

# MECyS Prototyp-Workshop

## Studierende Berufliches Lehramt

PH Freiburg – 23 Jan 2025

# ZIEL - ABLAUF

- Ziel
    - Durchführung: Workshop-Konzept, Tools
  - Ablauf
    - A - Einführung: MECyS-Projekt ...
    - *B - Workshop - Cybersecurity in KKU für – berufliche – Lehrkräfte*
      - *Awareness-Raising*
      - *Inhaltlicher Input*
- Pause – ca. 10.30
- *Test – (KI) Lehr/Lern-Tools*
    - *Unterrichtsszenarien / realistische?*

# A – EINFÜHRUNG

## MECYS – MICRO-ENTREPRISE-CYBER-SECURITY

[HTTPS://MECYS.EU/](https://mecys.eu/)

### Hintergrund und Ziele

Partner

Ziele und Zielgruppen

### Bisherige Ergebnisse

Reports, Workshop, Tools



# MECYS HINTERGRUND UND ZIELE

- MECyS ist eine Art Nachfolgeprojekt von ‚GEIGER‘ (<https://project.cyber-geiger.eu/>)
  - “Easy and affordable cybersecurity solution for small businesses”
- (Neue) Partner mit unterschiedlichen Hintergründen
  - Anemo (Paris), Fachhochschule Nordwestschweiz (Basel), A.B. INSTITUTE OF ENTREPRENEURSHIP DEVELOPMENT (Polis Chrysochous, CY), Association of Thessalian Enterprises and Industries (Larissa, GR), CENTRO SUPERIOR DE FORMACION EUROPA SUR (Malaga)
- Ziel: Verbesserung der Kenntnisse von **Nicht-IT-Personal** angesichts steigender Anforderungen der Digitalisierung
  - Entwicklung und Anpassung von Kursen und Lehr/Lernmaterialien für Cybersicherheit und Datenschutz für IT-Laien in kleineren Unternehmen und Organisationen
- Zielgruppen aus PH-Perspektive (andere Partner mit anderen)
  - Personal in kleineren Unternehmen und Organisationen, Lernende insbesondere im beruflichen Schulwesen, (angehende) Lehrkräfte

# BISHERIGE ERGEBNISSE

- Laufzeit: 1/23 bis 4/25
- Grober Zeitplan
  - Grundlagen in 2023 – Testungen bis Juli 24 – **Umsetzungen bis zum Ende ...**
- Grundlagen
  - Bericht über Lernhürden (qualitative und quantitative Erhebung)
  - Überblick über die berufliche Bildung im Bereich Cybersicherheit und Datenschutz
    - ‚Vergleich‘ der Verortung in den beruflich orientierten Bildungssystemen der Partnerländer
  - Überblick (Interaktive) Lernmittel / Tools aus den Partnerländern
  - Prototypen – Kurspläne
    - Basierend auf gemeinsamem Workshop in Paris
- Pilot-Workshops (verschiedene Zielgruppen)
- Entwicklung weiterer Tools
  - u.a. basierend auf gemeinsamen Workshops in Malaga und Larisa
- (Nationale) Online-Konferenzen
  - Präsentation der bisherigen Projektergebnisse
- **Prototyp für Schulungen von beruflichen Lehrkräften**

# CYBERSAFETY-HYPOTHESEN

- Cybersecurity - Hypothesen
  - „Ich kann Phishing-Strategien erkennen.“ „Ich bin zu klein/unbedeutend, um angegriffen zu werden.“  
Zielkonzept: Phishing-Strategien ändern sich; auch kleine Ziele sind für Angriffe attraktiv
  - „Google wird sich darum kümmern müssen.“  
Zielkonzept: Sensibilisierung für Sicherheitslücken und die Notwendigkeit aktiven Lernens und Handelns
- Datenschutz - Hypothesen
  - „Cookies / Datenschutz ... sind einfach lästig.“  
Zielkonzept: Datenschutz als Grundrecht, Verantwortung auch für die Daten anderer
  - "Ich habe nichts zu verbergen."  
Zielkonzept: Wahrnehmung der Einschränkung der Freiheit durch übermäßigen Austausch und die Speicherung von Daten
  - „Die haben sowieso schon alle meine Daten.“ - „Wo soll ich nur anfangen?“ (Resignation)  
Zielkonzept: Aktive Datenminimierung (auch in kleinem Umfang - Datenaggregation ...)

# BERICHT ÜBER LERNHÜRDEN - ZUSAMMENFASSUNG

Insgesamt gibt es **Ambivalenzen** zwischen risikobewusstem Wissen, eher pragmatischem Verhalten und divergierenden Einstellungen zum Datenschutz.

- Trotz eines meist klaren Verständnisses der Risiken weichen ihre **Handlungen** oft von diesem **Bewusstsein** ab. Es besteht ein möglicher Zusammenhang mit begrenzten Ressourcen, die insbesondere eine klare Trennung von privaten und beruflichen Geräten verhindern.
- (Gute) **Passwörter** werden als sicher angesehen; dennoch wird Mehr-Faktor-Authentifizierung verwendet, möglicherweise aufgrund technologischer Anforderungen.
- In Bezug auf das Vertrauen in die **großen Internet-Unternehmen** gibt es Inkohärenzen:

Ihnen wird bei Cybersicherheit Vertrauen entgegengebracht, nicht beim Datenschutz.

Die Befragten sind z. T. einverstanden, dass ihre Daten online für **Zwecke** verfolgt werden, die Unternehmen (und nicht unbedingt ihnen selbst) dienen, aber sie erwarten auch, dass ihre Daten vor den großen Unternehmen geschützt werden.

- Die Auswirkungen des Datenschutzes werden als positiv empfunden. Negative Auswirkungen betreffen vor allem Unsicherheiten und zusätzliche bürokratische Maßnahmen. Die (vielen) **Einwilligungserklärungen** (Cookies) werden von den Teilnehmern als eher negativ empfunden.

# KURSPLÄNE – GEEIGNETE SETTINGS (?)

- **Die erste Zielgruppe sind Lehramtsstudierende** (insbes. für berufsbildende Schulen), die unterrichten wollen, hauptsächlich in wirtschaftsbezogenen Fächern.  
Das Wissen der Lehramtsstudierenden über Cybersicherheit und Datenschutz kann je nach Zweifach variieren. Dennoch verfügen diese Studierenden an der PHFR in der Regel über ein gutes Allgemeinwissen über betriebliche Fragen, einschließlich Cybersicherheit.  
Kurse an der PHFR finden regelmäßig auf Deutsch statt, dementsprechend auch die MECyS-Workshops. Da in der Regel gute Englischkenntnisse vorhanden sind, können bestimmte Materialien und Hilfsmittel auch in englischer Sprache verwendet werden.
- **Die zweite Zielgruppe besteht aus Berufsschüler:innen** im Rahmen des deutschen – meist dualen – Berufsbildungssystems.  
Es hängt von der Bereitschaft der einzelnen Schulen und Lehrer ab, wo MECyS bei dieser Zielgruppe eingeführt werden kann. Es gibt ein bestehendes Netzwerk von Partnern der PHFR, das genutzt werden kann, um solche Fälle zu verpflichten.  
Diese Schulungen sind in deutscher Sprache. Es ist nicht davon auszugehen, dass diese Gruppe über ausreichende Englischkenntnisse verfügt, um mit englischen Materialien und Werkzeugen geschult zu werden.
- **Die dritte Zielgruppe sind Mitarbeitende von Kleinst- und Kleinunternehmen (KKU).**  
Die in den KKU beschäftigten Personen sind eine recht heterogene Gruppe, was ihr Alter, ihre Vorkenntnisse, ihre allgemeine Erfahrung im IT-Bereich und ihre Motivation angeht. Es ist davon auszugehen, dass diese Zielgruppe trotz wachsendem Risikobewusstsein nur wenig Zeit hat, um sich über Cybersicherheit zu informieren.  
Hier bietet es sich an, zur Nutzung von Selbstlernangeboten (nicht nur von MECyS) anzuregen, um ihr Cybersafety-Wissen zu verbessern.



# B – WORKSHOP: *CYBERSECURITY IN KKU FÜR - BERUFLICHE - LEHRKRÄFTE*

**Ziel:** Befähigung zur Gestaltung einer Bildungsmaßnahme – insbesondere für Lernende im beruflichen Bereich

Spezifische Ziel- und Bedingungsbestimmung

Mögliche Niveaudifferenzierung

Aufbau der Maßnahme

Auswahl geeigneter Mittel etc.

