Guarding Your Gateways: Security Basics

Fakten

- **Workshop Zeiten:**
  - **Donnerstag 28.11.2024**

    08:00 - 12:00
  - **Freitag 29.11.2024**

    08:00 - 12:00

- **Location:** Lakeside Science & Technology Park

Wer bin ich ?

- Christian Gubesch - sehr gerne per du 🚀
- Ausbildung
  - HTL Villach Schwerpunkt: Netzwerk- und Medientechnik
  - Bachelor - Business Informatics
  - Master - Digital Entrepreneurship & Business Development
- Laufbahn
  - Cyber Security Professional - BearingPoint GmbH
    - Operations - Network and Cloud Security
    - Consulting - Cloud, Application, and OT Security
    - Business Development and Employee Training
  - Coach and Trainer for IT and CyberSec
    - TU Graz, FH Campus 02 & Fern FH Porsche
    - Freelance for Companies
    - Cyber Security Academy

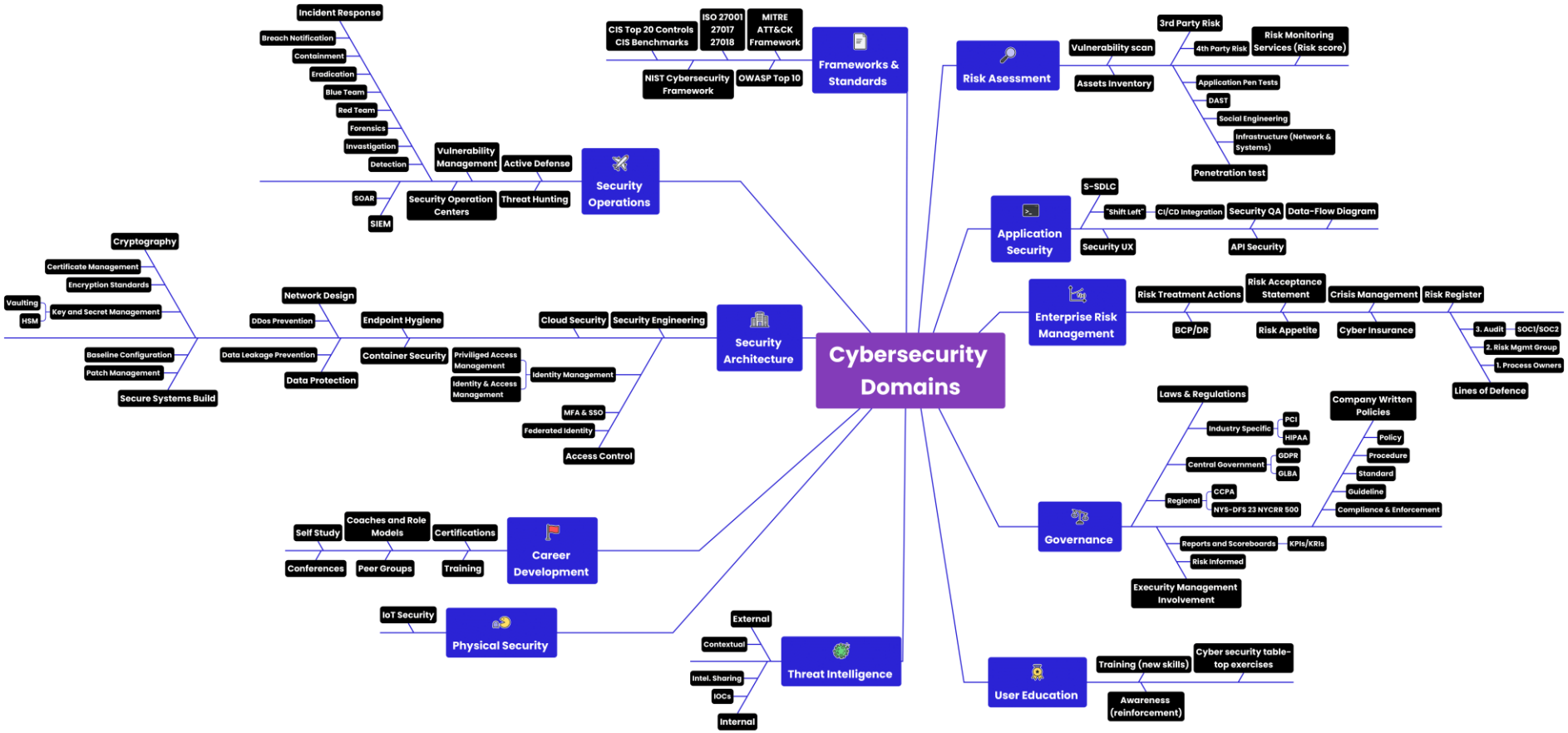
Cyber Security Academy

Wer seid ihr ?

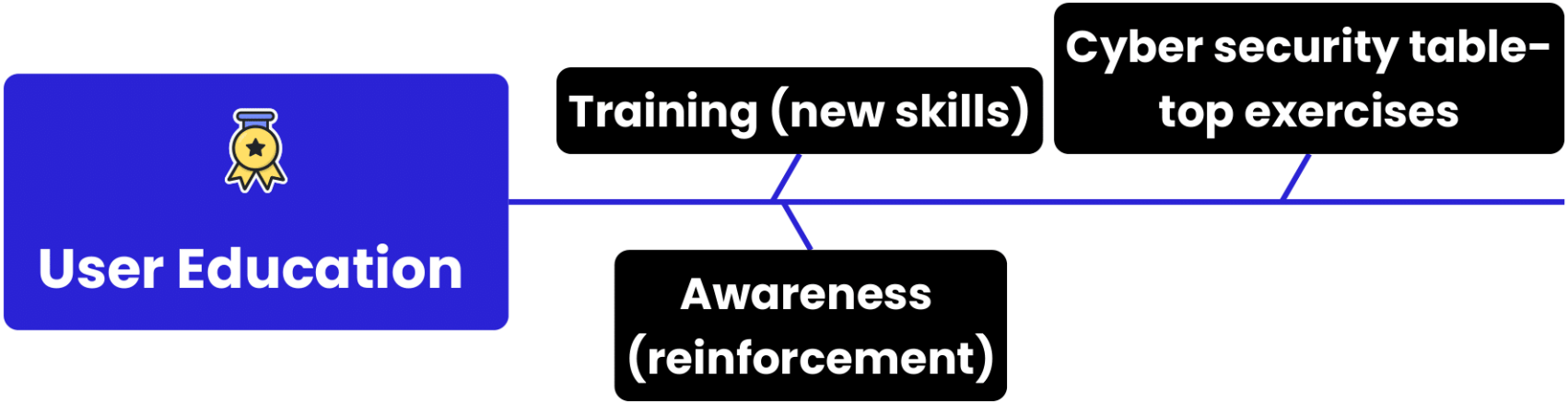
- Hintergrund
  - Job / Aufgabenbereiche
  - Berührungspunkte im Bereich Cyber-Security?
    (Privat als auch Unternehmen)
- Vorstellungen & Erwartungen
- Nach diesem Workshop will ich in der Lage sein, ...

