

Digitale Selbstverteidigung - Workshops und OER für die Schulen



Daniel Lohninger, Josef Hörmandinger



EPICENTER

.WORKS

for digital rights

VORRATSDATENSPEICHERUNG VERHINDERT





FREE KNOWLEDGE
NEEDS  
NET NEUTRALITY

CAN I HAVE NET NEUTRALITY?
SAPPHIRE/INTERNET/ED

MEMBER
MEINE WIRTSCHAFT
RETTE
NETZNEUTRALITÄT
RETTE DAS INTERNET

DON'T LET THE EU


MAX SPEED
56
kbit/s

...ly going to
Neutrality
and India?

EXCEPT PAYING
CORPORATIONS

T PAYING
ORATIONS

Ours.
Ximon

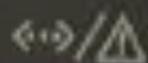
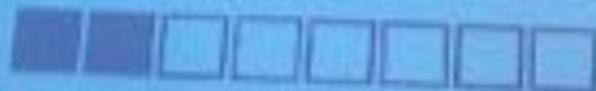
#SAVEDTHEINTERNET

NETZNEUTRALITÄT IN EUROPA
GESICHERT

Receiving Fax

P.2

SAVE THE INTERNET



JC63-02182A
JC63-02183A

Page 1 of 2
Fax Number: 1-800-368-3673
Fax Date: 20-02-2008
Fax Time: 10:00:00
Fax Status: Received

101 SAVE THE INTERNET
102 SAVE THE INTERNET
103 SAVE THE INTERNET
104 SAVE THE INTERNET
105 SAVE THE INTERNET
106 SAVE THE INTERNET
107

108 SAVE THE INTERNET
109 SAVE THE INTERNET
110 SAVE THE INTERNET
111 SAVE THE INTERNET
112 SAVE THE INTERNET
113 SAVE THE INTERNET
114 SAVE THE INTERNET
115

116 SAVE THE INTERNET
117 SAVE THE INTERNET
118 SAVE THE INTERNET
119 SAVE THE INTERNET
120 SAVE THE INTERNET
121 SAVE THE INTERNET
122 SAVE THE INTERNET
123 SAVE THE INTERNET
124 SAVE THE INTERNET
125 SAVE THE INTERNET
126 SAVE THE INTERNET
127 SAVE THE INTERNET
128 SAVE THE INTERNET
129 SAVE THE INTERNET
130 SAVE THE INTERNET

Page 2 of 2
Fax Number: 1-800-368-3673
Fax Date: 20-02-2008
Fax Time: 10:00:00
Fax Status: Received

Page	Line	Text
101	1	SAVE THE INTERNET
102	2	SAVE THE INTERNET
103	3	SAVE THE INTERNET
104	4	SAVE THE INTERNET
105	5	SAVE THE INTERNET
106	6	SAVE THE INTERNET
107	7	
108	8	SAVE THE INTERNET
109	9	SAVE THE INTERNET
110	10	SAVE THE INTERNET
111	11	SAVE THE INTERNET
112	12	SAVE THE INTERNET
113	13	SAVE THE INTERNET
114	14	SAVE THE INTERNET
115	15	
116	16	SAVE THE INTERNET
117	17	SAVE THE INTERNET
118	18	SAVE THE INTERNET
119	19	SAVE THE INTERNET
120	20	SAVE THE INTERNET
121	21	SAVE THE INTERNET
122	22	SAVE THE INTERNET
123	23	SAVE THE INTERNET
124	24	SAVE THE INTERNET
125	25	SAVE THE INTERNET
126	26	SAVE THE INTERNET
127	27	SAVE THE INTERNET
128	28	SAVE THE INTERNET
129	29	SAVE THE INTERNET
130	30	SAVE THE INTERNET

