stuff to work with.

Please contact Corporate IT if you are unsure about your backup and your password manager business continuity management.

Password Manager

- Use a Password Manager for your personal passwords
 - e.g. Bitwarden
- Passbolt is only for shared passwords
- Remember your Master Password
- + Auto-fill functions
- + You only need access to your password manager to setup a new device to work with

Speaker notes

See also the internal education from Finn from 2023-08-31 -> files.vshn.net/index.php/f/661851

You must use a password manager for your personal work passwords. We use Passbolt for our VSHN shared passwords. For personal passwords we recommend Bitwarden. Please come to Corp IT if you need support in setting up a password manager.

Important is, that you always remember your Master Password. This is crucial, that you could login again to your account. If you want to write down your master password, writing it with pen and paper (only the password), putting it in an envelope, and "seal" it, could be an appropriate fail safe. You must ensure that only the master password is there, without your login email, with that somebody who accidentally get your sealed password, cannot login.

A big plus of such a password manager is, that it auto-fill passwords in the browser. This improves the workflow in logging in. And second plus is, that you only need your password manager to get another system running, because all your data is somewhere stored on a remote system.

Encrypted Disk

- Your disk must be encrypted
 - Ensured during initial setup
 - If you are unsure, contact Corp IT to check
- Prevents access to files if stolen
 - Shut down better than standby

Speaker notes

According to our [Acceptable Use Policy](#) disks must be encrypted which is usually done during the setup on your first working day. You have to ensure that the disk is encrypted, if not please contact Corporate IT so it can be fixed. If you are unsure if your device uses encryption, then please come to Corp IT too.

With an encrypted disk the data is safe from being accessed. If the laptop is in standby, there are high sophisticated ways to get the decryption key out of your RAM, so a shut down laptop is better in case of loss or theft. With that our loss of your device is only a matter of financial loss and we don't share secrets with a thief.

Cloud and IT Tools

Speaker notes

VSHN's corporate IT provides some tools for the normal office work. The following slides should provide an overview where we are supposed to store data.

Further we gonna explain what cloud tools exist and how we are supposed to use them.

VSHN's IT Tools

Speaker notes

Nextcloud is our main data storage service. We — that is Polaris — run it ourselves at cloudscale.ch. We ensure backups and encryption and here we have the whole data sovereignty

Mail

- SGO is the front end you see the mails. It also is a groupware and stores calendar data.
- Behind the scenes couple of servers for mail handling, run by Polaris and owned by corp IT

Wiki

The main documentation must go to Wiki at wiki.vshn.net. The wiki is the internal documentation. If you have something to document that is longer living and public, the handbook is the place to go.

Jira

All task planning is done in our Jira on ticket.vshn.net

Google Cloud

Long lasting data like contracts should be in Nextcloud. Google cloud is more used as collaboration system, if you need to work on an excel sheet together. We should no store confidential data there.

Client Tools

- Client tools e.g. Mail Clients in responsibility of the User
 - Groupware client Thunderbird recommended
 - Outlook opens problems
- There is no standard and controlled setup yet
 - this means, the every VSHNeer must ensure secure and updated system
 - contact Corporate IT if we should support you here.

Speaker notes

If you need tools on your client to work with mail and calendar you can do that. It remains in the responsibility of yourself. As a groupware client we recommend Thunderbird. Please don't use Outlook as we in Corp IT cannot help with any of the hundreds of problems.

We don't have a standardised setup yet. Every VSHNeer is their own boss on their client. This reflects the VSHN style of work, but brings a lot of responsibility for the user.

You have to ensure your system is safe and secure. If you need help here, please contact Corporate IT. We can help you to find a solution.

AI/Language Tools (1/2)

- Tools
 - Chat GPT
 - Copilot
 - Language tool
 - DeepL
- Use it with caution (see rules next slide from [AUP 4.2](#))
- Copilot as of now not allowed
 - All code would be shared with github, including secrets
 - A proper policy and implementation guideline needed first; contact me if you're interested to define such thing.

Speaker notes

The new thing on the IT horizon are the AI tools like Chat GPT. In similar category do fall language tools, like deepL.

You must act with caution when using them. We have it regulated in [AUP 4.2](#).

