



**INNOCISE**

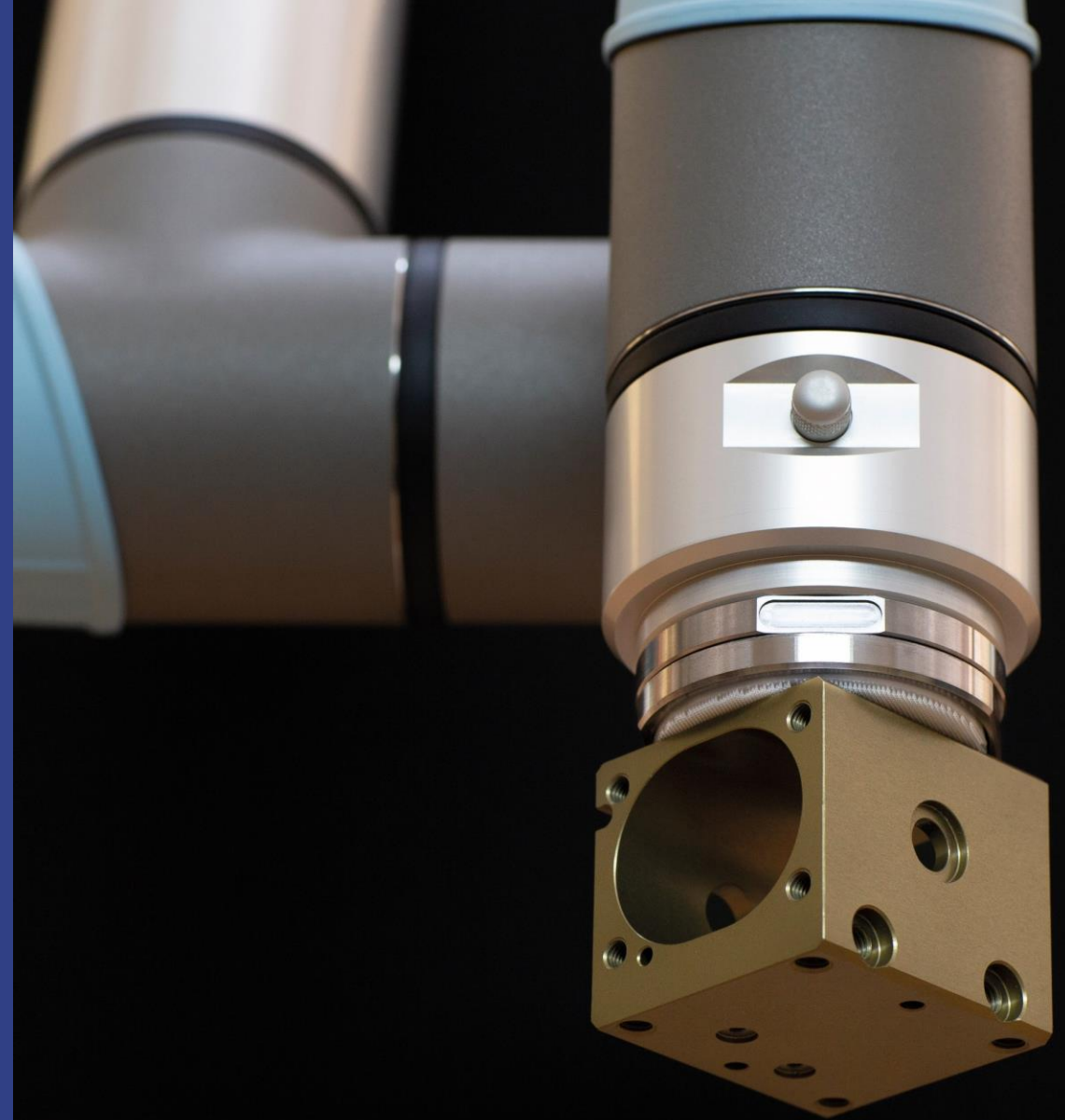
Precise Handling Solutions

# We turn Robots into Geckos

IT Training

Bakhtiar Ali Shah

Henrik Ollmann



# Topics

- **Archived Training Materials**
- Cyber Attack types (New)
- Recap (Quiz)
  
- GPT Prompts
- What is GPT
- Where does it come from?
- How the magic numbers work?
- Transformer
  
- Useful Shortcuts(Windows)



# General rules










- Keep your **passwords safe**
- Lock your screen before leaving (**Windows + L**)
- Follow the rules for **e-mail safety**
- Do not use **private storage media** of any kind
- Do not copy company data to **external services**
- Do not visit **unsafe websites**





# IT-Services and Applications



## On-Premise

- ERP 
  - CRM 
  - OpenProject 
  - GitLab 
  - INNOCLOUD 
  - HelpDesk 
  - INNO-GPT 
  - File-Server 
  - 3CX 
- › Cisco Phone

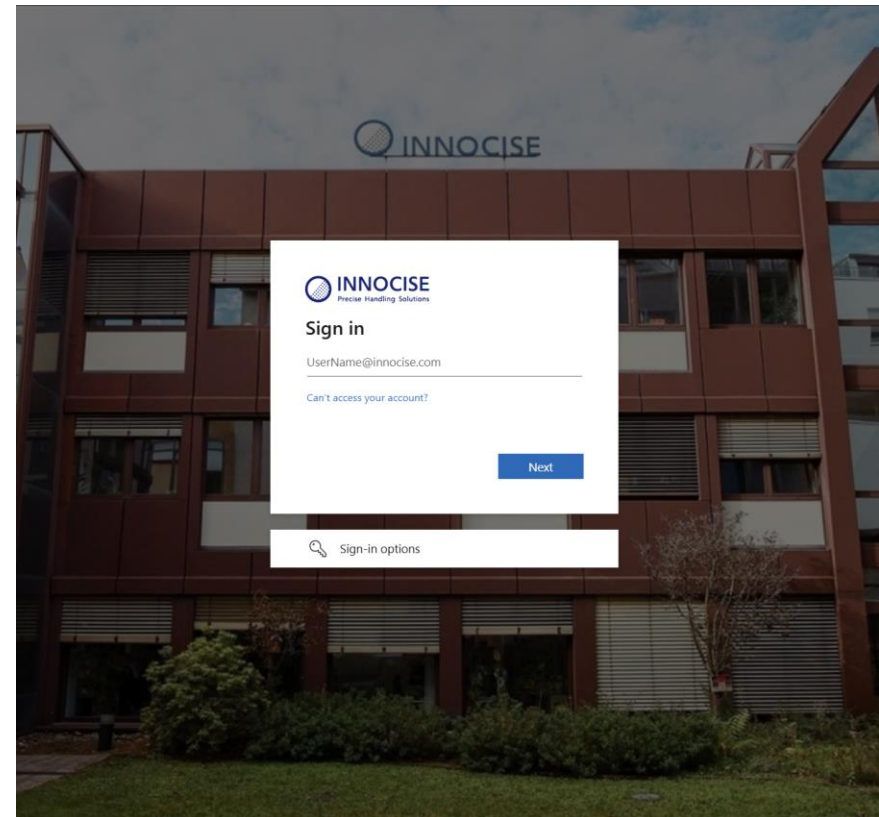
## Cloud

- HRWorks 
  - Q.Wiki 
  - Datev 
  - Microsoft 365 
- › E-Mail

# E-Mail



- Internal login: Via Outlook
- External login: [link to Login:](#)
  - › From trusted computers only
  - › Make sure that the INNO-Logo is present
  - › Use your username and add @innocise.com
  - › Click next and enter your password
- Use [this](#) template to setup your signature
  - › A How To can be found [here](#)
  - › Replace content in brackets first
  - › Remove brackets





