4.1 Schützen der digitalen Arbeitsumgebung

Digitale Geräte und Umgebungen schützen sowie Risiken und Bedrohungen verstehen. Über Maßnahmen, die die eigene Privatsphäre und Sicherheit schützen, Bescheid wissen.

Illustration: Daria Rüttimann

Kompetenzbereich

Privatsphäre und Mündigkeit

Kompetenz

Schützen der digitalen Arbeitsumgebung

Hier geht es zur zentralen Downloadseite der Materialien:
bit.ly/dja-material

Thematische Einführung

digitale jugend arbeit

Facebook, *Microsoft*, *Mastercard*, *Uber*, *Nintendo*, *Google*, *Reddit*, *Sony* und *Gmail*. Alle diese Unternehmen litten in den letzten Jahren unter sogenannten Data Breaches. Das heißt, dass riesige Mengen vertraulicher Daten durch die Handlung von Hacker:innen und durch Schwachstellen im Sicherheitsnetzwerk der Firmen nach Außen gelangen konnten. Diese Datensätze wurden dann meistens gegen Geld im Internet verkauft oder anderweitig missbraucht. Diese Größenverhältnisse sind zwar für uns nicht alltäglich, aber auch in kleineren Arbeitskontexten oder auf dem Privatlaptop können sensible Daten durch Hackingangriffe, Betrug-Emails oder Data Breaches bei größeren Firmen, denen wir (bewusst oder unbewusst) freiwillig unsere Daten anvertrauen, in die falschen Hände geraten.

Deshalb ist – egal ob im privaten oder professionellen Bereich – der Schutz von Daten ein hohes Gut. Hierbei werden besonders in Arbeitskontexten vertrauliche Daten verarbeitet, denen besondere Vorsicht bemessen werden sollte. Dies macht den Schutz der digitalen Arbeitsumgebung – unabhängig von der Größe einer Organisation – besonders beachtenswert.

Hierbei tun sich Fragen auf wie beispielsweise: Wo und wie speichere ich vertrauliche Daten im Arbeitskontext? Von welchen Daten sollte ich welches Backup erstellen? Wie kommuniziere ich sicher in Arbeitsbeziehungen? Wem gebe ich potentiell wichtige Daten in die Hände, wenn ich digital mit meinen Kolleg:innen zusammenarbeite? Welche Programme und welchen Service nutzt mein Arbeitgeber und wie sicher sind diese in puncto Datenschutz? Wie gehe ich mit meinen Passwörtern im Arbeits- aber auch privaten Kontext um?

Die Beantwortung der meisten dieser Fragen sollte zwar in der Verantwortung der Arbeitgeber:innen liegen, für die korrekte Umsetzung sind allerdings die Mitarbeiter:innen verantwortlich. Deshalb ist es besonders wichtig, allgemein ein Bewusstsein für diese Themen zu schaffen. Außerdem sollten alle Mitglieder einer Organisation mit einbezogen werden. Hiermit wird sichergestellt, dass nicht nur Arbeitnehmer:innen das jeweilige Datenschutzkonzept verstehen und umsetzen können, sondern auch dass mögliche Veränderungen im Arbeitsablauf mit Verständnis angenommen werden.

Dieses Modul nähert sich dem Schutz der digitalen Arbeitsumgebung, indem es über verschiedene Themenkomplexe in diesem Bereich aufklärt. Hierbei eignen sich die Teilnehmer:innen sowohl spielerisch als auch durch Eigenrecherche praktisches Wissen über Vorgehensweisen, Programme und mögliche Sicherheitslücken rund um dieses Thema an. Ein besonderer Fokus liegt dabei auf dem Abschätzen zwischen Funktionalität und Sicherheit.

Inhalt **Seite**

Privatsphäre-Arcaden

@Trainer:innen · Moderationsbriefing · 4.1

digitale jugend arbeit

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Ausgedruckte Arbeitsmaterialien

Dauer
90 Minuten

Ziel dieser Aufgabe ist es, dass die Teilnehmer:innen sich spielerisch mit den potenziellen Sicherheitsrisiken einer digitalen Arbeitsumgebung auseinandersetzen. Darüber hinaus entdecken sie Wege, wie sie sich davor schützen können.

