Ergebnisse aus dem dd#15

„Von der Zielscheibe zum Schutzschild - Cybersicherheit im Bildungsalltag“

Im 15. dialog digitalisierung wurden in den Co-Labs Fallbeispiele von Menschen diskutiert, die im Bildungsbereich aktiv sind. Aus der Erfahrung der Teilnehmenden wurden Handlungsoptionen für die Fallbeispiele entwickelt und im Zuge der redaktionellen Aufbereitung diese mit Handreichungen und Handlungsempfehlungen aus dem Bundesamt für Sicherheit in der Informationstechnik (BSI) angereichert. Die Ergebnisse stehen unter der Lizenz CC BY 4.0.







Arbeitsauftrag in den Co-Labs:
1. Macht euch zunächst gegenseitig mit eurem Protagonisten oder eurer Protagonistin bekannt: Auf welche Herausforderungen und Fragen könnte er ganz konkret in seinem Arbeitsalltag stoßen?
2. In welchen Bereichen muss eure Person besonders achtsam im Sinne der Cybersicherheit sein und was wären konkrete Schritte, um dort Gefahren zu vermeiden und mit „Ernstfällen“ umzugehen?

Die Fallbeispiele wurden vom Projektteam erdacht. Ähnlichkeiten mit real existierenden Menschen sind zufälliger Natur. Die Avatarbilder der Personen sind mit Hilfe von KI (Gemini) erstellt worden.

CC BY 4.0



Zur Person
- Leitet eine mittelgroße Volkshochschule
- Verantwortlich für Personal, Finanzen und Strategie

Beruflicher Medieneinsatz
- Nutzt digitale Verwaltungs- und Buchungssysteme
- Arbeitet unter anderem mit E-Mail, Cloud-Diensten und Videokonferenzsystemen
- Trifft Entscheidungen über Softwarebeschaffung, Softwarenutzung, Datenumgang, etc.

Medienkompetenz
- Gute organisatorische Kenntnisse
- Mittlere digitale Kompetenz
- Beschäftigt sich vor allem mit strategischen Fragen

Darauf könnte/sollte Sabine achten
- praktikable Sicherheitsmaßnahmen prüfen, die den Bildungsalltag nicht übermäßig einschränken und trotzdem Sicherheit bieten
- Beratung zur IT-Sicherheit einholen
- Bundesweite Initiative aller VHSen anstrengen → "Gemeinschaftskonto" für IT-Sicherheit, ggf. auf Verbandsebene?
- genaue Prüfung von Dienstleistern und Software
- Bsp. Ransomware: kein „Lösegeld“ zahlen; unabhängige Backupsysteme pflegen; ein passendes Sicherheitskonzept erstellen, bevor etwas passiert ist
- Zusammenarbeit z.B. mit RegioIT → Wer ist Ansprechpartner:in im Notfall?

Hier kann Sabine sich weiter informieren/Hilfe holen:
- Lagerbericht zur IT-Sicherheit in Deutschland: BSI - Die Lage der IT-Sicherheit in Deutschland
- Schadsoftware erkennen: BSI - Schadprogramme erkennen und sich schützen
- Das Cybersicherheitsnetzwerk des BSI: Die Ersthelferinnen und Ersthelfer des Cybersicherheitsnetzwerks (CSN)
- Rechtliche Lage: BSI - Recht im Internet



Zur Person
- Lehrt zu digitaler Kompetenzen und Mediengestaltung
- Arbeitet fast ausschließlich online

Beruflicher Medieneinsatz
- Nutzt zahlreiche Online-Tools, KI-Anwendungen und Kollaborationsplattformen
- Setzt digitale Whiteboards, Umfragetools und KI-Assistenten in Kursen ein
- Verwendet verschiedene Clouds und Apps

Medienkompetenz
- Sehr hohe digitale Kompetenz
- Experimentiert gern mit neuen Anwendungen
- Unterschätzt gelegentlich Cyberrisiken

Darauf könnte/sollte Lukas achten:
- Cybersicherheitsgrundlagen ändern sich ständig. Daher immer dran bleiben und niemals darauf ausruhen, dass man sich einmal gut ausgekannt hat!
- dauerhafte Selbstreflexion: Was gebe ich wo, wie und warum ein?
- eigene Mailadresse nur für bestimmte Anwendungen einrichten
- grundsätzlich nicht mit Klarnahmen/echten Daten arbeiten (besondere Vorsicht bei KI-Nutzung) → Datenschutz beachten
- vor dem Einsatz von Programmen/Apps diese auf Risiken prüfen → viele Schnittstellen erhöhen die Gefahr, sich mit Malware zu infizieren
- Vorab-Prüfung: Gibt ein Auftraggeber, bestimmte Regeln im Umgang mit Daten/Anwendungen/Software vor?
- „Virtuelle Maschinen“ installieren, um Websites unabhängig von deren Sicherheitseinstellungen sicher öffnen zu können (Virtuelle Maschine = Computer im Computer, der gesichertes Umfeld für externe Inhalte bietet)

Hier kann Lukas sich weiter informieren/Hilfe holen:
- Sicherheit in der Arbeit mit Clouds: BSI - Cloud-Dienste sicher nutzen
- Schutz für mobile Geräte: BSI - Schutz für Mobilgeräte
- Künstliche Intelligenz sicher nutzen: Künstliche Intelligenz sicher nutzen
- Datenverschlüsselung: BSI - Datenverschlüsselung



Zur Person
- Unterstützt (hauptsächlich) Senior*innen bei digitalem Medieneinsatz
- Ist begeisterter Social-Media-Nutzer

Beruflicher Medieneinsatz
- Nutzt seine privaten Geräte, um anderen die Freude an der digitalen Welt zu demonstrieren
- Nutzt bei Fragen, die er nicht direkt selbst beantworten kann, am liebsten KI-Chat-Bots und erklärt daran auch dessen Handhabung
- Richtet für andere Benutzerkonten für Softwareanwendungen, Apps und Sonstiges ein

Medienkompetenz
- Verfügt über eine breite Nutzungserfahrung
- Hat sich sein Wissen und Können selbst angeeignet
- Die Begeisterung für Neues überstrahlt meist sein Risikobewusstsein

Darauf könnte/sollte Harald achten:
- Passwortmanager nutzen & sichere Passwörter einrichten
- Vorsicht bei Anfragen über Social-Media und auch bei WhatsApp → „alternative“ Programme/Apps nutzen (z.B. Signal, Mastodon, ...)
- Übermittlungsweg von Passwörtern und Nutzerdaten kritisch hinterfragen
- Keine Eingabe von „personenbezogenen" Daten in die KI-Chat-Bots → die Gründe dafür auch mit Ratsuchenden teilen
- Nichts Überstürzen bei neuen Apps, Programmen und Services → erst Informieren
- Sicherheitseinstellung / Einschränkungen nutzen, um Informationen nicht "allen" zur Verfügung zu stellen → dieses Wissen weitergeben
- Apps und deren Zugriff einschränken - und diese vor der Installation prüfen

Hier kann Harald sich weiter informieren/Hilfe holen:
- Basistipps für die IT-Sicherheit: BSI - Wie kann ich meine IT zuhause absichern?
- Technologien sicher gestalten: BSI - 5G, Künstliche Intelligenz und Co. sicher gestalten
- sicher digital kommunizieren: BSI – Onlinekommunikation
- Accountschutz und Passwortsicherheit: BSI - Medienpaket zur Cybersicherheit - Account-Schutz
- Sicherheitseinstellung für Social Media: BSI - Sicherheitseinstellungen bei Facebook, WhatsApp und Co