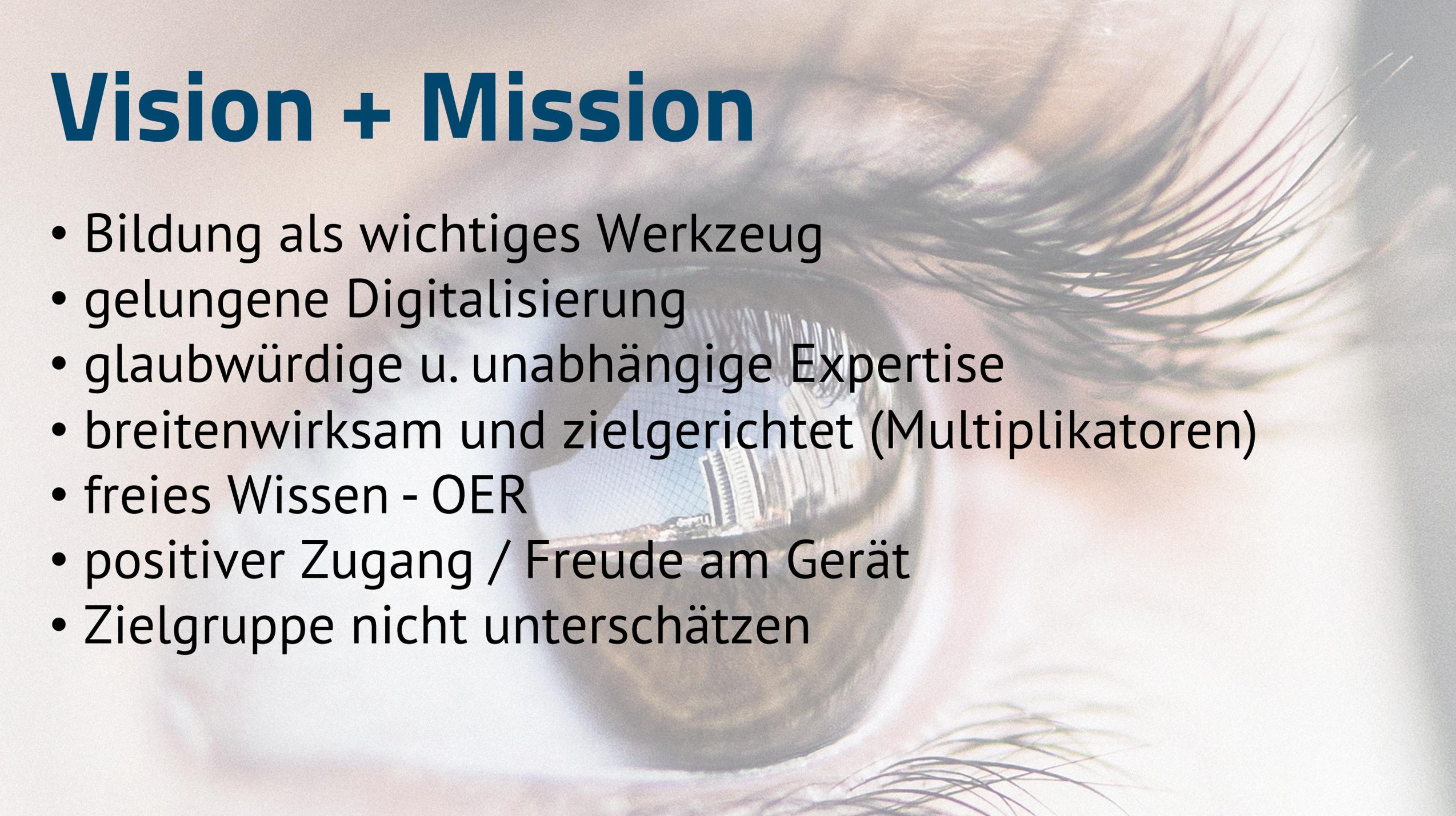


DIGITALE

SELBSTVERTEIDIGUNG

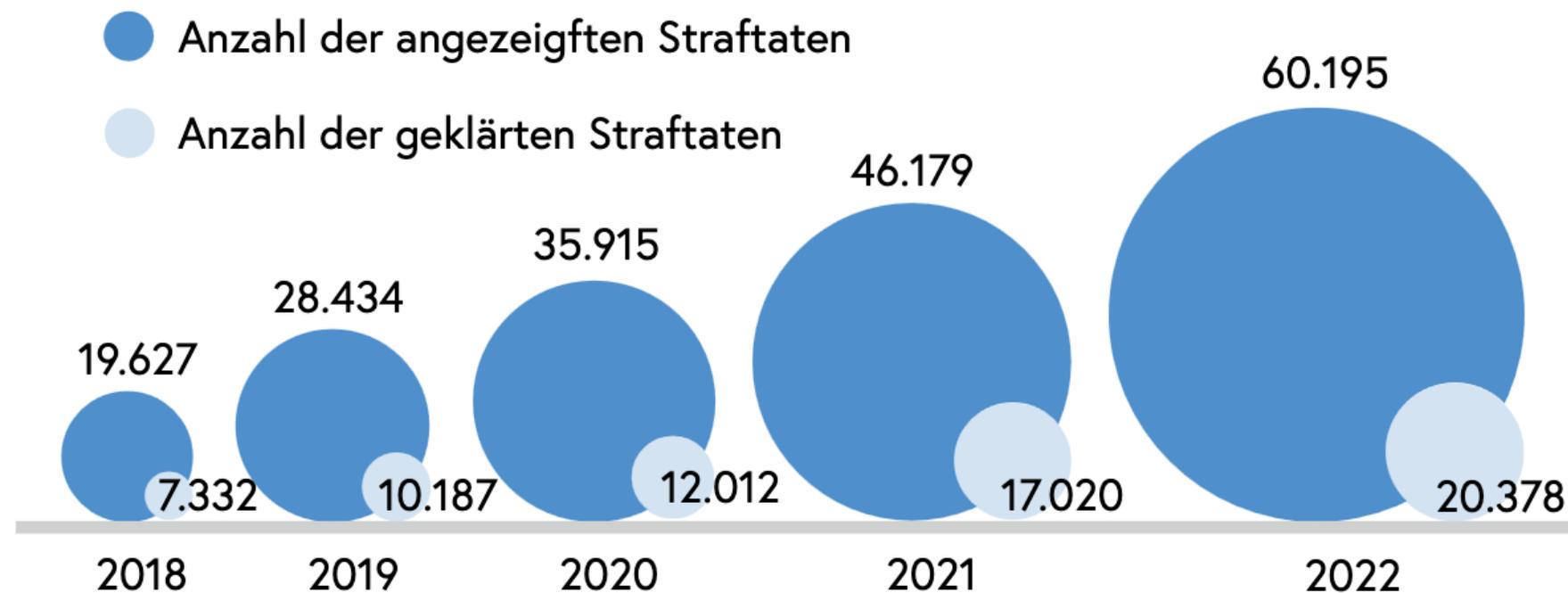
www.epicenter.works/crypto

Vision + Mission

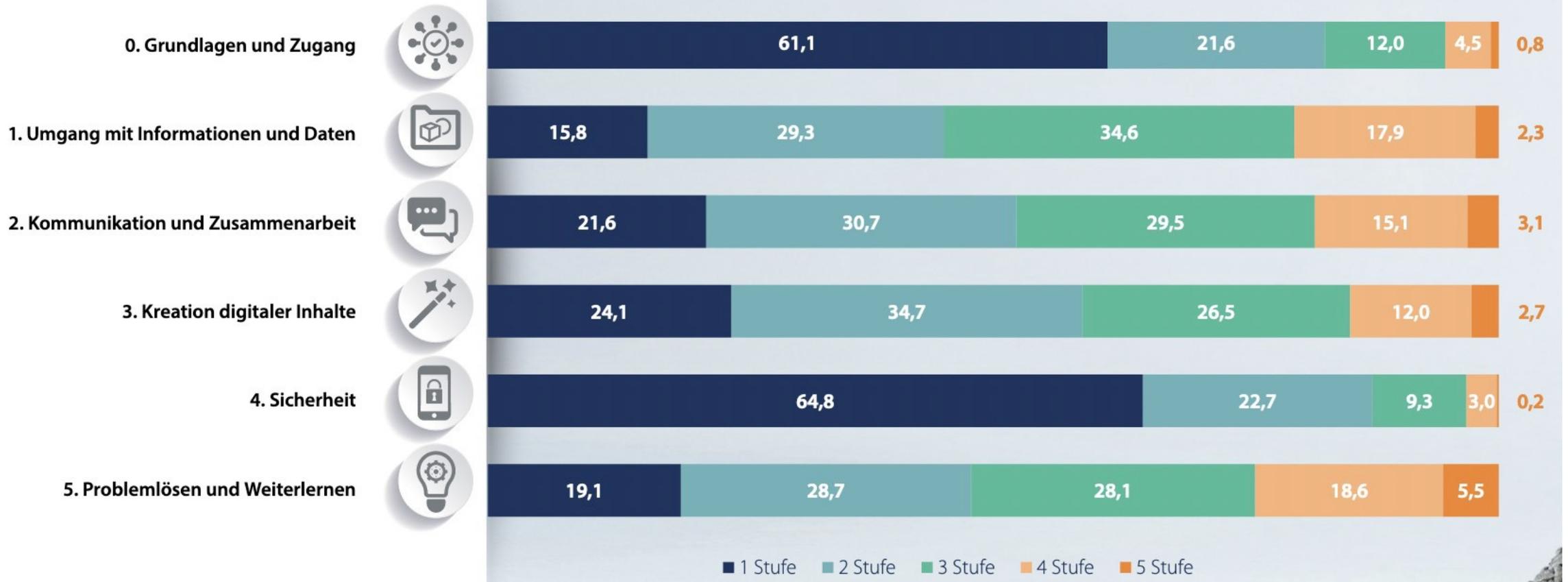


- Bildung als wichtiges Werkzeug
- gelungene Digitalisierung
- glaubwürdige u. unabhängige Expertise
- breitenwirksam und zielgerichtet (Multiplikatoren)
- freies Wissen - OER
- positiver Zugang / Freude am Gerät
- Zielgruppe nicht unterschätzen

Entwicklung der angezeigten und geklärten Cybercrime-Fälle von 2018 bis 2022 in Österreich



Anteil in % pro Kompetenzstufe



Digitale Selbstverteidigung

- OER E-Learning
- Workshopangebot
- Train-The-Trainers



E-Learning: Digitale Selbstverteidigung

BASIS

Anleitung

Eine kurze Anleitung für das selbstgesteuerte Lernen mit diesem Onlinekurs