Test von KI-unterstütztem Tool



# GESTALTUNG EINER BILDUNGSMAßNAHME

## ZIEL- UND BEDINGUNGSBESTIMMUNG

- Bezeichnung der Maßnahme, die den Charakter der Bildungsleistung am besten wiedergibt.
  - inkl. Lernziele etc., ggf. Assessment, Kosten ...
- Zeitstruktur einer Bildungsmaßnahme
  - minimale Zeiterfordernis / maximale Teilnahmebereitschaft
  - ein- oder mehrphasig
  - **extra- / curricular**
- Personalressourcen
  - Professionalisierung?
- Sächliche Ressourcen
  - Räume, Technik ... Alter ...
- Teilnehmeranzahl
  - limitierende Faktoren: Größe, Bereitschaft ... der Zielgruppe; räumlich, zeitlich; Methodik, Kosten ...
- Teilnahmevoraussetzungen
  - Vorkenntnisse – formell / informell
- Auswahl konkreter Maßnahmeninhalte
- Auswahl konkreter Methodik, ggf. der eingesetzten Bildungstechnologien

# GESTALTUNG EINER BILDUNGSMAßNAHME

## NIVEAUDIFFERENZIERUNG DER ZIELGRUPPE / ZIELE

Klein/Kleinstunternehmen haben meist keine professionelle/professionalisierte *IT-Abteilung*.

- **Anfänger**
  - Anwendung grundlegender Sicherheitsmaßnahmen, um online sicher zu sein, wie die Verwendung sicherer Passwörter und die regelmäßige Aktualisierung von Software und Antivirenprogrammen.
  - Kenntnis der häufigsten Arten von Cyberangriffen (z.B. Phishing) und von Wegen, wie man sich davor schützt.
- **Mittel**
  - Kenntnis der Grundlagen der Netzwerksicherheit und des Schutzes eines Heim- oder Kleinstnetzwerks.
  - Kenntnis der Risiken, die mit der Nutzung mobiler Geräte verbunden sind, und Nutzung von Maßnahmen, wie man die darauf gespeicherten persönlichen Daten schützt.
  - Kenntnis der besten Praktiken für sicheres Surfen im Internet, einschließlich der Verwendung verschlüsselter Verbindungen und der Überprüfung der Authentizität von Websites.
- **Fortgeschrittene**
  - Kenntnisse von Grundlagen der Computersicherheit und wie man sich vor grundlegenden Bedrohungen, wie z. B. Passwortdiebstahl, schützen kann.
  - Kenntnis der Risiken, die mit dem Online-Informationsaustausch verbunden sind, und Nutzung von Maßnahmen, wie man die Privatsphäre in sozialen Netzwerken und anderen Plattformen schützt.
  - Kenntnisse von Grundlagen der Datensicherheit und wie man wichtige Dateien sichert und sie vor Verlust oder unbefugtem Zugriff schützt.

# AUFBAU EINER MAßNAHME – FÜR LAIEN

- Typischer Dreischritt
  - i. Sensibilisierung - Awareness Raising
    - z.B. eigene Erfahrungen
  - ii. (Spezifischer) Input
    - Grundlagen: Ziele / Hauptgefahren / Verantwortungsstrukturen ...
    - Hilfe zur Selbsthilfe, da extrem dynamisches Feld
  - iii. Umsetzungsaufgabe
    - z.B. ‚Sofortmaßnahme‘
- Typisches Vorgehen: handlungsorientiert
  - mit (simulativer) Handlung in der Maßnahme - für Handlung in der Praxis
  - ggf. ‚spielerisch‘ (Thema hat ‚agonistische‘ Aspekte)

# I. SENSIBILISIERUNG

Erfahrungen

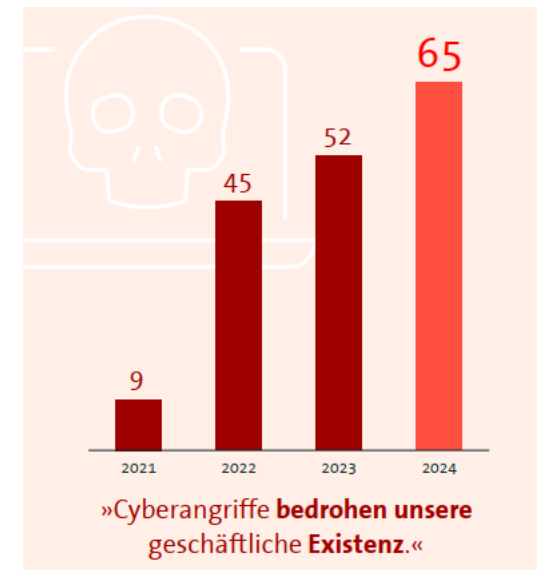
Informationen



# MÖGLICHKEITEN ZUR SENSIBILISIERUNG FÜR CYBERSECURITY-PROBLEME

- Fallbeispiel(e) eines Cybervorfalls (organisational oder persönlich) ggf. eigene Erfahrungen diskutieren
- Spiel zum Thema Cybersecurity
  - z. B. Kahoot
- relevante / aktuelle Probleme diskutieren
  - Awareness Tools
- Dimension der Schäden erläutern

bitkom



# FALLBEISPIEL

- Entweder Bericht über besonderen Fall – z.B. PH Freiburg
- Diskussion mit Teilnehmer:innen über deren Erfahrungen

??

# Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
<b>Gesamtschaden pro Jahr</b>	<b>266,6</b>	<b>205,9</b>	<b>202,7</b>

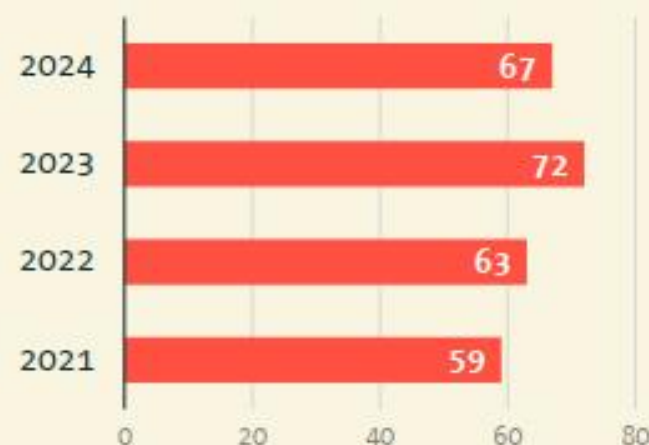


# Cyberattacken verursachen zwei Drittel der Schäden

Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?