Ablauf

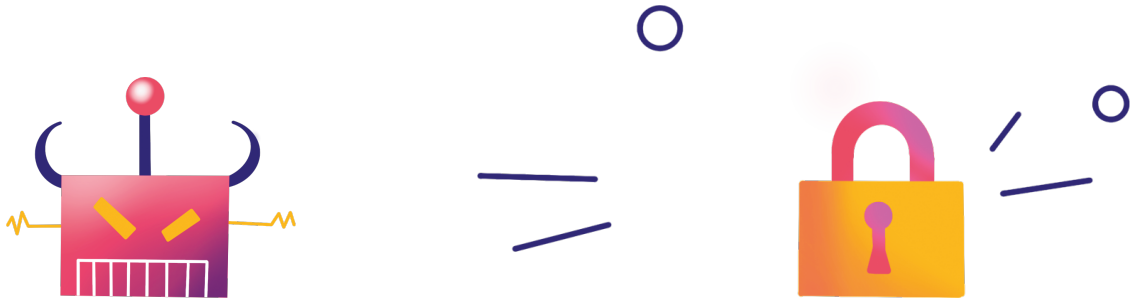
Diese Aufgabe ist als Stationenlernen gedacht. Die Teilnehmer:innen absolvieren die einzelnen Stationen zu zweit oder zu dritt und erfüllen dort die verschiedenen Aufträge oder Spiele. Nach dem Absolvieren des Spiels sollen sie auf einem ausliegenden Flipchart zur Station passende Ideen sammeln – ein konkreter Auftrag dazu ist an den Stationen jeweils beschrieben. Abschließend werden die Ergebnisse der einzelnen Stationen (auf dem Flipchart) im Plenum gemeinsam ausgewertet und offene Fragen geklärt.

Bis auf Station 1 ist es sinnvoll, die einzelnen Stationen mit (mind.) einem stationären Endgerät (Laptop bspw.) auszustatten, da die Aufgabe jeweils durch eine Webseite begleitet wird. Die Teilnehmer:innen können aber auch mit ihren eigenen Geräten die Tour durch die Stationen absolvieren.

Hinweise zur Moderation

- Da die Stationen nicht aufeinander aufbauen, können problemlos einzelne Stationen ausgelassen oder andere in ihrem Umfang erweitert werden.
- Bei den einzelnen Stationen ist jeweils eine Teilnehmer:innenzahl angegeben. Dies ist lediglich eine Empfehlung. Jede Station ist darauf ausgelegt, in Teams mit 2–3 Leuten absolviert zu werden, einige Stationen können aber auch in Einzelarbeit bearbeitet werden.
- Für die abschließende Besprechung im Plenum kann es sinnvoll sein, die Teilnehmer:innen im vorhinein darauf hinzuweisen, dass sie sich offene Fragen, die währenddessen aufkommen, notieren sollen.
- Im Arbeitsmaterial für Station 1 müssen Kärtchen ausgeschnitten und als Stapel auf der Station ausgelegt werden.
- Das Security Risks Game in Station 6 ist auf Englisch. Daher ist es sinnvoll, darauf zu achten, dass mindestens eine Person in den Teams über grundlegende Englischkenntnisse verfügt. Das Spiel funktioniert auf Touchscreens nicht ganz vollumfänglich – wenn ihr ein Gerät mit Tastatur zur Verfügung habt, setzt es an der Station alternativ ein.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«



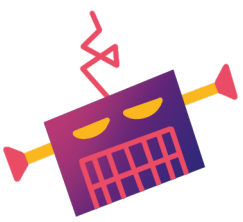
Stationsübersicht mit Lernzielen & *Hinweisen zur Vorbereitung*

digitale jugend arbeit

Safety-Buzzwords
Hier denken die Teilnehmer:innen gemeinsam über Begrifflichkeiten aus dem Bereich Schutz ihrer digitalen Umgebung nach. Im Anschluss notieren sie diejenigen Begriffe, die sie nicht kannten, auf dem ausliegendem Flipchart.
Hier sollten entweder die Karten aus Arbeitsmaterial 1 ausgedruckt und ausgeschnitten werden oder alternativ die Begriffe auf kleine Papierschnipsel geschrieben werden.