BASIS

→

Begriffe

Erklärung wichtiger Begriffe der Digitalisierung und Netzkultur



KAPITEL 01

Warum Datenschutz?

Wie werden Daten über uns gesammelt und warum? Welche Auswirkungen hat das?



KAPITEL 02

Überwachung am Arbeitsplatz

Wie wird an Arbeitsplätzen überwacht? Was ist erlaubt? Welche Rechte habe ich?



KAPITEL 03

IT-Sicherheit? Wovor schützen?

Schutzziele, Wovor will ich mich schützen? "Threat Model"



KAPITEL 04

Digitale Verschlüsselung

Warum Mathematik unsere Freundin ist? Datenträger: verschlüsselte Tresore



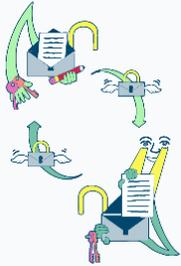
www.epicenter.academy/e-learning

E-Learning: Digitale Selbstverteidigung

KAPITEL 05

Sicher Kommunizieren

verschlüsselte Kommunikation im Internet, sichere Messenger



KAPITEL 06

Gute und schlechte Passwörter

Wann sind sie sicher? Schützen und Aufbewahren mit Passwortmanager



KAPITEL 07

Sicher im Internet surfen

Browser und Add-Ons, Suchmaschinen, Anonym im Netz mit Tor



KAPITEL 08

Geräte sicherer machen

Tipps für Einstellung und Handhabung deiner Geräte



KAPITEL 09

Phishing

Welche Tricks wenden Betrüger:innen an? Wie kannst du Gefahren erkennen und dich schützen?



KAPITEL 10

Digitale Kriminalität

Erfahre mehr darüber, wie Kriminelle versuchen dir zu schaden und wie du es verhinderst

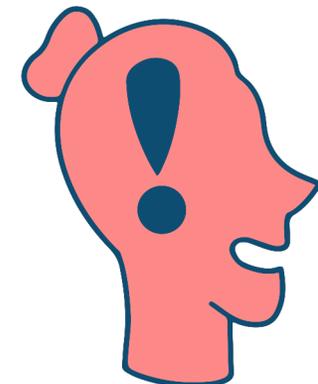
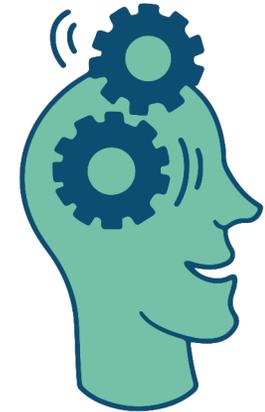
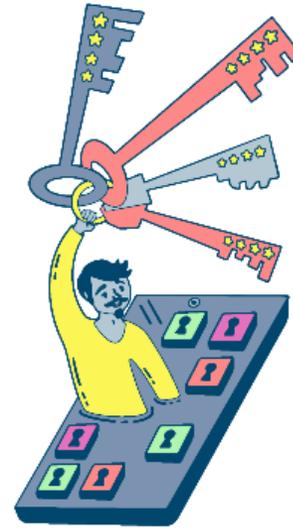


www.epicenter.academy/e-learning

Passwörter - P@\$\$w*Rt3r

In diesem Kapitel erfährst du was ein sicheres Passwort ausmacht und wie du sie auch einfach und bequem benutzt.