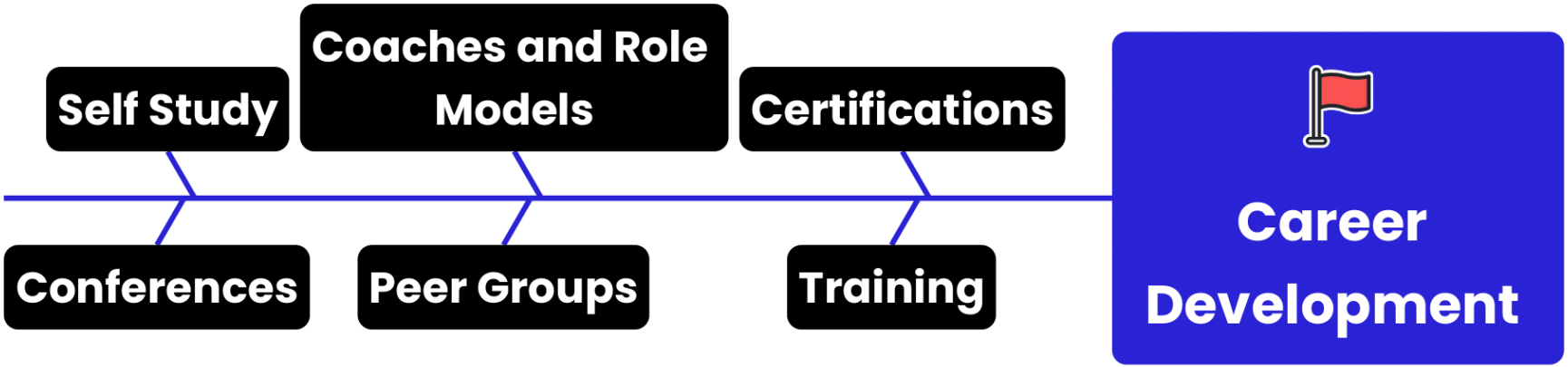
Was bedeutet Cybersicherheit für euch?

… nur mühsamer Overhead?



Quelle: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/


User Education
Training (new skills)
Cyber security table-top exercises
Awareness (reinforcement)


Self Study
Coaches and Role Models
Certifications
Conferences
Peer Groups
Training
Career Development

Warum denkt ihr, ist der euer Unternehmen ein interessantes Ziel?

Motivation von Angreifer:innen 🤺

Was macht eure Wertschöpfung aus?

Inhalte 📦

Cyberangriffe

Digitale Identitäten

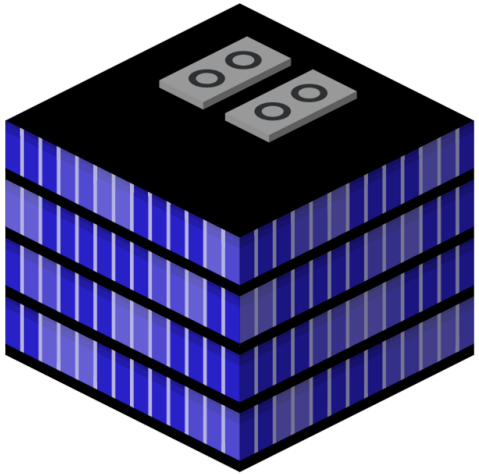
Incident Response

Datenschutz

Cyberangriffe 

und wie schnell etwas geschehen kann

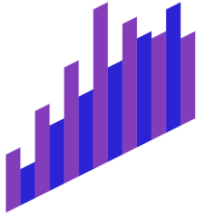
Warum werden Unternehmen gehackt?



Ghost Tech 👻

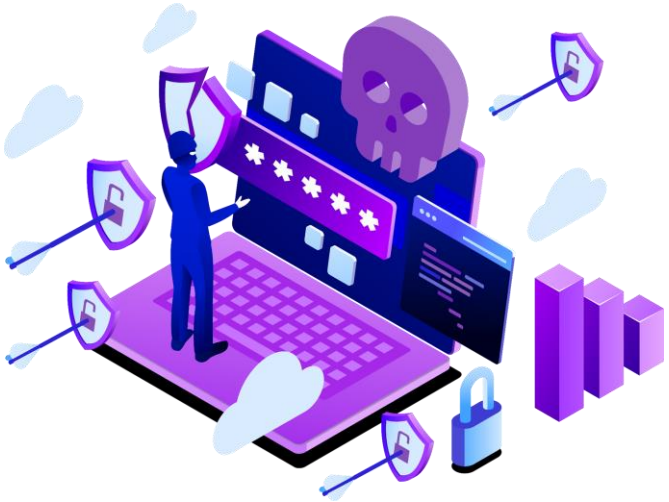
Mitarbeiter

Programme



Werbung

Wie werden Unternehmen gehackt?



vs.