- **INNOCISE Cloud:**

- › <https://cloud.innocise.com/>



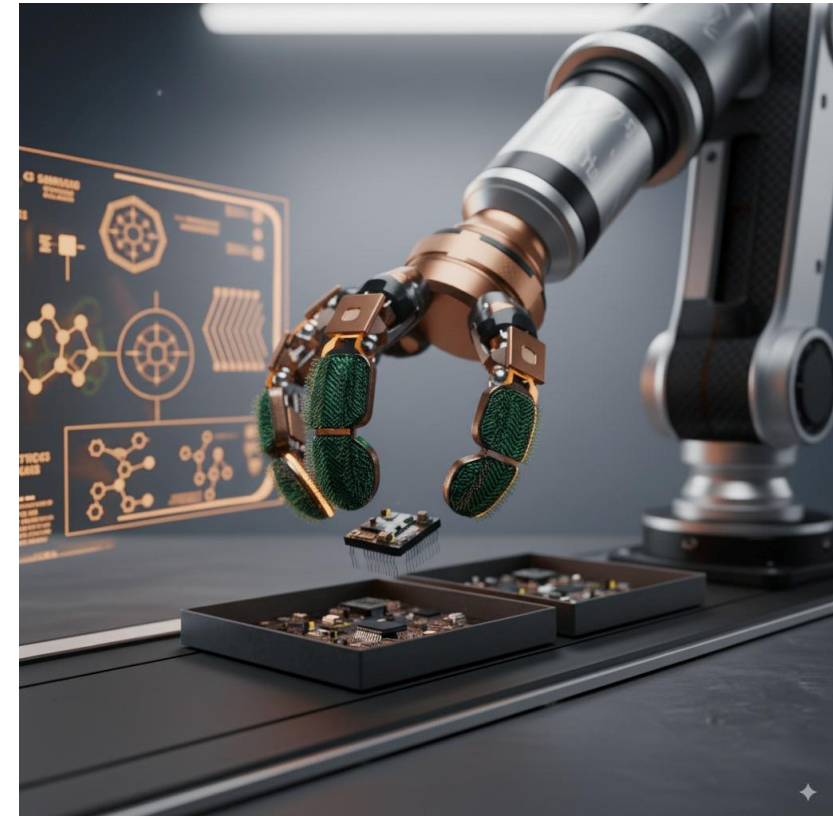
- › share files with people outside INNOCISE



- › Plan tasks with deck



- › Store Passwords



# HomeOffice



- Login: [INNOCISE GmbH](https://www.innocise.com/portal/webClient/index.html#/)



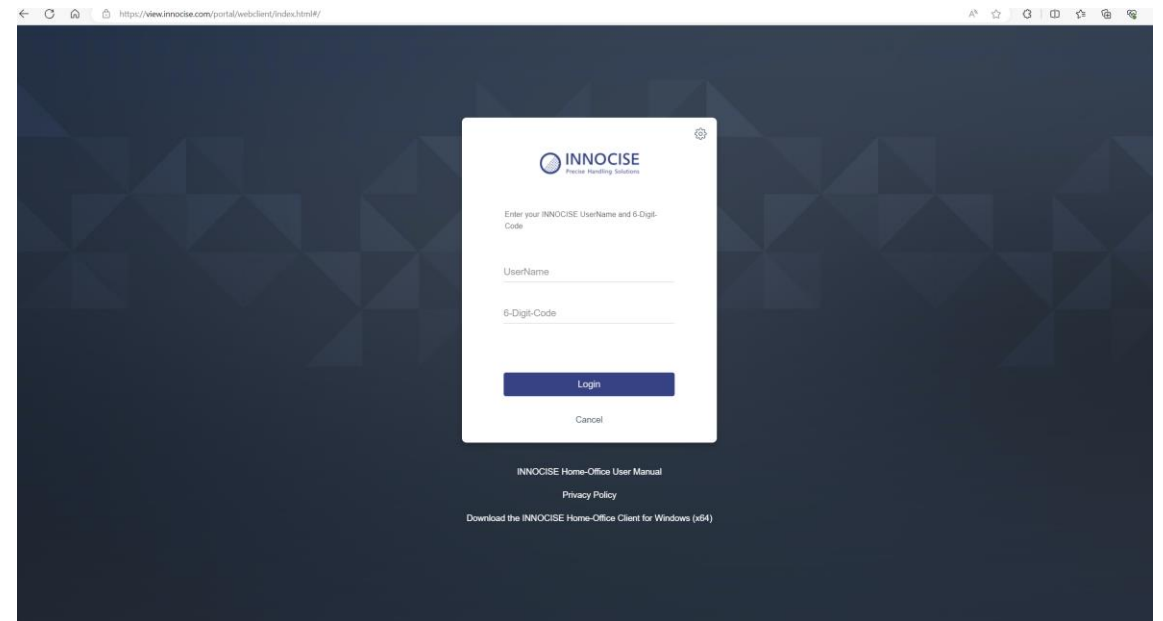
› From trusted computers only



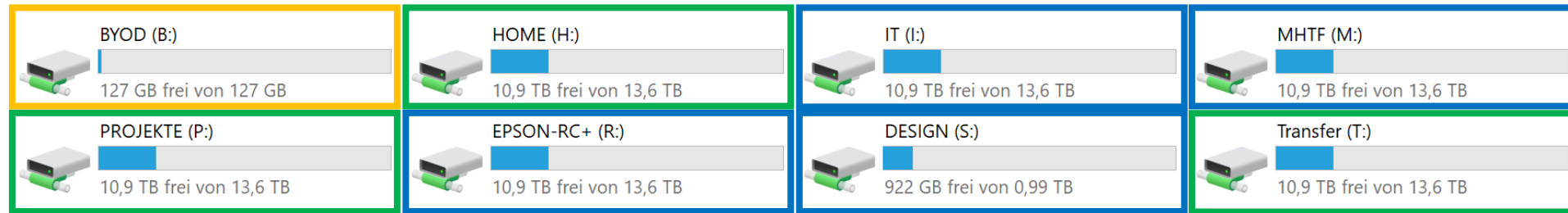
› TOTP required (Passcode)