E.g. if you use ChatGPT you must not enter sensitive data. Please don't enter Company names or VSHNeer names into chatGPT without consent. If I want to write something using chatGPT I replace VSHN with CORP in my request, so I could later change. Everything you enter there, could be reused to train their artificial intelligence model, so I would prefer to not let it know too much of myself.

With language tools it is similar. If you use a translator or spell checker that sends every word you type to their server, they could basically know everything you write the whole day, even your private conversations in a chat. Therefore our policy forbids to use the tools in that way.

Same for Copilot from Github. As of now the policy is to not use it. If you integrate it directly in your IDE, then it shares all code with github, also the secrets we store there (unfortunately). If you have exact use cases how to use it and how to configure, please come to the ISMS work group, and we will define a standard, which is allowed to use.

AI/Language Tools (2/2) — Rules

Speaker notes

This is a summary of our policy regarding AI and Language tools.

-→ see slide

Human

Speaker notes

- Even with advanced technology, people are really important for keeping information safe.
- Human error is the most vulnerable link of the security chain
- All technology does not help if there are malicious or negligent misconduct.
- The following slides should help you to understand, where some vulnerabilities are lying in the human part of information security

Social Engineering

What is Social Engineering?

- Manipulative tactic targeting individuals.
- Exploits psychology, not just technical vulnerabilities.

Examples

- Spam Calls: Beware of unsolicited calls seeking personal info.
- CEO Fraud (already mention)
- Try to get information in person

Protection Tips

- Verify Identities: Confirm before sharing info.
- Be Skeptical: Question unexpected requests; verify through trusted channels.
 - If contacted by mail, check via chat or zoom

Speaker notes

Explanation of social engineering

Social engineering is a tactic used by attackers to manipulate individuals into revealing sensitive information or taking certain actions. It exploits human psychology rather than relying on technical vulnerabilities.

Examples

Spam Calls: Be careful of unprompted calls, especially those asking for personal or financial information. Attackers often use tricky tactics to mislead people. The CEO scam mentioned earlier is another example of social engineering. And if someone approaches you personally and tries to find out information about the company, this is also a relevant attack vector.

Protection Tips

1. Verify Identities: Before sharing any information, verify the identity of the person or organization contacting you. Reputable companies will not be bothered by your caution.
2. Be Skeptical: Question unexpected requests, especially those urging urgent actions. Verify through trusted channels before complying, e.g. ask via chat if you get a special email

Key Message

Stay watchful against social engineering attempts, including spam calls. Awareness and skepticism are powerful tools in protecting yourself from manipulation.

Business Secrets

- Avoid sharing business information during informal settings, like social gatherings.
- Social Media: Be cautious about disclosing sensitive details online.
- We have several non-disclosure agreements (NDA) with customers, best approach do not talk about customers
- ❗ There are also some hard laws (such as Bankgeheimnis) we have to follow anyway.
- ⚡ Some customers want that our employees acknowledge some of the law articles, see [Annex to the Declaration of Confidentiality](#) in the handbook

Speaker notes

You have to handle Business Secrets carefully.

For example in social gathering don't tell strangers about anything in VSHN, which isn't public. E.g. avoid to name customer names and avoid to tell too much how our systems are running.

Please don't post sensitive stuff on social media. Rule of thumb, if you are unsure, don't post it ;-)

We have couple of NDAs with customers. We must not share details about such customers and their systems. Therefore your first approach must be, don't speak about customers with non-VSHNeers.

IMPORTANT: There is the Bankgeheimnis and also the Strafgesetzbuch and other laws. You have to follow them anyway, but we have some customers that want us to confirm, that our employees know about those laws. Please see [Annex to the Declaration of Confidentiality](#) in the handbook and read those.

Email Security Tips (1/2)

Be on Your Guard

- Be certain of who sent it

Spelling Errors

- Common in phishing attempts

Need for Urgency

- Time-sensitive calls to action create panic and bad choices.
- Extra caution for emails with imminent deadlines.

Check Before You Click

- Hover over a link to see the real URL.

Speaker notes

Email is a good entry point for social engineering and all other attack vectors. Links could be sent to guide you to a manipulated website to trick you to enter credentials or with some scripts using vulnerabilities in your browser.

Therefore some tips regarding email from ISF (www.securityforum.org/)

-> see slides

Email Security Tips (2/2)



Who Sent It?