Passwort-Merk-Spiel
Die Teilnehmer:innen treten gegeneinander an und versuchen dabei, sich möglichst starke Passwörter auszudenken und sich diese auch einzuprägen. Danach reflektieren sie ihre Passwort-Strategien auf dem ausliegenden Flipchart.
Hier sollten Stifte und kleine Zettel für die Teilnehmer:innen bereitliegen. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Phishing erkennen
Woran erkenne ich gefälschte E-Mails, die in meinem Postfach auftauchen und an meine Daten heranwollen? Nachdem die Teilnehmer:innen solche in einem Online-Spiel identifiziert haben, sammeln sie auf dem Flipchart Strategien zum Erkennen von Phishing-Mails.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von Google eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.



Reflexion Datenpreisgabe
Diese Station umfasst einen Test zur persönlichen Datenpreisgabe im Internet, welcher den Teilnehmer:innen am Ende einen Score ausgibt. Auf dem Flipchart sollen sie dann Tipps zum Schutz persönlicher Daten angeben.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von netzpolitik.org eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Twitter-Wettrennen
Hier versuchen die Teilnehmer:innen innerhalb eines *Twitter*-Accounts schnellstmöglich eine spezifische Einstellung zur Privatsphäre oder der Account-Sicherheit zu finden. Auf dem Flipchart ergänzen sie dann ihre Tipps und Tricks zu den Account-Einstellung sozialer Netzwerke.
Hier ist es sinnvoll, mind. 2 Endgeräte mit neu erstellten Twitter-Accounts auszulegen. Die Suchaufträge sollten in mehrfacher Ausführung ausgedruckt, ausgeschnitten und verdeckt auf den Tisch platziert werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Security Risks Game
In diesem englischsprachigen Klick-Such-Spiel identifizieren die Teilnehmer:innen mögliche Sicherheitsrisiken in einem Büro. Danach sammeln sie weitere mögliche Sicherheitsrisiken und ergänzen jene auf dem ausliegenden Flipchart.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von Living Security eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Ausgedruckte Arbeitsmaterialien

Dauer
90 Minuten

Hier geht es zur zentralen Downloadseite der Materialien:
»bit.ly/dja-material«

Safety-Buzzwords

Im Bereich Datenschutz findet man sich schnell mit vielen – in Teilen sehr kryptisch klingenden – Fachwörtern, die nicht selten aus dem Englischen entstammen, konfrontiert. Um Strategien zum Schützen der digitalen Arbeitsumgebung besser verstehen oder auch identifizieren zu können, ist es sinnvoll, sich einmal mit diesen Fachbegriffen auseinandergesetzt zu haben.

Im vor euch liegenden Stapel findet ihr Begriffskarten mit diversen Fachwörtern. Zieht nacheinander zufällig einen von den Begriffen und überlegt gemeinsam, was das Wort bedeuten könnte. Dann notiert ihr auf dem ausliegenden Flipchart, ob ihr den Begriff kanntet oder ob ihr zum Verständnis erst ein wenig recherchieren musstet. Wiederholt das beliebig oft. Vielleicht fallen euch ja auch noch weitere Begriffe ein, die ihr auf dem Flipchart ergänzen könnt.

Scammer	Passwort-Manager	Privacy	Phishing	Backup
PGP Key	Firewall	Antiviren-programm	Catfishing	Chatbot
Zwei-Faktor-Authentifi-zierung	Encryption	Cookies	Metadaten	Geoblocking
Profiling	VPN	DSGVO	BCC	Bot
Scam	Zählpixel	Ransom-ware	Zero-Click Attacke	

Passwort-Spiel

Merk-Spiel

An dieser Station tretet ihr gegeneinander an: Wer von euch kann sich das sicherste Passwort ausdenken und merken? Dazu braucht ihr **Zettel**, **Stift** und eine **Stoppuhr**.