› Use „HomeOffice“ to connect to available Remotedesktop



# File-Server and Drives



- **Green** always visible
- **Yellow** visible if you use a personal computer in the office
- **Blue** visible if you are part of dedicated usergroups
- Templates for presentations / documents / etc. can be found at [T:\ ALLGEMEIN\Vorlagen](T:\ALLGEMEIN\Vorlagen)

# WiFi



- Connect your private devices to: INNOCISE-GUEST
  - › SSID: INNOCISE-GUEST
  - › Password: **#INNO-Gu3\$tN3t#**
  - › or scan the QR-Code available in many offices



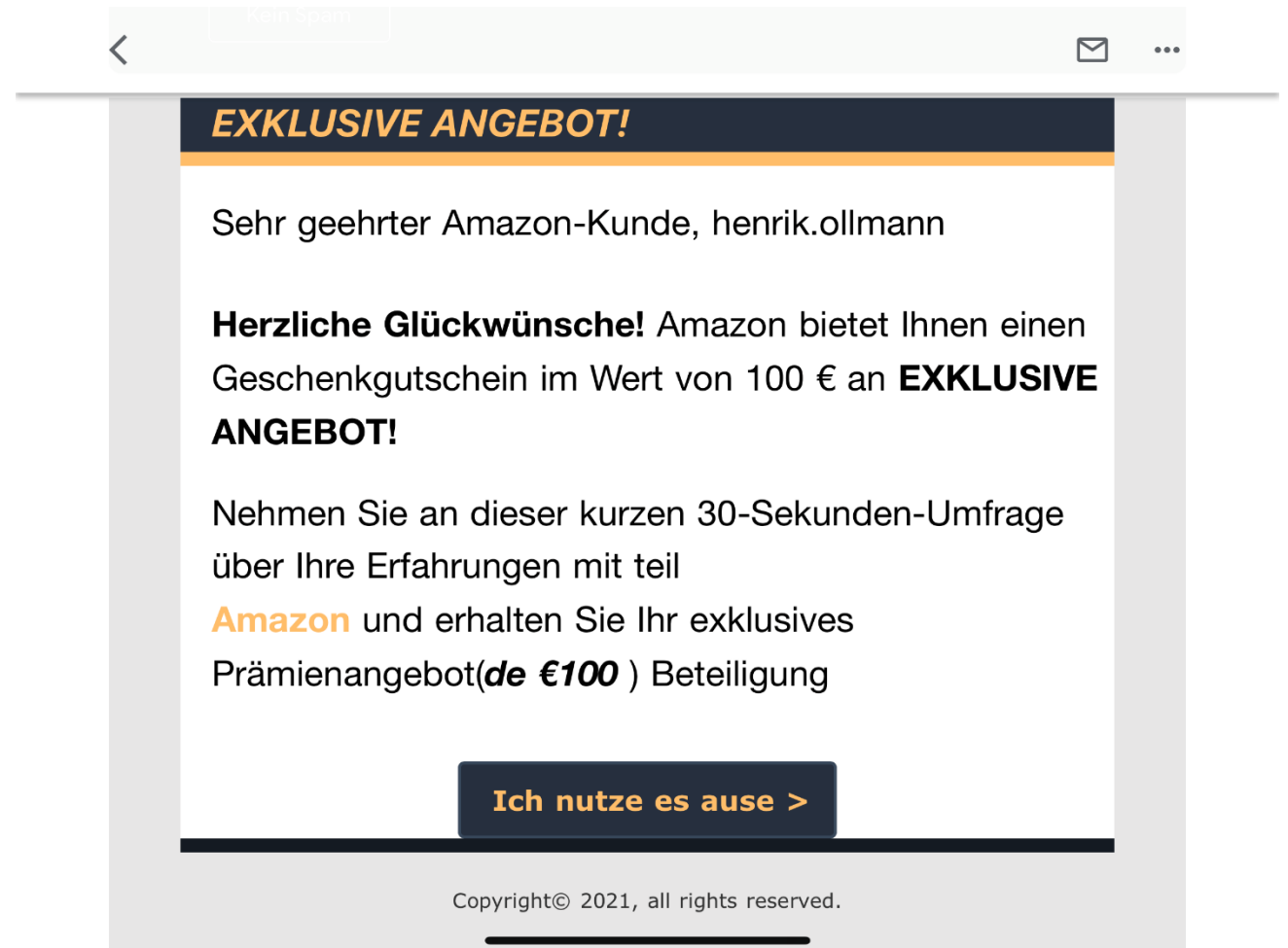
# E-Mail safety



# Phishing



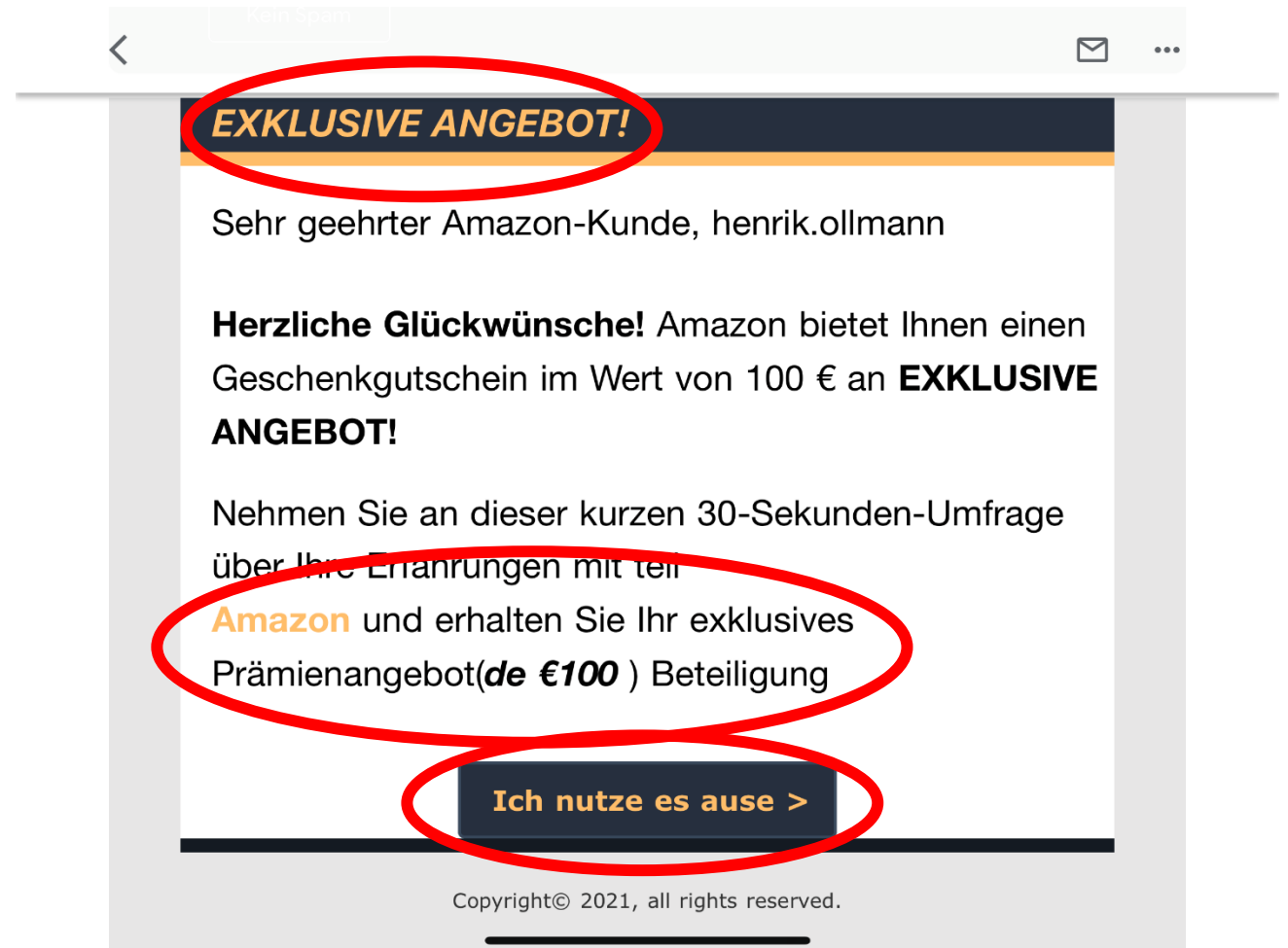
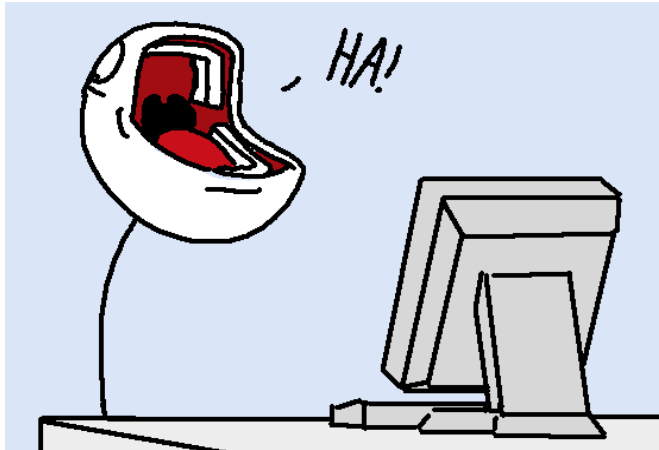
- It usually starts with simple SPAM-Mails



# Phishing



- It usually starts with simple SPAM-Mails



# Phishing



- These become elaborate phishing attacks

## **Wir steigern Ihre Sicherheit!**

**Lieber Sparkassen Kunde,**

Ihr Sparkassen-Konto wurde aufgrund von Inaktivität deaktiviert. Um es zu reaktivieren, besuchen Sie bitte nachfolgendes Formular und folgen Sie den Anweisungen.