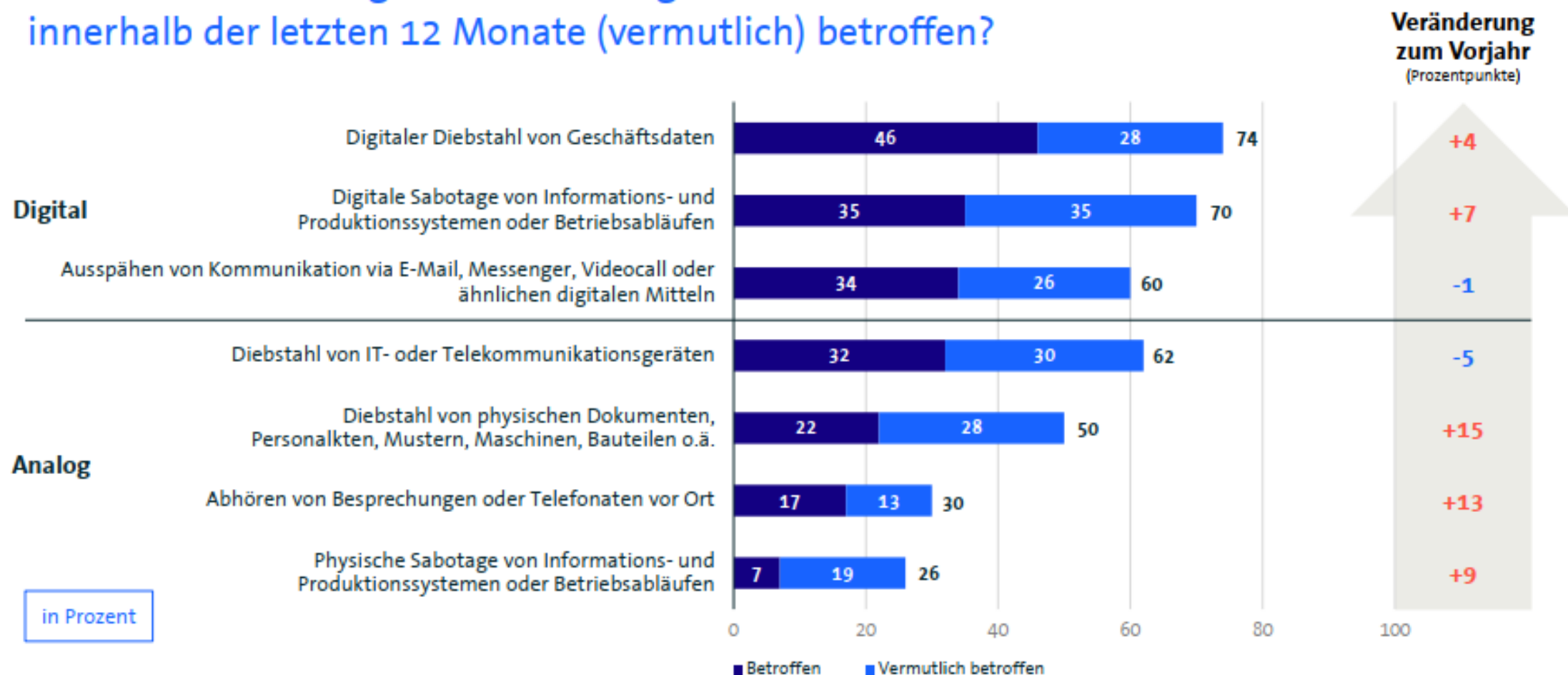


Anteil Cyberattacken an Gesamtschäden 2021-24



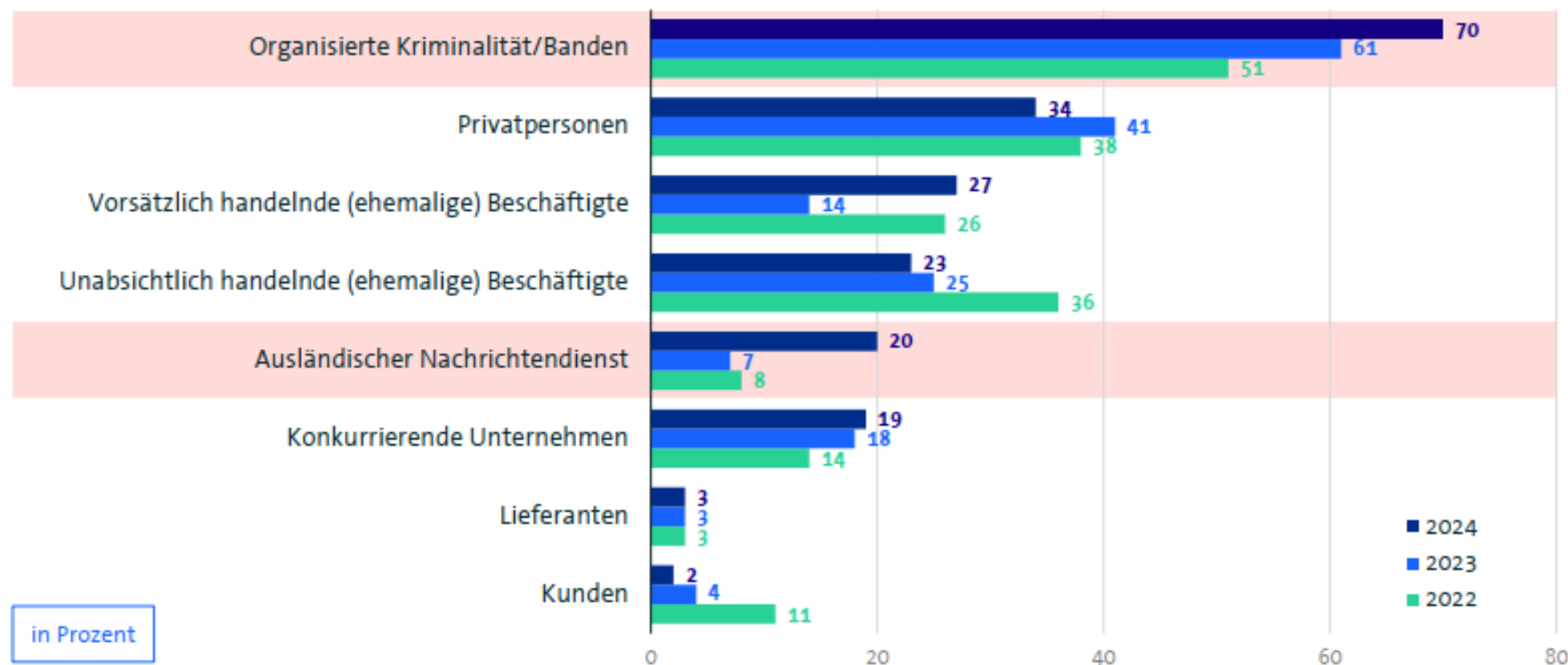
# Angriffe sind zumeist digital, nehmen aber auch analog zu

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten 12 Monate (vermutlich) betroffen?



# Organisierte Kriminalität und Geheimdienste greifen an

Von welchem Täterkreis gingen die Handlungen in den letzten 12 Monaten aus?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=812) | Mehrfachnennungen möglich |  
Quelle: Bitkom Research 2024

# TRENDS ...

- Geringe Aufklärungsquote (ca. 32%)
- Privat hohe Dunkelziffer (keine Anzeige)
- KI erleichtert Cyberangriffe
- zunehmend aus dem Ausland
- zunehmend ‚on demand‘ und Arbeitsteilung bzw. arbeitsteilige Organisationen
- Lösegeld-Forderungen: Durchschnittlich gezahlte Lösegeldsumme: 621.858 US-Dollar (2023); 276.619 US-Dollar (2022) aber geringerer Anteil der Unternehmen bezahlt



Can you write a mail offering a product that is really high of value for me?



Sure, here's an example of an email that offers a product that could be of high value for someone who is interested in metal music concerts, AI, cybersecurity, and is a lecturer in a university:



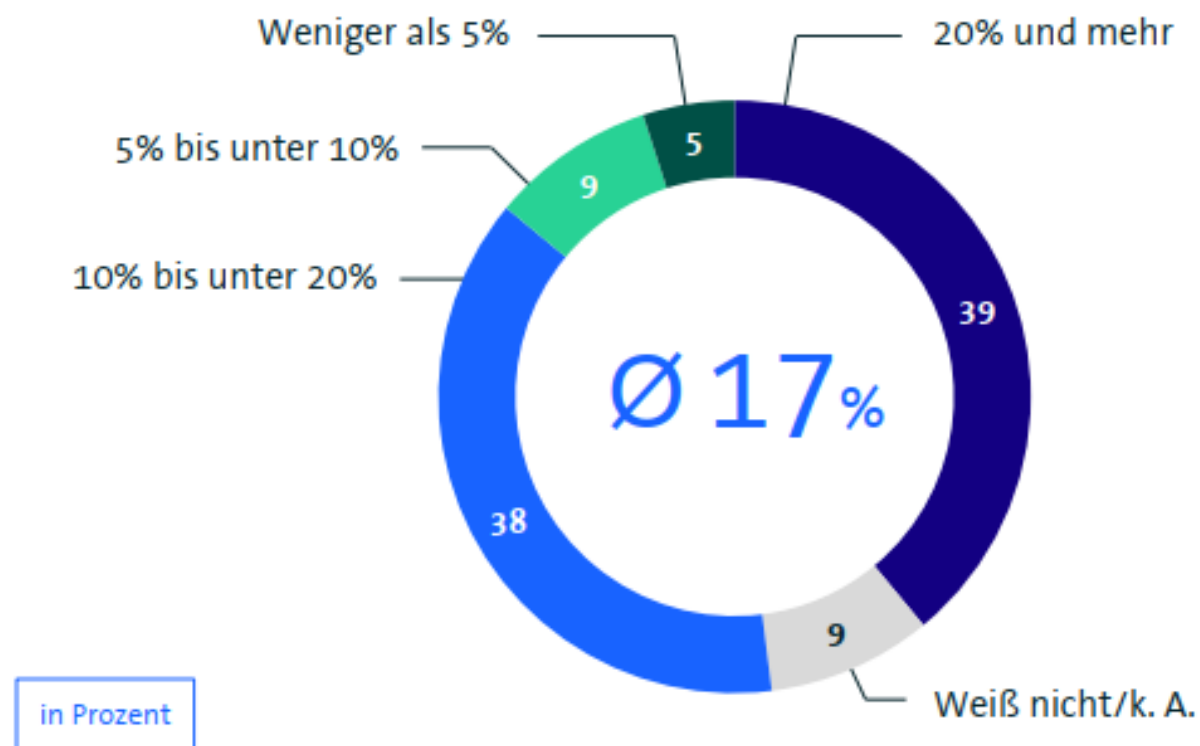
Subject: Exclusive Offer: VIP Tickets to Bad Omens Concert and AI Security Bundle

Dear [Your Name],

We hope this email finds you well. We are writing to offer you an exclusive opportunity to attend the upcoming Bad Omens concert in [City] as a VIP guest. Not only will you get to see your favorite band perform live, but you will also have access to VIP-only areas and perks.