Lest euch **zuerst die Arbeitsanleitung** komplett durch. Zückt danach einen Zettel und Stift pro Person. Startet die Stoppuhr, sobald ihr bereit seid.

Wenn ihr fertig seid, könnt ihr euch überlegen, welche Strategie für ein sicheres Passwort die beste war. Haltet diese auf dem ausliegenden Flipchart fest. Gerne könnt ihr auch eine Hitliste der eurer Meinung nach unsichersten Passwörter aufschreiben.

Anleitung

1) Jede:r von euch hat **30 Sekunden Zeit**, um sich ein möglichst starkes Passwort auszudenken, auf den Zettel aufzuschreiben und auch einzuprägen.

2) Sind die **30 Sekunden vorbei**, dreht ihr eure Zettel um und legt sie vor euch hin.

3) Jetzt habt ihr **2 Minuten Zeit**, um nicht an euer Passwort zu denken. Unterhaltet euch zum Beispiel über die lustigste Spammail, die ihr je erhalten habt.

4) Danach habt ihr 15 Sekunden, um das von euch **gemerkte Passwort auswendig auf einen Zettel aufzuschreiben** (ohne unter den umgedrehten Zettel zu gucken, selbstverständlich).

5) Jetzt könnt ihr die **Zeit anhalten** und überprüfen, ob ihr euch euer Passwort richtig gemerkt habt.

6) Gebt gemeinsam die Passwörter auf der Webseite wiesicheristmeinpasswort.de ein, die ihr im 4. Schritt aufgeschrieben habt.

7) Die Webseite verrät euch, wie lange ein Computer bräuchte, um euer Passwort zu knacken. Außerdem könnt ihr einsehen, aus welchen „Bausteinen“ sich euer Passwort zusammensetzt, nach denen ein Programm zum Passwortknacken Ausschau hält.

8) Das Passwort, für das ein Computer am längsten bräuchte, ist das sicherste und gewinnt, vorausgesetzt, ihr habt es euch richtig gemerkt.

wie sicher ist mein Passwort .de

Passwort-Sicherheits-Check

Phishing erkennen

Unter *Phishing* versteht man betrügerische Versuche, auf digitalem Weg an Daten oder Geld heranzukommen. Das passiert beispielsweise mittels gefälschter E-Mails, Kurznachrichten, oder Webseiten. Viele Phishing-Versuche bekommt ihr zum Glück nur in dem Spam-Ordner eures E-Mail-Accounts zu sehen, da sie automatisch als unecht erkannt werden. Viele dieser Nachrichten sind oft sogar sehr amüsant.

In diesem kleinen Quiz von *Google* könnt ihr testen, wie gut ihr Phishing-Mails von ungefährlichen Mails unterscheiden könnt. Wenn ihr wollt, könnt ihr auch gegeneinander antreten und schauen, wer von euch der:die Phishing-Expert:in wird.

phishingquiz.withgoogle.com/?hl=de

Wenn ihr fertig seid, könnt ihr überlegen, welche Strategie(n) ihr verwendet, um Phishing-Mails von echten Mails zu unterscheiden. Ergänzt diese auf der ausliegenden Mindmap. Wenn ihr möchtet, schreibt eure persönliche Hitliste der absurdesten Phishing-Mail-Maschen auf.

Wie sicher ist dein digitales Ich?

Wie sicher ist dein digitales Ich? Diese Frage stellt dir das Online-Magazin für digitale Freiheitsrechte *netzpolitik.org*. Durch 10 Fragen wird dein persönlicher Privacy-Score berechnet. Es geht bei diesem Quiz weniger darum, euch anschließend zu vergleichen, wer die meisten Punkte erreicht hat. Vielmehr soll ein wenig das eigene Verhalten reflektiert und ein Verständnis entwickelt werden, welche Faktoren einen Einfluss auf den erreichten Score haben.