[Reaktivierung](#)

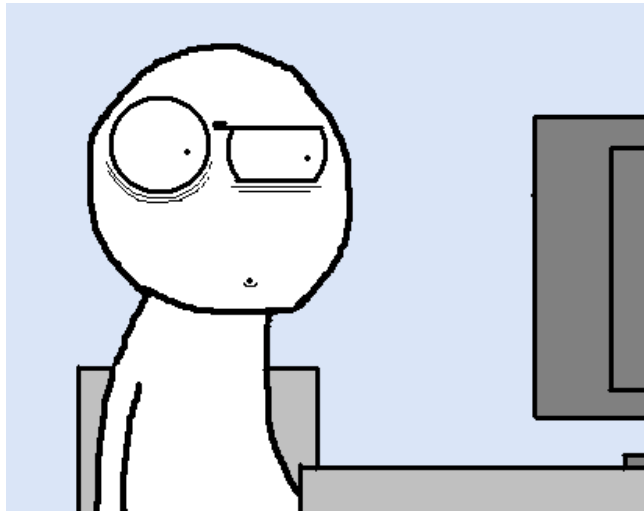
Für dringende Rückfragen sind wir Montag bis Freitag von 08.30 bis 19.00 Uhr und Samstag von 09.00 bis 14.00 Uhr für Sie da.

Mit freundlichen Grüßen  
Sparkasse Servicecenter

# Phishing



- These become elaborate phishing attacks



Henrik (Symbolbild)

## **Wir steigern Ihre Sicherheit!**

**Lieber Sparkassen Kunde,**

Ihr Sparkassen-Konto wurde aufgrund von Inaktivität deaktiviert. Um es zu reaktivieren, besuchen Sie bitte nachfolgendes Formular und folgen Sie den Anweisungen.

[Reaktivierung](#)

Für dringende Rückfragen sind wir Montag bis Freitag von 08.30 bis 19.00 Uhr und Samstag von 09.00 bis 14.00 Uhr für Sie da.

Mit freundlichen Grüßen  
Sparkasse Servicecenter

# E-Mail safety



- Check sender before opening a mail
- Check indicator on the top:

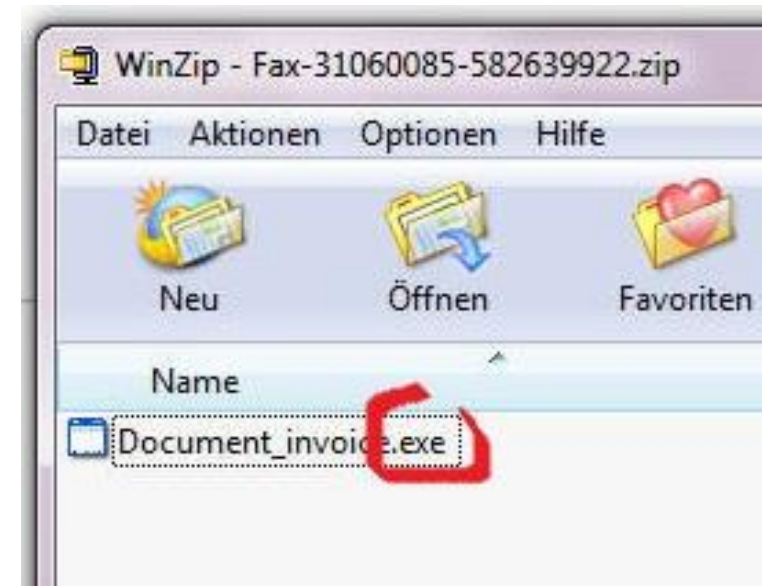
**INFORMATION:** This is an EXTERNAL email. Please take care when clicking links or opening attachments. When in doubt, contact INNOCISE IT.