Lernziele 🚀

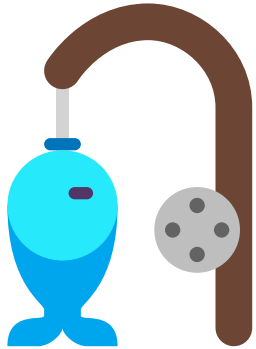
- Was sind die wichtigsten Arten von Cyberangriffen?
- Was ist Phishing und wie funktioniert es?
- Wie erkenne ich Cyberangriffe?

Welche Cyber Angriffsarten kennt Ihr?

Gängigste Cyberangriffe

2024

Phishing



Phishing nutzt Täuschung via E-Mails, Nachrichten oder Websites, um sensible Daten zu stehlen.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Phishing

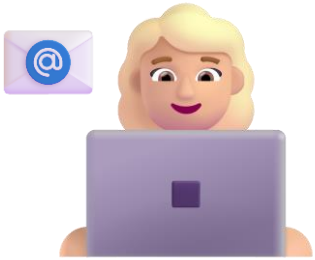
Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



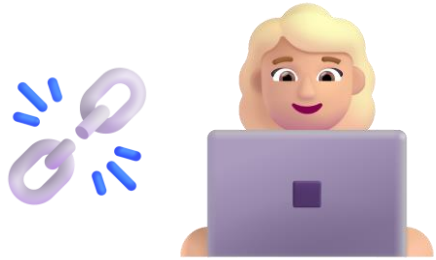
Ziel

1. Hacker sendet Phishing-Mail mit Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



Ziel

2. Benutzer öffnet Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

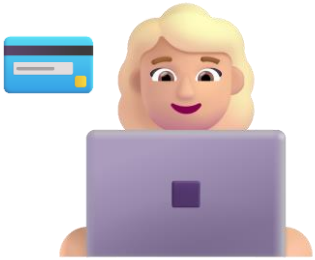
Ziel

2. Benutzer öffnet Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



Ziel

3. Hacker sammelt Benutzerdaten ein.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

3. Hacker sammelt Benutzerdaten ein.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

4. Hacker verwendet Benutzerdaten.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

4. Hacker verwendet Benutzerdaten.

Quelle: https://cybersecuritynews.com/

Ransomware

Schadhafter Code, der Daten verschlüsseln kann und für deren Entschlüsselung ein Lösegeld verlangt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Ransomware