# Cybersicherheit: Investitionsbereitschaft steigt

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?



Durchschnittlicher Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget



# SPEZIFISCHER INPUT - GEFAHRENLAGE: PERSONEN IN KKV BZW. KLEINEN ORGANISATIONEN

- existenz-gefährdende Angriffe richten sich zunehmend auf (vermeintlich) kleine Ziele
  - 43% der Cyberattacken haben kleine Unternehmen als Ziel: fehlendes Bewusstsein, leichter zu erpressen, Ausgangspunkt für größere Ziele  
<https://www.osibeyond.com/blog/3-reasons-why-hackers-target-small-businesses/>
  - je kleiner desto schlechter vorbereitet (Notfallplan)  
<https://www.heise.de/news/Umfrage-zu-Cyberattacken-Viele-Unternehmen-haben-keinen-Notfallplan-7268938.html>
- Besonders problematisch: mögliche Spill-over Effekte bei ‚Kleinen‘ vom Beruflich-Wirtschaftlichen in die private Sphäre
  - Familienangehörige als Mitarbeitende etc.
  - Anfallende finanzielle, zeitliche und psychische Kosten verschwinden nicht in einer anonymen Organisation oder Bilanz



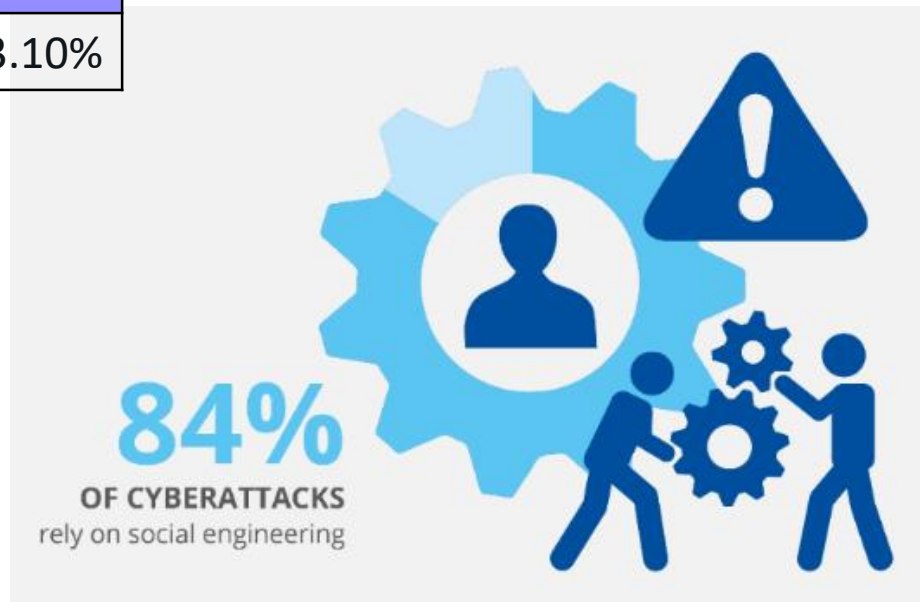
# SPEZIFISCHER INPUT - GEFAHRENLAGE: PERSONEN IN KKV BZW. KLEINEN ORGANISATIONEN

Angestellte	Unternehmen	IT-Abhängige	IT-Basierte	IT-Dienstleister
1-9	89.67%	51.10%	35.80%	2.77%
10-49	8.49%	4.68%	3.51%	0.28%
50-249	1.46%	0.87%	0.59%	0.05%
Total	99.72%	56.65%	39.29%	3.10%

Cyber-Attacken profitieren häufig von menschlichem Verhalten als 'weakest link' und auch das findet sich vorrangig bei den ,Kleinen'

Fricker/Shofar – nach Schweizer Daten von 2018

<https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Incidents%20A4.pdf>



# AWARENESS RAISING TOOLS

## GGF. AUCH FÜR INPUT-PHASE

- ENISA – EU Agency for Cybersecurity
  - z.B. Cybersecurity Awareness Raising: The ENISA -Do-It-Yourself Toolbox - auf Englisch
  - <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box>
  - Leitfäden für Kommunikationsstrategien, Spielesammlung ...
- ein paar Links zu deutschen Spielen etc.:
  - <https://www.bakgame.de/Spiele/>
  - <https://www.cybersecurity-awareness.at/massnahmen/die-macht-der-mini-spiele>
  - <https://www.ihk.de/bodensee-oberschwaben/innovation/e-commerce-und-e-business/it-sicherheit-in-unternehmen/quiz-zur-it-sicherheit-form-4615152>
  - Sehr viele kommerzielle Gamification-Angebote ...
- ggf. wirkungsvoll:
  - Cybersecurity Quiz – Internxt: <https://internxt.com/cyber-security-quiz>
  - Have I Been Pwned - Identity Leak Checker: <https://sec.hpi.de/ilc/>
  - Phishing Test, inkl. Spamfilter: <https://phish-test.de/>
  - Betrieblichen Sicherheitsbedarf bestimmen: <https://sec-o-mat.de/>

### ANSWER SHEET

What is the name of the first known victim of the PHISHING ATTACK?  
Surname Name as seen in the Badge with space\*

Which Badge ID was used to performed unauthorized access?

ENCRIPTION KEY

What is the filename of the decrypted file?





# WEITERE TOOLS AUS MECYS UND PARTNERPROJEKTEN

- Kahoot als Awareness Raising: Cybersecurity

<https://create.kahoot.it/share/cybersecurity/88736641-bc4f-4318-a47e-764035dffd36>



- Kahoot zum Thema Phishing: Lerntool Mysec

<https://create.kahoot.it/share/lerntool-mysec/f30b5e6c-2e08-4952-99b8-d4fa30d267e8>



- Diverse Arbeitsblätter zum Thema ‚Phishing‘

## II. INPUT FÜR SCHÜLER:INNEN

Wichtige Quellen ...

für Schüler:innen ggf. handlungsorientiert: Recherchen o.ä.



# INPUT – Z.B ENISA - THREAT LANDSCAPE ERSCHEINT JÄHRLICH



- Analyse der jeweiligen ‘**Prime Threats**’  
Impact, Motivation, Angriffstechniken, Erfassungsverfahren für relevante Trends, **gezielte Abhilfemaßnahmen**

## Aktuelle Rangliste:

- Threats against availability: DOS/DDOS/RDOS
- Ransomware
- Threats against data
- Social engineering threats
- Malware
- Supply chain attacks
- Web threats
- Foreign Information Manipulation and Interference (FIMI)
- Zero day

<https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024.pdf>

- **Threats against availability (DDoS) and Ransomware ranked at the top during the reporting period for another year.**
- **Living Off Trusted Sites (LOTS):** Threat actors extended their stealth techniques into the cloud, using trusted sites and legitimate services to avoid detection and disguising Command and Control communications (C2) as ordinary traffic or innocuous messages on platforms like Slack and Telegram.
- **Geopolitics continued to be a strong driver for cyber malicious operations.**
- **Advancements in defensive evasion techniques:** Cybercrime groups, especially ransomware operators, evaded detection by using Living Off The Land (LOTL) techniques, to blend into environments and mask their malicious activities.
- There has seen a **sharp increase<sup>13 14</sup> in Business Email Compromise (BEC) incidents<sup>15</sup>**
- **Extortion by weaponizing disclosure requirements**, pushing companies to fulfil extortion demands ahead of the required reporting deadline.
- **Ransomware attacks appear to have stabilized in quite high numbers in regards to the previous reporting period**
- **Ever more impactful law enforcement operations**, such as Operation Chronos and Operation Endgame.
- **AI tools for cyber criminals:** Threat actors used tools such as FraudGPT and large language models to co-author scam emails and generate malicious PowerShell scripts.
- **19,754 vulnerabilities** were identified with 9.3% fell into the ‘critical’ category and 21.8% were categorised as ‘high’.