**CAUTION:** This is an EXTERNAL email with a **suspicious subject or content**. Verify sender **before** clicking links or opening attachments. When in doubt, contact INNOCISE IT.

**WARNING:** This is an EXTERNAL email with a **highly suspicious subject or content**. **Do not click on any links or open attachments!** Please inform INNOCISE IT.

- Do not open unsafe attachments
- Check links by hovering before clicking
- Do not click on unknown links

→ **Contact IT if you're not sure**



# E-Mail safety



Di 13.06.2017 11:33  
David Coons <David.Coons@rasmussen.edu>  
: ITS Help-desk

An

Dear Staff/Employees,

We are migrating all email accounts into Outlook Web App 2017 and as such all active Account Holder are to verify and Log in for the upgrade and migration to take effect now. This is done to improve the security and efficiency due to recent spam mails received.

Click ( [Upgrade](#) ) Account to migrate and block further Spam mails.

Best Regards,  
ITS Help-desk  
Office of Information Technology Services (ITS)

Di 13.06.2017 11:33  
David Coons <David.Coons@rasmussen.edu>  
: ITS Help-desk

An

Dear Staff/Employees,

We are migrating all email accounts into Outlook Web App 2017 and as such all active Account Holder are to verify and Log in for the upgrade and migration to take effect now. This is done to improve the security and efficiency due to recent spam mails received.

Click ( [Upgrade](#) ) Account to migrate and block further Spam mails.

Best Regards,  
ITS Help-desk  
Office of Information Technology Services (ITS)

<http://www.imxprs.com/free/supperwiseone/web-mail-portal>  
Klicken oder tippen Sie, um dem Link zu folgen.

→ Always check the sender and links by hovering over them **WITHOUT** clicking

# Topics

- Archived Training Materials
- **Cyber Attack types (New)**
- Recap (Quiz)
  
- GPT Prompts
- What is GPT
- Where does it come from?
- How the magic numbers work?
- Transformer
  
- Useful Shortcuts(Windows)



# Common Cyber Attack types we should know



- **Phishing**

- › Fake emails or messages to steal info or spread malware
- › Don't click unknown links or attachments

Re : PayPal Security Alert!: Latest Login added Informed from Tokyo, Japan (Bestellung Mobile Legends) ... Tuesday, October 20, 2020. #51961060 [FWD]

secure@intl-limited.com <mailsecuredaccounts-lvp6dgrzqr@keyosens.com>

Tue 10/20/2020 4:39 PM

To:user-7688988021@live.summary.com <user-7688988021@live.summary.com>



Your PayPal account has been limited.

Hi Dear Customer,

We just wanted to let you know that a recent Unauthorized login was found in your Paypal account Which is blocked successfully.

You can't use your account at the movement Please Verify And Secure your account by following link

Verify Now

Kind regards,  
PayPal Service

This email was sent to keep you informed about changes to your products or accounts.  
Copyright 1996-2020, Paypal.com, Inc. or its affiliates

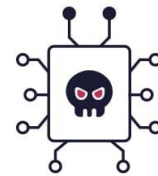


# Common Cyber Attack types we should know



- **Malware**

- › **Malicious software** damaging systems or stealing data
- › Only download **approved software**, avoid **unknown USBs**



**VIRUS**  
Spreads between computers



**WORM**  
Spreads between computers in one company or location



**TROJAN**  
Sneaks malware onto your computer



**SPYWARE**  
Steals your data



**ADWARE**  
Spams you with ads



**RANSOMWARE**  
Encrypts files and blackmails you



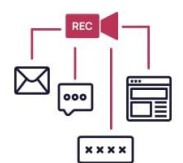
**FILELESS MALWARE**  
Operates in your system's memory



**ROOTKIT**  
Gives remote access to your device



**BOTNET**  
Turns your PC into a puppet



**KEYLOGGER**  
Records user activity

# Common Cyber Attack types we should know



- **Social Engineering**

- › Tricks to get **confidential** info via **calls, emails, or in person**
- › Always **verify** requests for **sensitive information**

## Social engineering explained

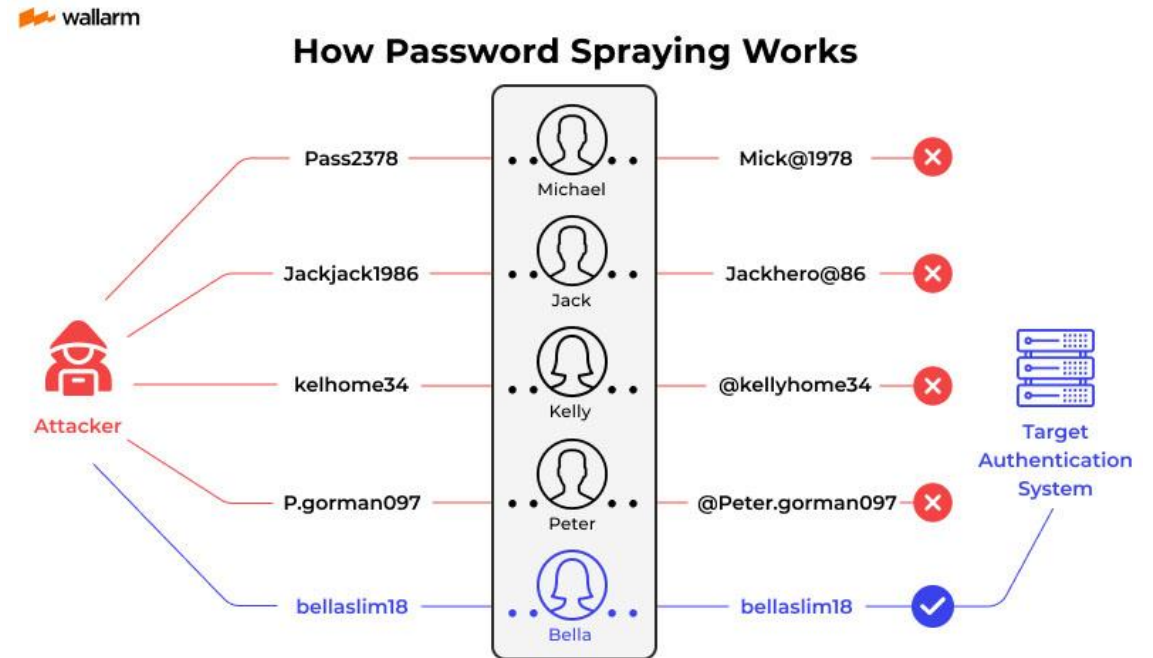


# Common Cyber Attack types we should know



- **Password Attacks**

- › **Guessing** or **stealing** passwords
- › Use **strong, unique passwords** + Multi-Factor Authentication (MFA)