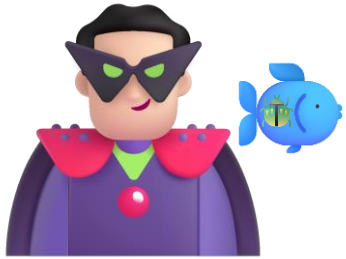
Hacker

Ziel

1. Hacker bringt Malware auf Computer von Ziel.

Quelle: https://cybersecuritynews.com/

Ransomware



Hacker

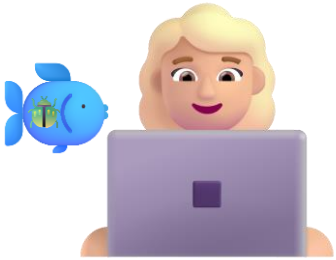
Ziel

1. Zum Beispiel durch Phishing.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

1. Zum Beispiel durch Phishing.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

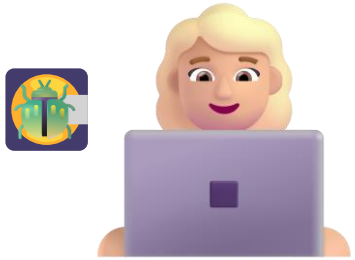
Ziel

1. Oder einem infizierten USB-Stick.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



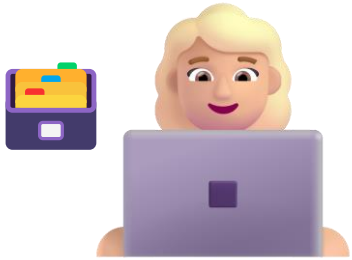
Ziel

1. Oder einem infizierten USB-Stick.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

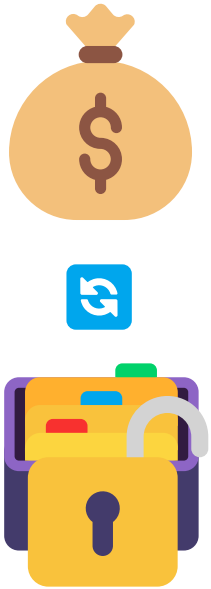
Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

3. Hacker fordert Lösegeld für Entschlüsselung.

Cyber Security Academy

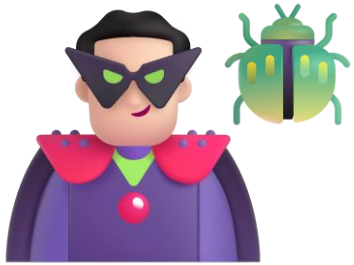
Quelle: https://cybersecuritynews.com/

Denial of Service

Eine Überlastung von Server oder Netzwerk verursachen, sodass diese nicht mehr ordnungsgemäß funktionieren.

Quelle: https://cybersecuritynews.com/

Denial of Service



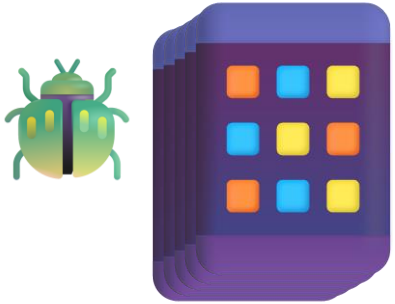
Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker



Ziel

1. Hacker kompromittiert viele Geräte mit Malware.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

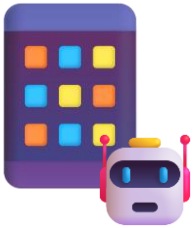
Ziel

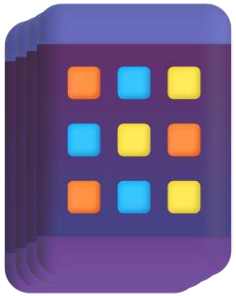
1. Hacker kompromittiert viele Geräte mit Malware.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker





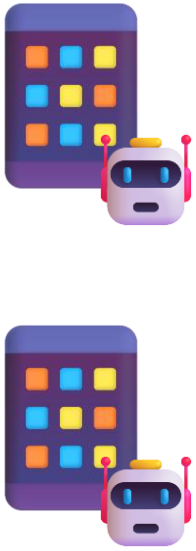
Ziel

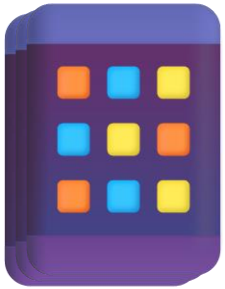
2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker





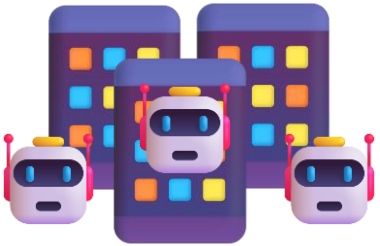
Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker



Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

3. Hacker greift mit „bot net“ an.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

3. Hacker greift mit „bot net“ an.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

4. Ziel Service wird beeinträchtigt.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

4. Ziel Service wird beeinträchtigt.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Quelle: https://sosafe-awareness.com/de/glossar/ceo-fraud/

CEO Fraud

Geld- oder Datenklau durch gefälschte Anweisungen von Führungskräften.