# INPUT - Z.B. BKA – BUNDESLAGEBILD ERSCHEINT JÄHRLICH

- 1. Cybercrime
  - 1.1 Bedrohungslage
  - 1.2 Branchen im Fokus
  - 1.3 Herausragende Sachverhalte
- 2. Polizeiliche Kriminalstatistik
- 3. Relevante Phänomenbereiche
  - 3.1 Eintrittsvektoren
  - 3.2 Malware
  - 3.3 Ransomware & Data Extortion
  - 3.4 Distributed Denial-of-Service
- 4. Quo vadis, Cybercrime?

**Aktuelle Trends  
aber  
keine Abhilfemaßnahmen**



Polizeiliche Maßnahmen schwächen zunehmend die globale Infrastruktur der Cybertäter.



Die Aufklärungsquote ist bei den Cybercrime Delikten mit 32% leicht angestiegen.



Den leicht rückläufigen Cyberstraftaten in der Inlands PKS steht ein stärkerer Anstieg der Auslandstaten\* gegenüber



Über 800 Unternehmen und Institutionen haben Ransomware-Angriffe zur Anzeige gebracht.



Die weltweiten Ransomware-Zahlungen steigen auf über 1 Mrd. US-Dollar.



DDoS Angriffe sind das "Mittel der Wahl" hacktivistischer Gruppierungen



Einzelne Software-Schwachstellen wurden für massive Angriffskampagnen ausgenutzt.



Die vom Bitkom e.V. bezifferten Schäden in Deutschland belaufen sich auf 205,9 Mrd. Euro - 72% davon entstanden direkt durch Cyberangriffe.

# WEITERE AUSWAHLMÖGLICHKEITEN INPUT

## Was ist für wen relevant?

- bitkom – ‚Wirtschaftsschutz‘
  - heise – Abwehrmaßnahmen
  - Verbraucherzentrale NRW
  - Verband der Internetwirtschaft
  - BSI – Allianz für Cybersicherheit
  - Verfassungsschutz – Cyberabwehr
  - ...
  - Kammern ...
- 
- Wenn man ‚cybersicherheit / quiz‘ oder ‚cybersicherheit / maßnahmen‘ ... googelt, erhält man eine Vielzahl an Treffern ...



# VOM INPUT ZUR AKTION

## INSBESONDERE HILFE ZUR SELBSTHILFE

- aus betrieblicher Sicht zwei Ebenen:
- Organisationale Ebene, z.B.
  - Verantwortlichkeiten klären, u.a. CS zur Chefsache machen
  - Prozesse effektiv/effizient gestalten (Updates, Notfälle ...)
- Detail/individuelle Handlungsebene
  - Sensibilisieren, Motivieren
  - Handlungsanweisungen vermitteln (Umgang mit Psw, VPN, ...)

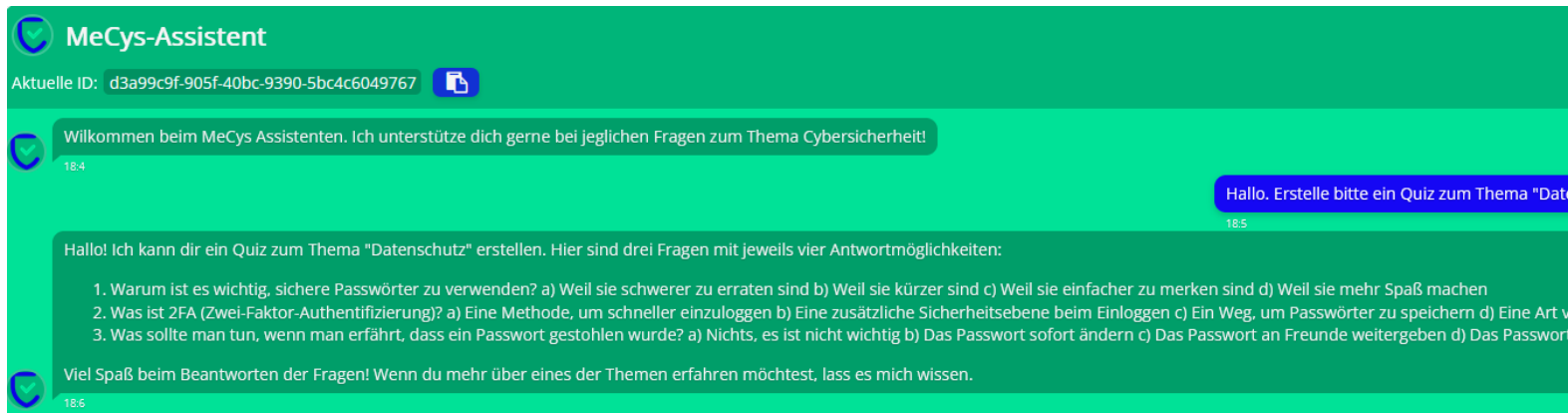
# INPUT – PHISHING (SMISHING, QUISHING ...)

- eigene Erfahrungen zum Thema Phishing
- ggf. Kahoot (je nach Einstieg)
- Arbeitsblätter zum Thema Phishing:
  - Merkmale
  - Formen
  - Gefahren
  - Reflexion: Präventionsmaßnahmen



# INPUT – VERMITTLUNGSMÖGLICHKEIT

- Weiter- bzw. Neuentwicklung (KI) eines Tools aus GEIGER
- <https://cybersecurityassistant.rhieszeros.ch/mecys/>
- u. a. Erstellen von Quizen





# III. UMSETZUNGSAUFGABE

Curriculares Priorisieren



# GESTALTUNGSAUFGABE

- Wenn Sie (nur) eine Doppelstunde Zeit hätten,  
um **Ihre** SuS beim Thema Cybersecurity voranzubringen,  
wie sähe diese Einheit aus?

# GESTALTUNGSAUFGABE – FRAGEN ZUR VORBEREITUNG DER BILDUNGSMAßNAHME

- Wie müsste ein Workshop oder eine Sequenz aussehen, um insbes. Berufsschullehrkräfte in die Lage zu versetzen, die (absoluten) Grundlagen zu vermitteln?
  - Wer braucht das überhaupt noch?
- Wie könnte eine geeignete Maßnahme für Berufs-SuS dann aussehen?
  - Braucht es unterschiedliche, je nach Beruf?
  - Aktualisierungsrhythmus?
- Welche (Online)Angebote wären hierfür jeweils wichtig?
- Welches Potential hat ein KI-Tool, wie das vorgestellte?
  - Wohin sollte die Reise gehen?

• **Vielen Dank**

[mecys.eu](https://mecys.eu)



Co-funded by  
the European Union

# MECyS Prototype – Vocational Teacher Trainees

University of Education Freiburg – 23 January 2025

**Project name:** Micro-Enterprise-Cyber-Security

**Project Number:** 2022-I-DEO2- KA2 20-V ET- 000087 22

## List of participants

	Name	Role	Signature
1.	Alber, Jens	Workshop Instructor	Jens Alber
2.	Remmele, Bernd	Workshop Instructor	B. Remmele
3.	Krzymowski, Deborah	Project Staff	D. Krzymowska
4.	Hampel, Dominik	Teacher Trainee	D. Hampel
5.	Knaack, Keno	Teacher Trainee	K. Knaack
6.	Ams, Frank	Teacher Trainee	F. Ams
7.	Katzer Julian	Teacher Trainee	Julian Katzer
8.	Tessa Rosenfeld	Teacher Trainee	T. Rosenfeld

**MECyS** | Micro-Entreprise Cybersecurity

## MECyS Workshop Berufliches Schulzentrum Waldkirch

PH Freiburg – 27.03.2025

 Pädagogische Hochschule Freiburg  
Université des Sciences de l'Éducation - University of Education

 Co-funded by the European Union

1

## ERASMUSMUS – PROJEKT MECYS – MICRO-ENTREPRISE CYBERSECURITY

- erasmus+ = Bildungsprogramm der Europäischen Union
  - Austauschprogramme insbesondere für Studierende aber auch für Schüler:innen ...
  - Kooperationsprojekte zwischen europäischen Bildungsorganisationen
- MECyS = Kooperationsprojekt mit Partnern aus Frankreich, Griechenland, Schweiz, Spanien, Zypern
- Micro-Entreprise = Betrieb/Organisation mit weniger als 10 Personen, die dort ‚arbeiten‘ darunter meist keine IT-Spezialisten → besonders gefährdet → MECyS
- Workshops zu ‚Cybersecurity – Awareness‘ in der (jungen) Bevölkerung



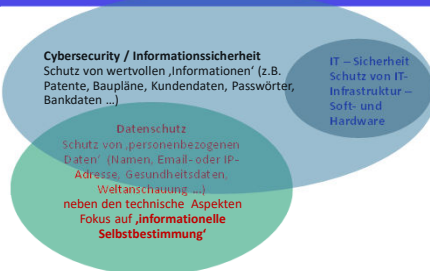
2

## ÜBERSICHT

1. Quiz und Diskussion über Eure Erfahrungen zu Cybersecurity etc.
2. Ein paar Hintergrundinformationen zu Cybercrime
3. Aufgabe/Diskussion zu Phishing
4. Test unseres KI-Assistenten
5. Ein paar Hintergrundinformationen zu Datenschutz
6. Reflexion

3

## CYBERSECURITY – IT-SICHERHEIT - DATENSCHUTZ



**Cybersecurity / Informationssicherheit**  
Schutz von wertvollen ‚Informationen‘ (z.B. Patente, Baupläne, Kundendaten, Passwörter, Bankdaten ...)