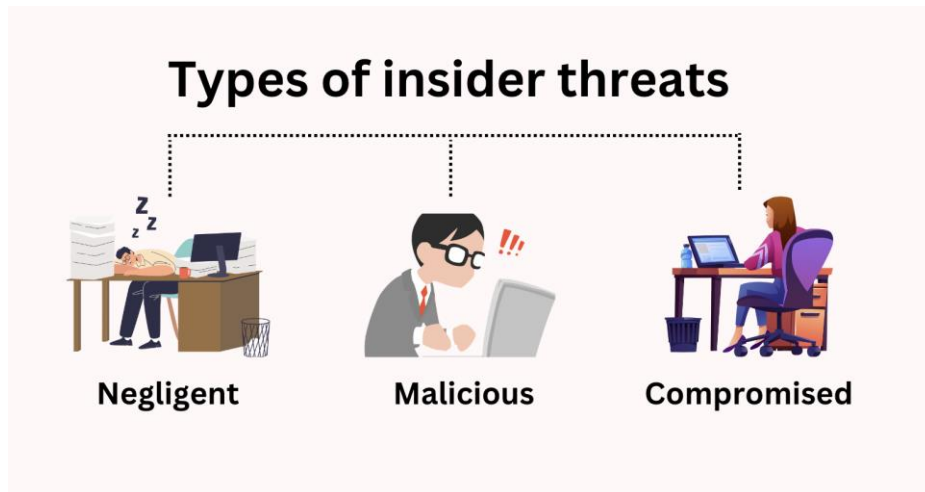


# Common Cyber Attack types we should know



- **Insider Threats**

- › Risks from within the company, intentional or accidental
- › Handle data carefully, report suspicious behavior



## TYPES OF INSIDER THREATS

**Malicious:** Individuals within the company who intentionally cause harm or give out sensitive data.

**Compromised:** Individuals who have, despite their best efforts, have been compromised by an outside threat. Credentials are often stolen or phished.

**Negligent:** Employees who neglect to protect their login information or fail to follow proper security and IT procedures, which leaves the organization vulnerable.

**SWIMLANE**

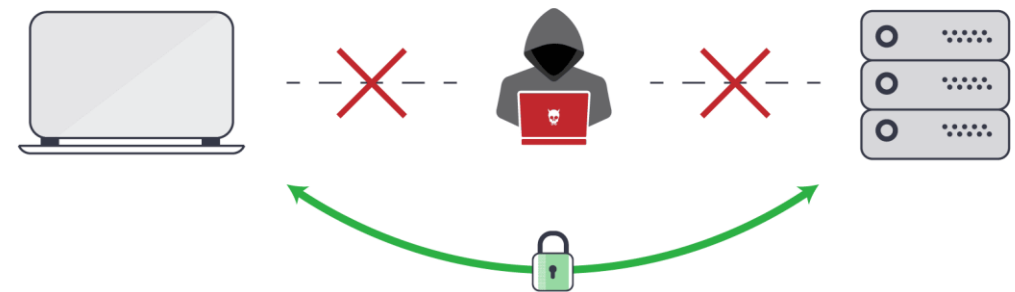
# Common Cyber Attack types we should know



- **Man-in-the-Middle (MitM)**

- › Intercepted communications to **eavesdrop** or **alter** info
- › Use **secure networks, HTTPS** and **VPNs** when needed





## Avoiding **Man-in-the-Middle** Attacks



# Best Practices



- **Verify sender** before opening emails
- Use **strong passwords & MFA**
- Avoid **unauthorized** software and devices
- Report **suspicious activity** to IT immediately

<p><b>VERIFY SENDER BEFORE OPENING EMAILS</b></p> 	<p><b>USE STRONG PASSWORDS &amp; MFA</b></p> 
<p><b>AVOID UNAUTHORIZED SOFTWARE AND DEVICES</b></p> 	<p><b>REPORT SUSPICIOUS ACTIVITY TO IT IMMEDIATELY</b></p> 

# Topics

- Archived Training Materials
- Cyber Attack types (New)
- **Recap (Quiz)**
  
- GPT Prompts
- What is GPT
- Where does it come from?
- How the magic numbers work?
- Transformer
  
- Useful Shortcuts(Windows)



## Quiztime (1 / 7)



If you receive an email attachment from a colleague that you were not expecting, it's safe to click on the attachment because you know the sender.

True or False

## Quiztime (2 / 7)



As long as I keep my antivirus up to date, I can safely open attachments.

True or False

## Quiztime (3 / 7)



It is OK to leave your unlocked computer behind in the conference room when you leave to get a cup of coffee.

True or False

# Quiztime (4 / 7)



Imagine you do banking online at InnoBank. A friend posts about a new rewards program on social media and includes a link to the signup page. Which of the URLs listed is likely to be a safe link to that page:

1. <http://tinyurl.com/innobank>
2. <https://innobank-rewards.com>
3. <https://innobank.com/rewards>
4. If your friend posted it, any link is safe

## Quiztime (5 / 7)



When building a strong passphrase, you can use a famous quote or movie line because it's easy to remember but still long enough to be strong.

True or False

# Quiztime (6 / 7)



You are browsing the Internet. Which of the pop-up windows is safe to click on if it appears during your session.

1. An ad for free movie downloads
2. An alert prompting you to scan your PC for viruses and spyware
3. A reminder to update your browser
4. None are safe

## Quiztime (7 / 7)



Peter uses the USB charger built into the desk in his hotel room to charge his laptop.

Risky or Safe

# Topics

- Archived Training Materials
- Cyber Attack types (New)
- Recap (Quiz)
  
- **GPT Prompts**
- What is GPT
- Where does it come from?
- How the magic numbers work?
- Transformer
  
- Useful Shortcuts(Windows)



# GPT Best practices for prompt engineering



## Better

- Use the latest model
- Separate instruction and context eg `"""` or `###`

```
Summarize the text below as a bullet point list of the most important points.
```

```
Text: """  
{text input here}  
"""
```

## Less Affective

```
Summarize the text below as a bullet point list of the most important points.
```

```
{text input here}
```

# GPT Best practices for prompt engineering



**Better** 

- **Specific, Descriptive and Detailed**

Write a short inspiring poem about OpenAI, focusing on the recent DALL-E product launch (DALL-E is a text to image ML model) in the style of a {famous poet}

**Less Affective** 

Write a poem about OpenAI.

# GPT Best practices for prompt engineering



Better 

- **Articulate the desired output format through examples**

```
Extract the important entities mentioned in the text below. First extract all company names, then extract all people names, then extract specific topics which fit the content and finally extract general overarching themes
```

Desired format:

Company names: <comma\_separated\_list\_of\_company\_names>

People names: -||-

Specific topics: -||-

General themes: -||-

Text: {text}

Less Affective 

```
Extract the entities mentioned in the text below. Extract the following 4 entity types: company names, people names, specific topics and themes.
```

Text: {text}

# GPT Best practices for prompt engineering



Better 

**Start with zero-shot, then few-shot, neither of them worked, then fine-tune**

Extract keywords from the below text.