Die Authentifizierung, d.h. der Nachweis, dass jemand derjenige oder diejenige ist, der er/sie vorgibt zu sein, ist eine der häufigsten und wichtigsten Sicherheitsaufgaben, mit denen Benutzer:innen konfrontiert werden.



INHALTSVERZEICHNIS

Passwörter sind wichtig ^

1. [Es gibt drei Arten der Authentifizierung](#)
2. [Zwei-Faktor-Authentifizierung](#)

Was gute und schlechte Passwörter ausmacht v

Passwörter schützen und aufbewahren v

PRAXIS



Auskunftsersuchen stellen

Wir haben ein Formular (Vorlage) für ein Auskunftsersuchen, das du einmal testweise ausfüllen kannst, um zu wissen wie das geht. Wenn du tatsächlich ein Auskunftsersuchen stellst, musst du eine Kopie deines Personalausweises mitschicken.

[Zum Formular](#)

MERKE



In Betrieben OHNE Betriebsrat

In Betrieben ohne Betriebsrat dürfen technische Überwachungsmaßnahmen nur mit Zustimmung der betroffenen Arbeitnehmer:innen eingeführt und verwendet werden. Die Zustimmung kann jederzeit und ohne Einhaltung einer Frist schriftlich widerrufen werden. Achtung: Wenn du eine Einwilligung unterschrieben hast, in der auch eine Vereinbarung über die Dauer gemacht wurde, kannst du diese nicht mehr jederzeit widerrufen. Wenn du die Einwilligung zur Verarbeitung deiner Daten widerrufst, kannst du die Löschung dieser Daten verlangen. (Recht auf Löschung).

ÜBUNG



Überlege dir das Gefahrenmodell für deine Daten

Denke nun an dich: Welche Daten gibt es von dir? Welchen Gefahren sind sie ausgesetzt? Wie schützt du sie? Wie solltest du sie schützen? Erstelle dafür am besten eine Tabelle, genau wie im Beispiel von Ulrike. Vergiss nicht, den Zettel mit der Tabelle danach zu zerstören, wenn du etwas aufgeschrieben hast, das geheim bleiben soll.

ÜBUNG: STARKE UND SCHWACHE PASSWÖRTER

Ziehe die richtigen Wörter in die Lücken, damit die Zu

Ein sicheres Passwort sollte aus mindestens []
besser merken zu können, kann ein []
Passwort aus Groß- und Kleinbuchstaben, Ziffern und []
Wörter enthalten, welche in [] zu finde
kann zusätzlich eine Sicherheitsfrage zur Feststellung der []
um sich Zugriff auf den eigenen Account zu beschaffen. Um r
ein Passwort für mehrere Accounts verwendet werden.
Ein Passwort aus höchstens 8 Zeichen könnte z.B. []
Möglichkeit, um das Problem der Wiederverwendung von Pas
bietet ein [] .

Überprüfen

ÜBUNG: DATENSCHUTZ VON MESSENGERN BEWERTEN

Ordne die Messenger aus Datenschutzsicht richtig ein. Manche Messengerdienste erfüllen nicht alle erforderlichen Kriterien und sind deshalb weder als "sicher" noch als "unsicher" einzustufen.



unsicher ← → sicher

Three empty boxes for sorting the messengers.