**IT – Sicherheit**  
Schutz von IT-Infrastruktur – Soft- und Hardware

**Datenschutz**  
Schutz von ‚personenbezogenen Daten‘ (Namen, Email- oder IP-Adresse, Gesundheitsdaten, Weltanschauung ...)  
neben den technischen Aspekten  
Fokus auf ‚informationelle Selbstbestimmung‘

4

## QUIZ: KAHOOT „HACK ATTACK“

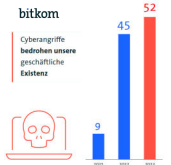
<https://create.kahoot.it/share/hack-attack/695312ae-1826-41ab-a651-0189f86a4f30>




5

## FRAGE

- Gab es in eurem Umfeld Cyberangriffe oder habt ihr von welchen erfahren?



bitkom

Cyberangriffe bedrohen unsere geschäftliche Existenz

Jahr	Prozent
2021	9
2022	45
2023	52

6



## CYBERANGRIFFE – TYPISCHE MOTIVE

- Geld (Bankkonto-Daten, Lösegeld, Shopping, ...)
- Zugang zu IT-Systemen (weitere Ziele je nach System)
- politische Ziele (z. B. Schwächung kritischer Infrastruktur)
- Spionage (z. B. Datendiebstahl)
- Sabotage (z. B. Betriebsstörungen)
- Rechenleistung (z.B. Crypto-Mining)
- 'Persönliches' (z.B. Stalking – auch physisch)



7

## FAKTEN ZUR CYBERKRIMINALITÄT IN DE

### Cybercrime-Bilanz: 7 von 10 Internetnutzern betroffen 2023

Welche der folgenden Erfahrungen mit kriminellen Vorfällen haben Sie persönlich in den vergangenen 12 Monaten im Internet gemacht?



Quelle: <https://www.bitkom.org/Presse/Pressemitteilung/Bilanz-Cyberkriminalitaet-2-von-10-Internetnutzern-2023>

Basis: 1.018 Internetnutzern und Nutzer ab 16 Jahren in Deutschland (Befragungszeitraum: 1. bis 31. März 2024) | Quelle: Bitkom Research 2024

bitkom

8

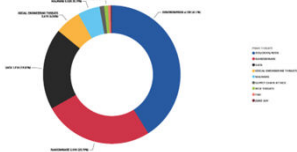
## CYBERANGRIFFE – HÄUFIGE ARTEN

- Ransomware
  - Verschlüsselung von Daten - Lösegeldforderung
- Phishing (Varianten: Vishing, Smishing)
  - Diebstahl sensibler Informationen mithilfe von betrügerischen E-Mails oder Websites, Voicemails, SMS ...
- Malware
  - Infektion von Systemen mithilfe von Viren, Würmern oder Trojanern
- DDOS-Attacks
  - Distributed-Denial-of-Service – Überlastung von IT-Systemen durch viele Anfragen

9

## ENISA THREAT LANDSCAPE 2024

Figure 2: Breakdown of analysed incidents by threat type (July 2023 till June 2024)

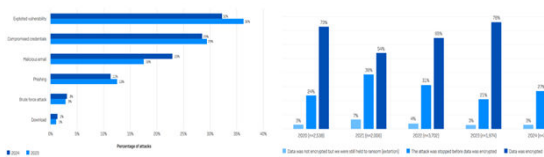


[https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024\\_0.pdf](https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf)

10

## RANSOMWARE – GRÜNDE DER ANGRiffe UND VERSCHLÜSSELUNGSRATE

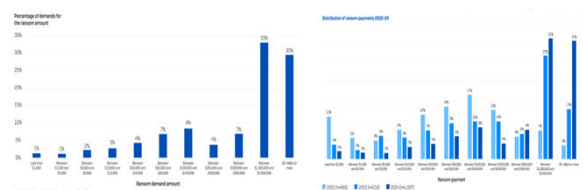
### Sophos Ransomware-Bericht 2024:



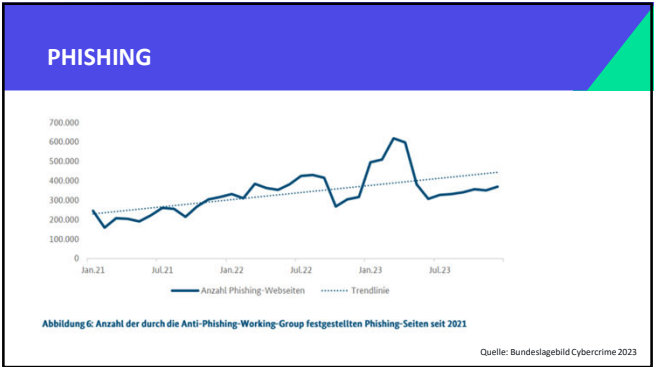
<https://assets.sophos.com/X2AW1U0J4t/mcww5bHd0q48B24nqmbfaw/sophos-state-of-ransomware-2024-update.pdf>

11

## RANSOMWARE – GEFORDERTE UND BEZAHLTE SUMMEN



12



13

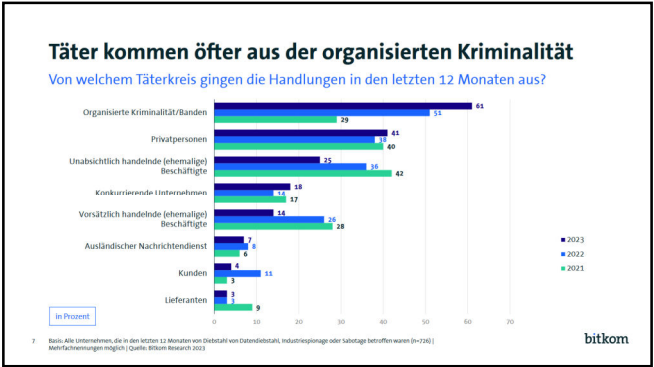
**Schaden pendelt sich über 200 Milliarden Euro ein**

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	35,3	23,6	12,3
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	35,0	41,5	61,9
Kosten für Rechtstreitigkeiten	29,8	16,2	12,4
Kosten für Ermittlungen und Ersatzmaßnahmen	25,2	10,1	13,3
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	21,5	41,5	29,0
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	16,1	10,7	24,3
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	15,3	21,1	22,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	12,4	18,3	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	10,4	18,8	30,5
Geldabfluss durch Betrugsversuche	3,9	-	-
Sonstige Schäden	1,1	0,9	0
<b>Gesamtschaden pro Jahr</b>	<b>205,9</b>	<b>202,7</b>	<b>223,5</b>

[https://www.bitkom.org/sites/main/files/2023-09/Bitkom\\_Charts-Wirtschaftsschutz-Cybercrime.pdf](https://www.bitkom.org/sites/main/files/2023-09/Bitkom_Charts-Wirtschaftsschutz-Cybercrime.pdf)

14



15

**PHISHING MIT UND OHNE KI**

- **Phishing ohne KI:**
- Phishing-Mails früher leichter identifizierbar:
  - fehlende oder fehlerhafte Anrede
  - Rechtschreib- und Grammatikfehler
  - dringliche Nachricht

16

**PHISHING MIT UND OHNE KI**

- **Phishing mit KI viel schwerer zu identifizieren:**
  - viel weniger bis keine Grammatik- und Rechtschreibfehler
  - überzeugend professioneller Schreibstil
  - Imitation der Stimme eines vertrauenswürdigen Kontakts
    - gefälschte Audiodateien wie z. B. Sprachnachrichten
  - viel schnellere und effektivere Informationsbeschaffung (durch Zugriff auf große Teile des Internets)
    - schnellere Erstellung und Verbreitung von kompromittierten Geschäfts-E-Mails und anderen Phishing-Kampagnen