Text: {text}

Keywords:

Less Affective 

# GPT Best practices for prompt engineering



Better 

**Start with zero-shot, then few-shot, neither of them worked, then fine-tune**(no discussion)

```
Extract keywords from the corresponding texts below.
```

```
Text 1: Stripe provides APIs that web developers can use to integrate payment processing into their websites and mobile applications.
```

```
Keywords 1: Stripe, payment processing, APIs, web developers, websites, mobile applications
```

```
##
```

```
Text 2: OpenAI has trained cutting-edge language models that are very good at understanding and generating text. Our API provides access to these models and can be used to solve virtually any task that involves processing language.
```

```
Keywords 2: OpenAI, language models, text processing, API.
```

```
##
```

```
Text 3: {text}
```

```
Keywords 3:
```

Less Affective 

# GPT Best practices for prompt engineering



**Better** 

- **Reduce “fluffy” and imprecise descriptions**

Use a 3 to 5 sentence paragraph to describe this product.

**Less Affective** 

The description for this product should be fairly short, a few sentences only, and not too much more.

# GPT Best practices for prompt engineering



## Better

- Instead of just saying what **not** to do, say **what to do instead**

The following is a conversation between an Agent and a Customer. The agent will attempt to diagnose the problem and suggest a solution, whilst refraining from asking any questions related to PII. Instead of asking for PII, such as username or password, refer the user to the help article [www.samplewebsite.com/help/faq](http://www.samplewebsite.com/help/faq)

Customer: I can't log in to my account.

Agent:

## Less Affective

The following is a conversation between an Agent and a Customer. DO NOT ASK USERNAME OR PASSWORD. DO NOT REPEAT.

Customer: I can't log in to my account.

Agent:

# GPT Best practices for prompt engineering



Better 

- **Code Generation Specific - Use “leading words” to nudge the model toward a particular pattern**

```
# Write a simple python function that
# 1. Ask me for a number in mile
# 2. It converts miles to kilometers

import
```

Less Affective 

```
# Write a simple python function that
# 1. Ask me for a number in mile
# 2. It converts miles to kilometers
```

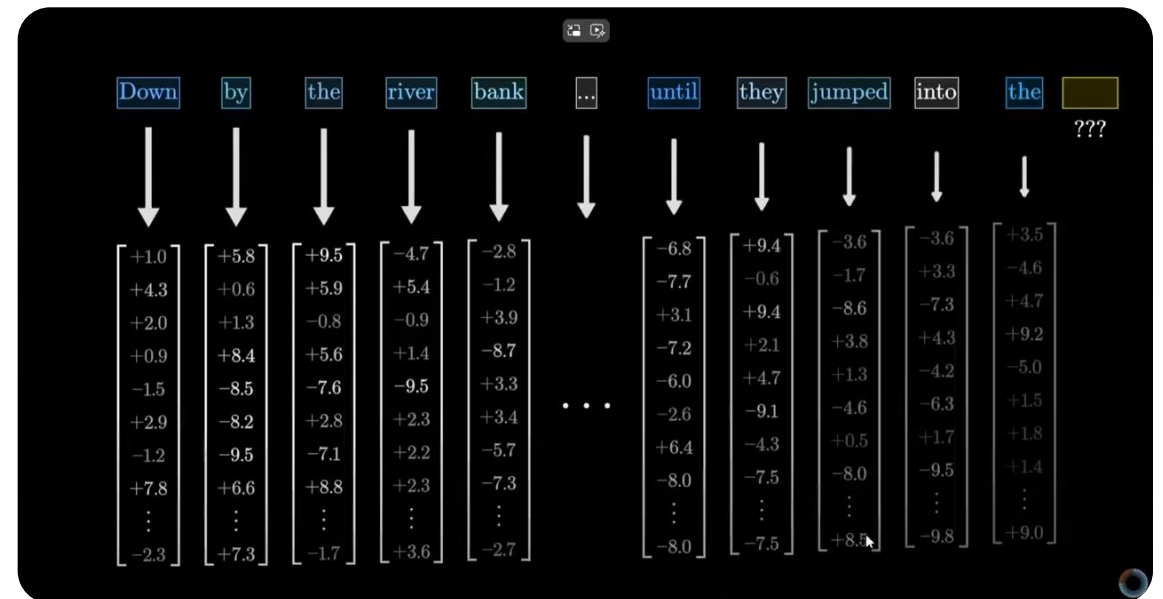


# Understanding AI and GPT: Some Insights

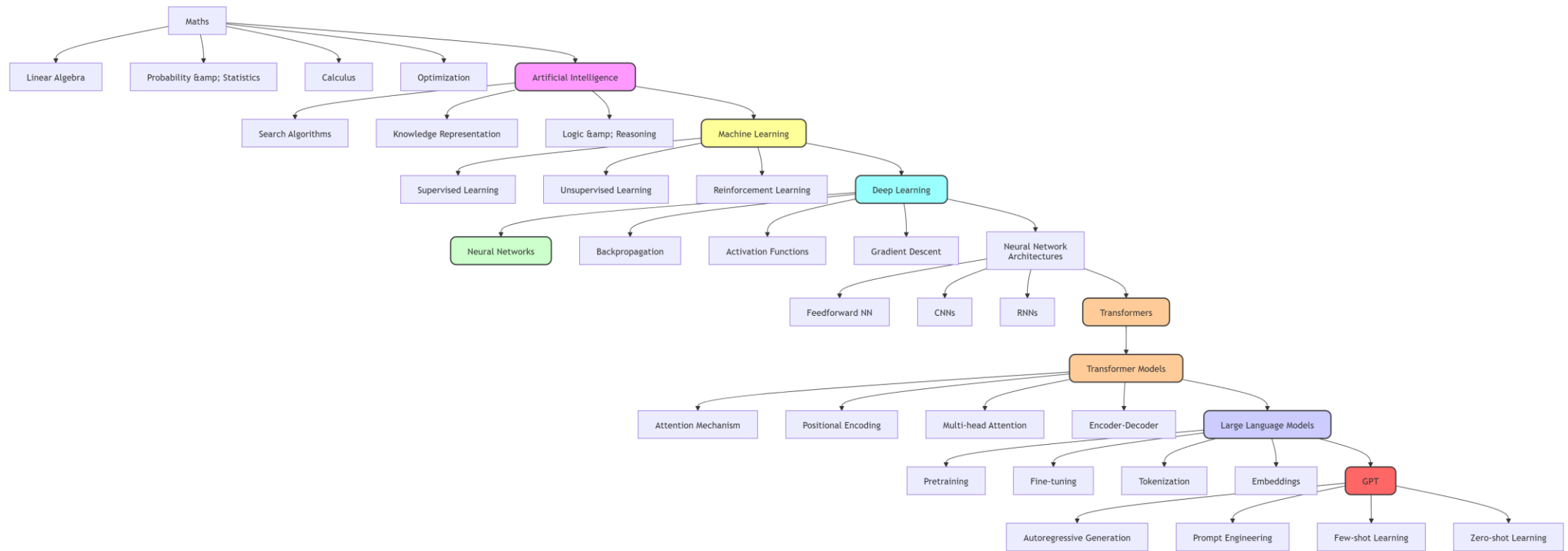


## GPT

- **Generative Pre-trained Transformer**
  - LLM (Large Language Model)
    - Output is non-deterministic
- [Transformer Explainer: LLM](#)  
[Transformer Model Visually Explained](#)