Überprüfen

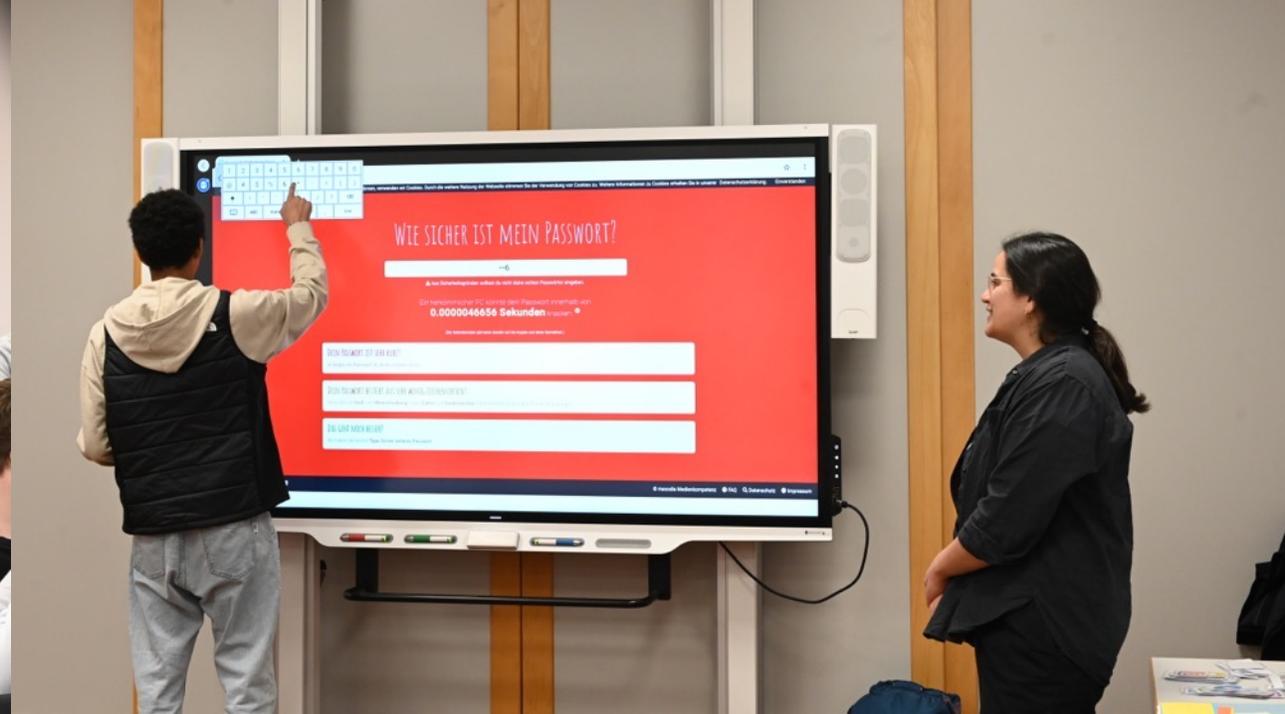


Zusätzliche Grundsätze der Gestaltung

- Diversität darstellen
- bestmögliche Barrierefreiheit







Evaluierung für Erfolgsmessung und laufende Verbesserungen

- **95%** der Befragten geben an, dass ihnen durch den Workshop **eher zw. sehr klar** geworden ist, dass sie ein **Recht auf Privatsphäre** bei der **Nutzung von Online-Tools am Arbeitsplatz** haben. (n: 273)
- **93%** der Befragten geben an, dass ihnen durch den Workshop **eher zw. sehr klar** geworden ist, dass sie für **die Sicherheit ihrer Daten aktiv sorgen** können. (n: 271)



www.epicenter.academy/workshops

O-Töne der Schüler:innen:

„Das "WIR" eingebunden wurden.“

„Es wurde alles sehr gut erklärt und durch die Videos noch etwas einfacher erklärt und verbildlicht.“



O-Töne der Schüler:innen:

„Bis jetzt bin ich noch nie bei einem Workshop gewesen, bei dem ich alles verstanden habe, also Hut ab.“

„Dass sie uns auch Apps gezeigt haben oder Beispiele, wie wir es verbessern können.“



Train-the-Trainers



didaktische Grundlagen
rechtliche Grundlagen
Geschichte
und Arbeitsweise des Vereins
Kennenlernen
des Programms und der Lernziele und der Evaluierung
Workshopdesign technisches Wissen und Verständnis
verstehen, planen und gestalten
Kenntnisse Umgang mit schwierigen Situationen im Klassensetting
über Netzpolitik, staatliche Überwachung und
Trainer*innen-Skills Überwachungskapitalismus Inhalte zu digitale Sicherheit
vermitteln Verständnis für Meta-Ebene spezielle
Kenntnisse über die Rahmenbedingungen für die Abhaltung von
Workshops an Schulen und in Unternehmen
E-Learning kennenlernen Vermittlungshandlungswissen/kompetenzen
von Haltung und Rolle/Aufgaben Trainer*in (Einbindung Lehrpersonen?)
Vermittlung
von Bewusstsein, Wissen bzw. Handlungswissen und Kompetenzen
Vermittlung
der vorab entwickelten Methoden für den Praxisworkshop nach
E-Learning Möglichkeit
Methoden Trainingssequenzen auszuprobieren und zu üben

Ausblick