17



18



## UNTERNEHMEN OHNE IT-ABTEILUNG BESONDERS GEFÄHRDET

- **Gefahren:**
  - kein oder unzulängliches IT-Sicherheitskonzept
  - oft keine klare Trennung der Zuständigkeiten
  - Nutzung privater Geräte für berufliche Zwecke und andersherum
- **Lösungsansatz:**
  - kostenlos zugängliche Materialien, z. B. von der ENISA

19

## CYBERSECURITY MATURITY ASSESSMENT (ENISA)



20

## ARBEITSBLÄTTER ZUM THEMA PHISHING

Aufgabe:

Bearbeitet die Arbeitsblätter in Partnerarbeit und diskutiert die Fragen.  
(ca. 10 Min. Bearbeitungszeit)

21

### Arbeitsblatt 1: Phishing-Mails analysieren - Musterlösung

#### Eine E-Mail-Nachricht

Hallo,  
dein Paket wurde zurückgehalten, da die Lieferadresse unvollständig ist. Bitte bestätige deine Adresse hier: [www.dhl-paket-info.de](http://www.dhl-paket-info.de)

Dein Paketdienst-Team

#### Fragen:

1. Welche Informationen fehlen in der E-Mail, die sie glaubwürdiger machen würden?

Persönliche Anrede und Grußformel, Name eines Mitarbeitenden des Paketdienstes (z. B. in der E-Mail-Signatur)

22

2. Welche Schritte könntet ihr unternehmen, um herauszufinden, ob die Nachricht echt ist?

URL des Links prüfen (durch Drüberfahren mit dem Cursor), beim Paketdienst anrufen und nachfragen, Mail an Service-Hotline des Paketdienstes schreiben

3. Welche Gefahr besteht, wenn ihr persönliche Daten oder Zahlungsinformationen auf der verlinkten Seite eingibt?

Missbrauch der gestohlenen Daten, z. B. Schreiben von Mails in eurem Namen, Käufe und Abbuchungen in eurem Namen, Veröffentlichung und Verkauf der Daten im Darknet

23

### Aufgabe 2: Phishing-Analyse und Prävention

4. Welche drei Merkmale würdet ihr bei jeder E-Mail prüfen, um sicherzugehen, dass sie echt ist?

Absenderadresse, URL (falls die Mail Links enthält), Aufforderung zu schneller Handlung, Grammatik- und Rechtschreibfehler

5. Was sind typische Tricks, die Phishing-Betrüger anwenden, um ihre Nachrichten vertrauenswürdig erscheinen zu lassen?

Verwendung von Firmenlogos, Schreiben von Mails im Namen von Vorgesetzten

6. Warum ist es wichtig, verdächtige E-Mails oder Nachrichten direkt zu melden?

Damit möglichst wenige (im Idealfall keine) weiteren Personen Opfer des Angriffs werden.

24

## Arbeitsblatt 2: Eigene Schutzstrategien entwickeln

### Aufgabe 1: Reflexion über Sicherheitsmaßnahmen

1. Welche Sicherheitsmaßnahmen gegen Phishing nutzt du bereits?

individuelle Lösungen, z. B. Verwendung sicherer Passwörter, Multi-Faktor-Authentifizierung, Passwort-Manager

2. Welche weiteren Sicherheitsmaßnahmen kennst du?

individuelle Lösungen, z. B. Homeoffice und Nutzen von Netzwerken nur über VPN

25

3. Warum ist es wichtig, E-Mails kritisch zu hinterfragen, selbst wenn sie auf den ersten Blick vertrauenswürdig aussehen?

Phishing-Mails werden immer „besser“ und sind immer schwieriger als solche zu identifizieren, potenziell hohe (finanzielle und psychische) Schäden

4. Wie können sichere Passwörter dazu beitragen, Schäden durch Phishing zu begrenzen?

Sie sind schwer zu knacken und erschweren den Hackern so den Zugriff auf Konten

5. Welche Maßnahmen wenden viele Unternehmen an, um sich vor Phishing-Angriffen zu schützen?

Zugang im Homeoffice über VPN, MFA, strenge Einstellungen der Firewalls

26

## TEST UNSERES KI-BASIERTEN CYBERSECURITY-ASSISTENTEN

1. Fragen überlegen
2. Auf „Neue Konversation Starten“ klicken
3. Frage – in beliebiger Sprache – eingeben  
... ein bisschen Geduld ...
4. Antwort lesen, mit Partner diskutieren und ggf. Nachfrage oder neue Frage stellen



<https://cybersecurityassistant.rhymeseros.ch/mecys/>

27

## AUFGABE MIT DEM KI-BASIERTEN CYBERSECURITY-ASSISTENTEN

- 1) Kommuniziert mit dem Cybersecurity-Chatbot. Ihr könnt beispielsweise folgende Fragen stellen:
  - Wie kann ich meinen Instagram-Account schützen?
  - Was ist beim Schutz personenbezogener Daten bei kleinen Unternehmen anders als bei Großen?
- 2) Erstellt ein Quiz (für deine/n Nebensitzer/in zum Thema "xy" mit 3 Fragen und jeweils 4 Antwortmöglichkeiten. Eine Antwort davon soll richtig sein.

28

## DATENSCHUTZ - IM ALLTAG

- Was sind personenbezogene Daten?
- Wo teilt ihr solche Daten? Wo entstehen sie?  
Bewusst oder unbewusst?
- Wo und zu welchem Zweck werden eure Daten (von Unternehmen) gespeichert?



29

## WIE ENTSTEHEN PERSONENBEZOGENE DATEN?

- Zugriff auf Websites und Accounts (Psw etc.)
- Cookies (Computererkennung, Systemeigenschaften)
  - häufig aber nur wenn man einwilligt
- Gesundheitssektor (besonderer Schutz)
- Logins z.B. in Fitnessstudios
- Zahlungsdaten
- Videoüberwachung
- Google (Maps ...)
- ...



**Stammdaten / Vertragsdaten / Kontaktdaten**  
(öffentlich & privat)  
Name, Titel, Alter, Geburtsdatum, Foto, Familienstand, Hobby, Adresse, Telefonnummer, Mail-Adresse



**Digitaler Daten / Finanzdaten**  
Geräte-Identifikationsdaten, IP-Adresse, Meta-Daten, Verbindungsdaten, Log-In-Daten, Inaktivitätsdaten (Click)



**Authentifizierungsdaten**  
Passwörter, Identifikationsnummern (Steuernummer, Sozialversicherungsnummer), Ausweisnummer (Personalausweis)



**Bezugsdaten**  
Fahrzeug, Immobilien, Grundbuchbeitrag



**Ort und Zeit**  
Geolokation (GPS, Smartphone), Zeitstempel (Datenverbreitung), Terministen



**Bank-, Finanzdaten, Abrechnungsdaten**  
Gehaltsdaten, Bankdaten, Kontostausätze, Schulden, Invoizen



**Physische Daten**  
Statur, Geschlecht, Augenfarbe, Größe, Gewicht



**Werkzeuge**  
Bewertungen, Zeugnisse, Berichte, Zertifikate

30

## REFLEXION – WAS NEHME ICH MIT?

- Was war das Eindrücklichste heute?
- Wie sinnvoll erscheint euch so ein spezialisierter Chatbot?
- Worüber hättet ihr gerne etwas/mehr erfahren?
- Was könnt Ihr noch vor dem Wochenende tun, um eure Daten-Sicherheit zu erhöhen?

31

**MECys** Micro  
Enterprise  
Cybersecurity

• Vielen Dank

mecys.eu



Co-funded by  
the European Union

32

## FEEDBACK



33

## LINKS ZU INTERESSANTEN SEITEN UND MATERIALIEN ZU DEN THEMEN CYBERSICHERHEIT UND DATENSCHUTZ

- Bitkom: Bilanz Cyberkriminalität 2023:  
<https://www.bitkom.org/Presse/Presseinformation/Bilanz-Cyberkriminalitaet-7-von-10-betroffen#item-19028>
- Bitkom: Wirtschaftsschutz 2023:  
<https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf>
- Bundesamt für Sicherheit in der Informationstechnik (BSI):  
[https://www.bsi.bund.de/DE/Home/home\\_node.html](https://www.bsi.bund.de/DE/Home/home_node.html)
- Bundeslagebild Cybercrime 2023:  
<https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=229942>
- Stiftung Datenschutz:  
<https://stiftungdatenschutz.org/startseite>

34

## **mögliche Maßnahmen zum Schutz vor Cyberangriffen**

### **Multi-Faktor-Authentifizierung (MFA):**

- Bei der Anmeldung wird neben dem Benutzernamen und dem Passwort eine zweite Authentifizierungsmethode verwendet.
- Bsp.: Code, der per SMS geschickt wird; TAN (Online-Banking); Passwort über gesonderte App, etc.