# GPT



# Few Useful Shortcuts

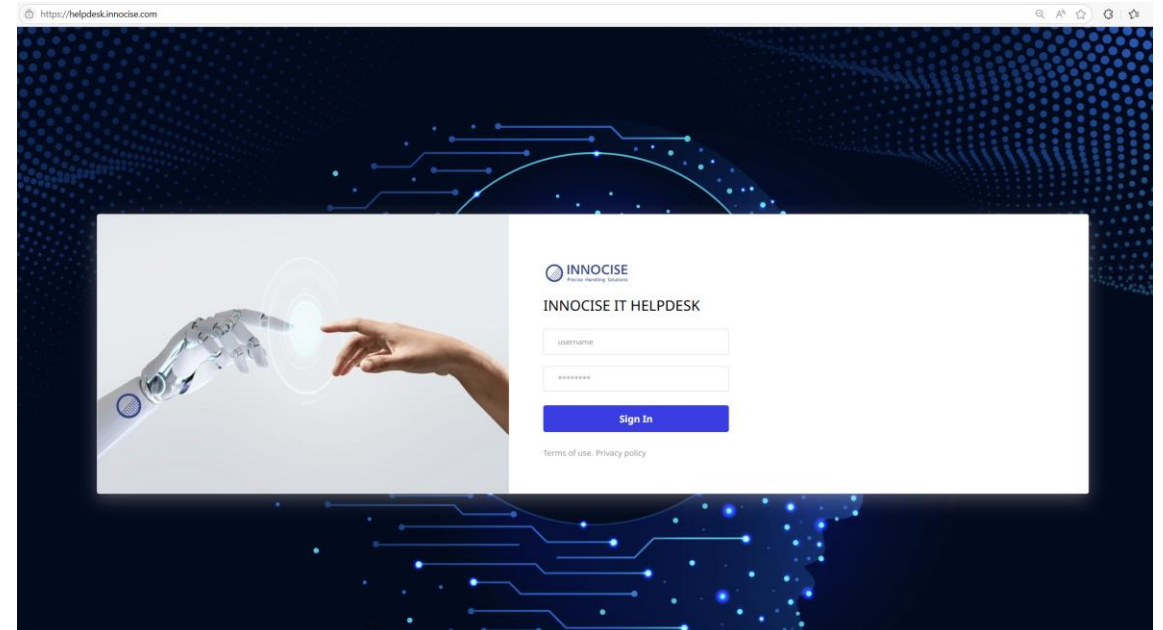


- **Windows key + L:** Locks your computer.
- **Windows key + D:** Shows the desktop by minimizing all open windows.
- **Windows key + S:** Opens the Windows search bar.
- **Windows key + Tab:** Opens Task View, which shows all open apps and virtual
- **Windows key + Left/Right Arrow:** Snaps the current window to the left or right side of the screen.
- **Ctrl+Shift+T:** Reopen the last closed tab browser.
- **F2:** Rename a selected file or folder.
- **Windows + E:** Open New explorer window
- **Windows key + Druck:** Takes a screenshot of the entire screen and saves it to your Pictures/Screenshots folder.

# IT-HelpDesk



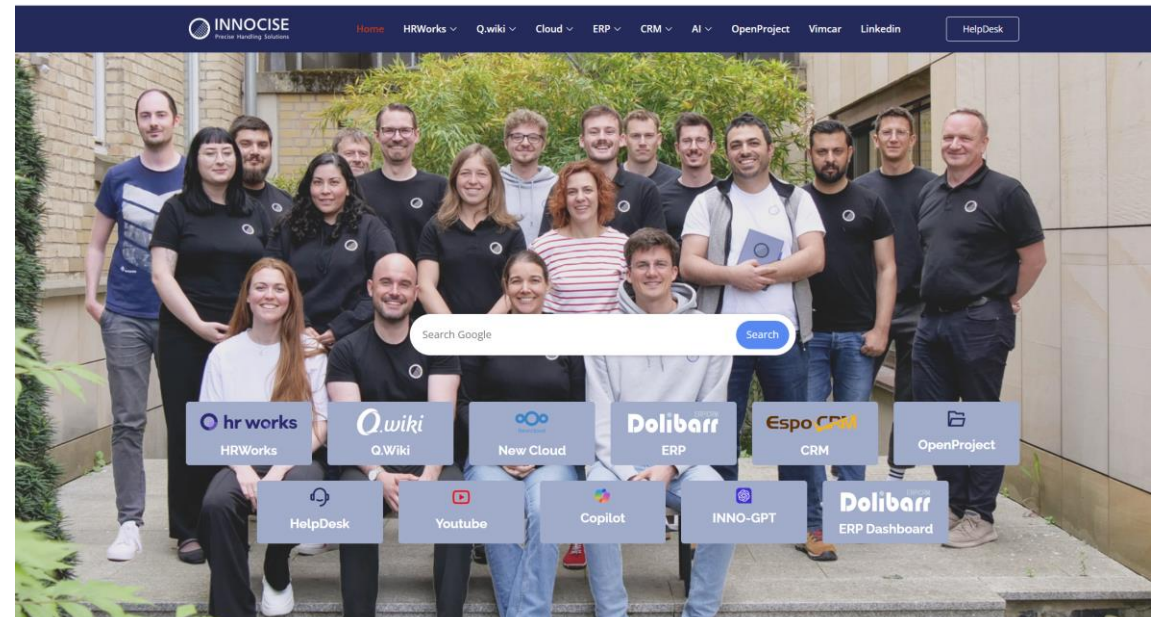
- Login: <https://helpdesk.innocise.com>
  - › Login via username and password
  - › Create new ticket and follow.
  - › We will get back to you as soon as possible.



# Intranet



- Open new tab on the browser
  - › INNOCISE Intranet will load automatically.
  - › You can quickly access the most used links from INNOCISE intranet.



# In case of Problems with IT-Systems



- Relax
- Do not try to fix problems your self
- IT-HelpDesk :
  - › <https://helpdesk.innocise.com/>
  - › +49 681 9659-**2345**
  - › +49 681 9659-**2314**