- "From:" field can be spoofed to appear elsewhere.
- Small typos can make it look like the email is from someone else.

Personal Information

- Unexpected requests for personal info should be treated as suspect.
- 💡 Financial institutions will never ask you to supply personal information or click a link to access your online account.

Copyright ©

- Regulated in the [Acceptable Use Policy, Section 8](#)
- Users must not make unauthorized copies of software.
-  Do not copy unauthorized software or material; users are responsible for legal consequences under intellectual property laws.
 -  e.g. copy random images from the internet and use it publicly

Speaker notes

Copyright is something not directly relevant for attacks or data loss in regards of information security. But important to adhere as we have to follow the law and regulations which is also part of the C-I-A triad (confidentiality, integrity, availability).

Rules regarding copyright are documented in the AUP in Section 8; actually a lot of your responsibilities is documented in that AUP as you may have noticed during today's presentation.

You must not download and use copies of software you don't have the license to use. E.g. don't install a cracked photoshop on your laptop. It must be licensed.

Also you are not allowed to copy text and pictures without authorisation and use it as your own. You must not use images from some random source and use it publicly.

You should also not use VSHNeer pictures in any place but vshn.ch/team, without consent of the VSHNeer to use that image.

Physical Security

Speaker notes

The last category of today's presentation is the physical security.

In the next five slides I'm going to show you something about:



1. Clear desk and clear screen Policy
2. Office Rules
3. Work from home Rules
4. USB stick Usage
5. Work from outside of Switzerland.

In our famous [AUP, in section 4.3](#), we have regulated the rules for clean desk and clean screen.

If you are not at your desk, all paper documents that could contain sensitive data, must be removed from the desk and other locations (printer, copier, etc.) to prevent unauthorized access. Sensitive paper documents and media must be stored securely in accordance with the Information Classification Policy.

If you are not at your desk, sensitive information must not be displayed on the screen. That means, you have to lock your screen every time you leave your desk. If your lock screen is a blurred screen, it must be ensured that no data can be shown. I would not recommend such a blurred lock screen.

Clear Desk and Clear Screen Policy

- Regulated in [AUP 4.3](#)
- Keep your workspace tidy to prevent unauthorized access to sensitive data.
- Store sensitive information securely when not in use 
- Always lock your screen when not on the desk 

Office Rules

- Regulated in [ISMS Physical Security Policy](#).
- Office in Neugasse 10 is considered a security perimeter.
- VSHNtower is considered as public 🏢
 - Not leave data lying around
 - always close the office door.
 - Ensure visitors are never left alone.
 - Visitors need to fill a visitor form.
- 📄 Paper must be stored in a locked filing cabinet ("Aktenschrank")
- 🪟 Ensure windows are closed end of day.
- 🎭 Ensure no confidential paper is lying around.
- ⌨️ 🔑 Check your keyboard's physical connections (keyloggers)
- 🏢 Keep VSHNtower clean of information

Speaker notes

The physical access is regulated in the [ISMS Physical Security Policy](#). In this policy everything important regarding the office in terms of the ISMS is documented, it's worth reading.

In general we say, that the Office in Neugasse 10 is considered inside the ISMS scope, that means it has to be secured. We don't have locked office boxes for everything and there could be information lying around, such as customer information, documents, etc. They actually should be handled carefully anyways, but having for example a flipchart from a retro with some names on it is a possible thing to have. Therefore, it is important to...

- Not leave data lying around
- always close the office doors
- don't leave customers and non VSHNeers alone in the office.
- Visitors need to fill a visitor form
 - This rule implements the ISO requirements.
 - It follows the good enough approach.

Further all VSHNeers must ensure:

In work from home the same rules apply as in the office for your device. Other residents in the house must not have access to data on your device, therefore also the screen lock applies.

The devices must be supervised, meaning that you should lock the laptop in your home.

Work from Home Rules

- Follow security principles applied in the office.
- Keep the home office area secure and organized.
- Your device must be supervised at home, also screen lock applies.

Work on the Go

- Be careful in public spaces such as trains or coffee shops.
 - There could be people watching your screen.
 - See social engineering earlier this presentation.
 - Use a physical screen privacy filter if you work often in public spaces.
- Lock your screen when not actively using your device.
- Supervise your device, don't leave it alone.
- Prefer your hotspot instead of a random WiFi.