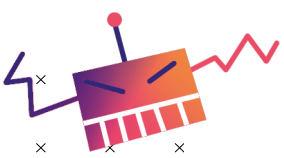
Wenn ihr fertig seid, könnt ihr euch überlegen, welche Auswirkung die Nutzung bestimmter Medien im Arbeitsalltag auf euren Datenfußabdruck hat. Danach könnt ihr Tipps zum Schützen der persönlichen Daten im Netz auf der ausliegenden Mindmap ergänzen.

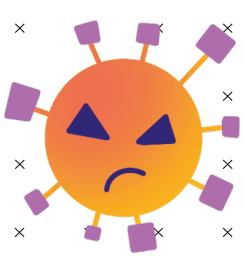
Twitter-Wettrennen: Privatsphäre Einstellungen

In den Einstellungen deines Social-Media-Accounts kann man weitaus mehr ändern als nur die Sprache oder das eigene Passwort. An dieser Station sollt ihr ein wenig in die Einstellungen eines *Twitter*-Accounts eintauchen – verpackt in einem kleinen Suchspiel.
Jede:r von euch benötigt ein eigenes Endgerät. Wenn ihr ein kleines Wettrennen daraus machen wollt, solltet ihr zunächst sicherstellen, dass ihr mit den gleichen Startvoraussetzungen antretet. Dazu gehören bspw. die gleiche *Twitter*-Anwendung (App oder Browser, iOS oder Android bspw.) auf eurem Endgerät, den gleichen Internetzugang und am besten ein möglichst unkonfigurierten *Twitter*-Account.

Anleitung
Vor euch findet ihr kleine Zettel (noch sind sie allerdings umgedreht). Darauf befinden sich 5 kleine Suchaufträge, die ihr in den „Einstellungen" eures *Twitter*-Accounts finden könnt.
Wenn ihr bereit seid, könnt ihr gemeinsam die Zettel umdrehen und so schnell wie möglich versuchen, euch an die Orte in den entsprechenden Einstellungen zu navigieren. Gefunden? Das ist gut, jetzt schreibt ihr euch entweder den entsprechenden Pfad auf einen Zettel oder ihr macht einen Screenshot als „Beweis", dass ihr die Aufgabe erfüllt habt.
Wer zuerst alle 5 Einstellungen gefunden hat, gewinnt das *Twitter*-Wettrennen. Wenn ihr möchtet, könnt ihr eure Zeit stoppen und euer Ergebnis auf dem Flipchart festhalten. Dann solltet ihr für die nächste Gruppe noch die Aufgabenzettel wieder umdrehen.

Wenn ihr damit fertig seid, könnt ihr auf dem ausliegenden Flipchart eure persönlichen Empfehlungen für „Das solltet ihr unbedingt in den Einstellung eures Sozialen-Netzwerks festlegen" ergänzen.





Teilnehmer:in Twitter-Wettrennen | Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße	Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums	Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen	Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können	Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort	Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Teilnehmer:in Twitter-Wettrennen | Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße	Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums	Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen	Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können	Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort	Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Security Risks Game

Herumliegende Festplatten oder unverschlüsselte Tablets, die mit wichtigen Daten gefüllt sind, werden meistens erst dann zum Problem, wenn sie in die falschen Hände geraten. Der Teufel steckt wie so oft im Detail. Dieses kleine Wimmelbild-Spiel sensibilisiert für jene Details, die im eigenen Arbeitsalltag potenzielle Sicherheitslücken darstellen.