### **sichere Passwörter:**

- lange Passwörter, die neben Klein- und Großbuchstaben auch Zahlen und Sonderzeichen enthalten (zufällige Kombination dieser Elemente)
- keine ganzen Wörter im Passwort
- Möglichkeit: Bezug zu persönlichen Ereignissen

### **Passwort-Manager:**

- erzeugt für jeden Account ein einzigartiges und extrem sicheres Passwort → Wenn ein Passwort gehackt wird, sind die anderen Accounts trotzdem noch sicher!
- speichert die Passwörter an einem Ort
- Master-Passwort wird benötigt, um den Passwort-Manager zu öffnen → Passwörter sind dort sicher, solange das Master-Passwort nicht geknackt wird
- Man muss sich nur wenige Passwörter merken.
- Einfache Synchronisierung auf verschiedenen Geräten möglich → Man hat die Passwörter immer dabei.
- Tipp: Passwort-Manager in Verbindung mit einer Multi-Faktor-Authentifizierung verwenden
- Beispiele: KeyPass, Dashline, bitwarden, etc.

### **Antiviren-Programm:**

- überprüft (neue) Dateien und das gesamte Gerät auf Anzeichen einer möglichen Infektion
- regelmäßige Updates wichtig, um auch vor neueren Viren geschützt zu sein
- auf jedem Gerät nutzen und nicht nur auf dem PC

### **regelmäßige Datensicherung:**

- Dateien (selbst erstellte Dokumente, Bilder, Texte, Tabellen, etc.) in regelmäßigen Abständen sichern, damit sie nicht verloren gehen, falls sie durch einen Angriff beschädigt oder verschlüsselt werden
- Speichern auf externer Festplatte (oder in Cloud)
- Speichermedium (z. B. externe Festplatte) nicht an das Netzwerk anschließen

## Phishing-Mails erkennen

### Was ist Phishing?

Was ist **Phishing**? Das Wort „Phishing“ setzt sich aus „**password**“ und „**fishing**“ zusammen. Es ist eine der häufigsten sowie wirkungsvollsten Methoden, die Cyberkriminelle anwenden, um **vertrauliche Informationen** zu entwenden.

Die Technik nutzt menschliche Psychologie, unvorsichtiges Verhalten und Vertrauen aus, um Sie **über gefälschte E-Mails, Nachrichten oder Websites zur Preisgabe von Passwörtern, Finanzinformationen und/oder anderen sensiblen Daten** zu bewegen.

### Merkmale von Phishing-E-Mails:

Phishing-E-Mails können häufig an den folgenden Merkmalen erkannt werden:

- **UNBEKANNTER ABSENDER:** Phishing-E-Mails werden oft von einer **nicht vertrauenswürdigen oder unbekannten Adresse** gesendet. Man soll daher die **E-Mail-Adresse und den Absender überprüfen, bevor man Links oder Anhänge anklickt** – z.B. indem man mit der Maus über die Absenderinformation fährt.  
Manchmal verwenden Betrüger E-Mail-Adressen, die ähnlich aussehen wie legitime E-Mail-Adressen. Man muss daher genau auf **Abweichungen zwischen dem angeblichen Absender und der neben dem Absender stehenden E-Mail-Adresse achten!** In E-Mail-Clients kann der Absendername beliebig verändert werden, jedoch nicht die eigentliche E-Mail-Adresse.
- **VERDÄCHTIGE ANHÄNGE:** Phishing-E-Mails enthalten z. T. **Anhänge**, die mit **Malware** infiziert sein können. Dies können auch Bilder oder Visitenkarten sein!
- **FALSCHER URL:** Phishing-E-Mails enthalten oft **Links zu gefälschten Websites**, die echt aussehen, aber tatsächlich betrügerische Ziele haben.
- **DRINGLICHE NACHRICHT:** Phishing-E-Mails **fordern oft DRINGEND dazu auf, auf einen Link zu klicken oder eine Anforderung auszuführen**, um ein bestimmtes Problem zu lösen. Seriöse Absender fordern in dieser Form nicht zur Eingabe persönlicher Daten per E-Mail oder SMS auf!
- **UNVERLANGTE NACHRICHT:** Wenn eine E-Mail **unverlangt oder unerwartet** eintrifft, sollte man generell vorsichtig sein. Ist der Zweck der **E-Mail plausibel?** Im Zweifel kann man auch beim Absender nachfragen – mit offiziellen Kontaktdaten und nicht mit den in der E-Mail angegebenen!
- **FEHLERHAFTE GRAMMATIK ODER RECHTSCHREIBUNG:** Phishing-E-Mails weisen z. T. – dank KI aber immer seltener – **Fehler in Grammatik oder Rechtschreibung** auf. Das **Fehlen von Umlauten in deutschsprachigen E-Mails** ist so auch ein Alarmzeichen.
- **FEHLENDE ODER FEHLERHAFTE ANREDE:** Ihr **Name fehlt in der Anrede gänzlich oder ist falsch geschrieben**. Wurden die **Grußformeln** wie üblich formuliert?

# Arbeitsblatt 1: Phishing-Mails analysieren

## Eine E-Mail-Nachricht

Hallo,  
dein Paket wurde zurückgehalten, da die Lieferadresse unvollständig ist. Bitte bestätige deine Adresse hier: [www.dhl-paket-info.de](http://www.dhl-paket-info.de)

Dein Paketdienst-Team

### Fragen:

1. Welche Informationen fehlen in der E-Mail, die sie glaubwürdiger machen würden?

---

---

2. Welche Schritte könntet ihr unternehmen, um herauszufinden, ob die Nachricht echt ist?

---

---

3. Welche Gefahr besteht, wenn ihr persönliche Daten oder Zahlungsinformationen auf der verlinkten Seite eingibt?

---

---

## Aufgabe 2: Phishing-Analyse und Prävention

4. Welche drei Merkmale würdet ihr bei jeder E-Mail prüfen, um sicherzugehen, dass sie echt ist?

---

---

---

5. Was sind typische Tricks, die Phishing-Betrüger anwenden, um ihre Nachrichten vertrauenswürdig erscheinen zu lassen?

---

---

6. Warum ist es wichtig, verdächtige E-Mails oder Nachrichten direkt zu melden?

---

---

## Arbeitsblatt 2: Eigene Schutzstrategien entwickeln

### Aufgabe 1: Reflexion über Sicherheitsmaßnahmen

1. Welche Sicherheitsmaßnahmen gegen Phishing nutzt du bereits?

---

---

2. Welche weiteren Sicherheitsmaßnahmen kennst du?

---

---

3. Warum ist es wichtig, E-Mails kritisch zu hinterfragen, selbst wenn sie auf den ersten Blick vertrauenswürdig aussehen?

---

---

4. Wie können sichere Passwörter dazu beitragen, Schäden durch Phishing zu begrenzen?

---

---

5. Welche Maßnahmen wenden viele Unternehmen an, um sich vor Phishing-Angriffen zu schützen?

---

---





## Bestätigung über die Durchführung eines Workshops mit Schülern und Schülerinnen

Hiermit bestätige ich, dass das Team der Pädagogischen Hochschule Freiburg im Rahmen des Projekts „MECyS – Micro-Enterprise-Cyber-Security“ am Beruflichen Schulzentrum Waldkirch einen 90-minütigen Workshop zu den Themen Cybersecurity und Datenschutz durchgeführt hat.

Der Workshop wurde durchgeführt am 27.03.2025 in Klasse Berufskolleg 2 im Fach Wirtschaftsinformatik.

An dem Workshop nahmen 7 Schüler und Schülerinnen teil.

## Confirmation of the conduction of a workshop with students

I hereby confirm that the team of the University of Education Freiburg conducted a 90-minutes workshop at Berufliches Schulzentrum Waldkirch on cybersecurity and data protection in the context of the project “MECyS – Micro-Enterprise-Cyber-Security”.

The workshop was conducted in class on 27.03.2025 in class vocational college year 2 in the subject business informatics.

7 students participated in the workshop.

9.5.25

Datum / Date

Christoph Hecker

Unterschrift / Signature



**Co-funded by  
the European Union**