Speaker notes

If you work in public spaces you must take care that you don't share data with others. Try to work with back to a wall and in train that nobody sits next to you. Information revealed like that could always be used for threats like Social Engineering we discussed before.

Also here applies the screen locking rule.

Don't leave your device unattended. So if you are in a coffee shop working and need a break, make sure your laptop cannot be stolen.

Use your phone hotspot instead of some random WiFi you cannot trust. There could be metadata they get from your connections. A VPN is possible to redirect all data through it, contact Corporate IT if you want a VPN for your device.

USB Stick Usage

- Be cautious with USB sticks; avoid unknown devices.
- Only use trusted USB from VSHN's stock.
- USB flash drives may only be used for:
 - Creating bootable sticks to install or run operating systems.
 - Personal/private data.
 - Business data where there is no alternative, for example quotations.



It is explicitly forbidden to use USB flash drives that came from an unverifiable origin or were given as promotional gifts.



Speaker notes

You have to be cautious with USB memory sticks and other external media. You must not plugin unknown devices. Plugging in a malicious devices could infect your laptop with malware, like described in the beginning of this presentation.

- USB flash drives may only be used if they come from VSHN's stock in the storage room or if they were bought from a reputable shop and are still in the original, unopened package.
- USB flash drives may only be used for:
 - creating bootable sticks to install or run operating systems.
 - personal data.
 - business data where there is no alternative, for example quotations.

It is explicitly forbidden to use USB flash drives that came from an unverifiable origin or were given as promotional gifts.

Work Outside Switzerland

- Absolutely follow the [Checklist for Working from Abroad](#).
- Customers may lose their banking license if access is done from outside Switzerland.
- See the page [Definition of "Leistungserbringung"](#) which customers have that rule.

Speaker notes

Unfortunately some customers may only be operated from Switzerland. Mainly banking customers have this requirement. They refer to Swiss Financial Market Supervisory Authority FINMA regulations. They could lose their banking license if customer data is processed outside Switzerland.

We don't have enough technical safeguards to avoid that. And as every engineer has root rights, they would be able to connect to servers where sensitive data is stored. We solve that requirement with organisational measures. Engineer outside Switzerland must follow the rules and the checklists provided in the [Definition of "Leistungserbringung"](#).

Summary

Speaker notes

Now we came to an end of the presentation. The main goal of this presentation was to raise awareness regarding information security. The most important part in the security chain is the human and being aware threats and security helps to secure that possible vulnerability.

Review

We had a look at these security topics today

Speaker notes

Today I tried to give you an overview about the following topics regarding awareness.

General

General threats were shown and introduced, as Virus / Malware / Phishing / CEO fraud. Most important takeaway is to be always careful. Never trust strange emails, don't click on links if you are not 100% sure what mail you are looking on.

Your device

Your device as your daily tool is also crucial part of the security chain. Threats like Ransomware and Viruses can be mitigated if you use an updated system and some support from browsers to block known malicious pages.

Cloud / IT Tools

In the cloud / IT tools section we've seen the tools we use at VSHN in cloud and locally. We further did a small excursion in AI tools and the security concerns here. Most important takeaway, don't share too much with AI and store your documents on VSHN owned systems.

Human

Some important points are in the human factor. With social engineering hacker could get to important information to later use to get into systems. If you reveal too much info to other persons, they could use this against VSHN. Here you must be as watchful as in emails. Always be on guard to know who the counterpart of your conversation is.

Physical

Thank you for your attention.

I hope I brought the awareness in the information security topic a bit closer to everybody. I hope you are now aware of the fact, that the most important part in security are you as the users of our systems.

Please don't hesitate to contact me or every other person in the ISMS WG if you have questions regarding information security.

Please don't hesitate to contact Corporate IT if you need support using our systems or configuring your device securely.

Thanks!



Daniel Hauswirth, CISO – daniel.hauswirth@vshn.ch

VSHN AG – Neugasse 10 – CH-8005 Zürich – +41 44 545 53 00 – vshn.ch – info@vshn.ch

Questions?

Speaker notes

I'm now open for questions.

Please feel free to contact me if you think I told nonsense.

Feel free to pose questions via chat or during a coffee talk, actually coffee talk would be more appreciated.

...

Thank you and enjoy your day.