Besucht die folgende – leider nicht für Touchscreen-Bildschirme optimierte – Webseite und schult eure Wahrnehmung für solche Sicherheitslücken. Ihr könnt gegeneinander antreten und schauen, wer von euch schneller ist oder gemeinsam versuchen, einen Überblick zu bekommen: hotspot.livingsecurity.com

Da die Webseite auf Englisch ist, solltet ihr schauen, dass keine:r allein den Sprachbarrieren ausgesetzt ist und dass ihr am Ende die Ergebnisse besprecht.
Wenn ihr fertig seid, dürft ihr euren (Gruppen-)Highscore, die Zeit, die ihr gebraucht habt, und die gefundenen Dinge auf dem ausliegenden Flipchart in eine Liste ergänzen. Danach könnt ihr gemeinsam überlegen, welche potentiellen Sicherheitslücken euch noch einfallen oder welchen davon ihr vielleicht im Alltag begegnet. Ergänzt diese ebenfalls auf dem Flipchart und fügt auch ein paar Strategien zum Verhindern dieser Sicherheitslücken hinzu, sofern euch welche einfallen.

Pitch mir meine Sicherheit

@Trainer:innen · Moderationsbriefing · 4.1

digitale jugend arbeit

In dieser Aufgabe lernen die Teilnehmer:innen diverse Methoden zum Schutz der digitalen Arbeitsumgebung im Hinblick auf ihre Vor- und Nachteile einzuschätzen. Außerdem erwerben sie die Kompetenz, ihr erlerntes Wissen an andere weiterzugeben.

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Vertiefung

Methode
Elevator Pitch

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

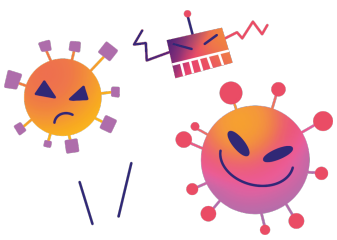
Ablauf

Die Teilnehmer:innen teilen sich in Gruppen von je 2–3 Personen auf. Jede Gruppe zieht eine der Recherchefragen (Trainingsmaterial 1), sammelt dazu selbstständig Informationen im Internet und bereitet einen kurze Präsentation vor (maximal 5 Minuten). Danach stellen sich die einzelnen Gruppen die Antworten auf ihre jeweiligen Recherchefragen gegenseitig im Plenum vor.

Hinweise zur Moderation

- Das Trainingsmaterial 1 muss vorher ausgedruckt und die einzelnen Recherchefragen ausgeschnitten werden, sodass sie zufällig bspw. aus einer Schüssel gezogen werden können.
- Die Gruppengröße und Recherchezeit kann je nach Bedarf und Anzahl der Teilnehmer:innen variiert werden.
- Abhängig von der Zeit können im Anschluss, nach Bedarf, einzelne Aspekte der Vorträge im Plenum diskutiert werden.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«



Recherchefragen

Lokaler Server vs. Cloud:

Welche Vor- und Nachteile bringt es, die Daten der Organisation auf einem eigenen, lokalen Server bzw. bei einem externen Cloud-Dienstleister zu speichern?
Welche verschiedenen Optionen bieten diese Dienste jeweils an?

Kommunikation im Arbeitskontext:

Welche Kommunikationstools nutzt ihr im Arbeitskontext?
Wie sicher sind diese jeweils?

Backup von Daten:

Für welche Daten und Dokumente sollten definitiv Backups erstellt werden? Wie oft sollte gebackuped werden? Sollten alte Backupversionen aufbewahrt werden? Wenn ja, wie weit sollte das zurückreichen? Wo werden die Backups gespeichert? Sollte diese Aufgabe auf externe Unternehmen ausgelagert werden?

Passwort-Manager:

Lohnt es sich einen Passwort-Manager zu verwenden? Welche Arten von Passwort-Managern gibt es und wie sicher und praktisch sind diese jeweils?

Daten und Dienste:

Was passiert, wenn ich mich bei verschiedenen Diensten z. B. mit meinem oder dem Arbeits-Google-Konto anmelde? Wie wird hier mit meinen Daten umgegangen?

Digitale Teamarbeit:

Welche Programme und Dienste zur Online-Teamarbeit (bspw.: Programme zum kollaborativen Schreiben, geteilte Teamterminkalender, etc.) nutze ich? Wie wird hier jeweils mit meinen vertraulichen Daten umgegangen? Gibt es hierzu Alternativen, die besonderen Wert auf Datensicherheit legen?