Quelle: https://sosafe-awareness.com/de/glossar/ceo-fraud/

CEO Fraud

Hacker

Ziel

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

Ziel

1. Hacker gibt sich als CEO aus.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

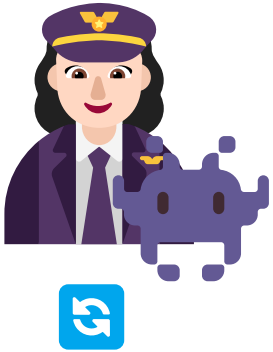
Ziel

1. Hacker gibt sich als CEO aus.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker



Ziel

1. Zum Beispiel mit AI-Voice.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

Ziel

2. Hacker kontaktiert Mitarbeiter.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

Ziel

2. Hacker kontaktiert Mitarbeiter.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

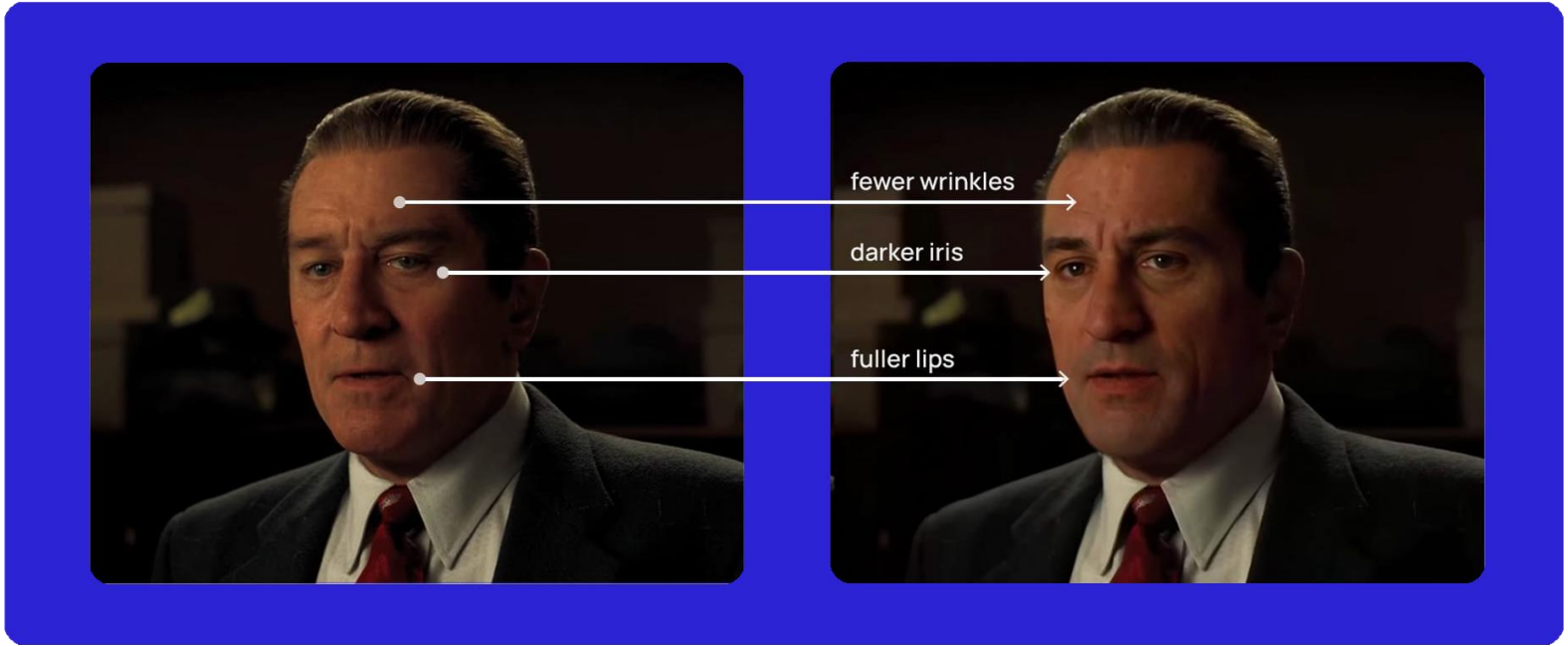
Ziel

3. Hacker fordert Geld oder Daten als „CEO“.

Cyber Security Academy

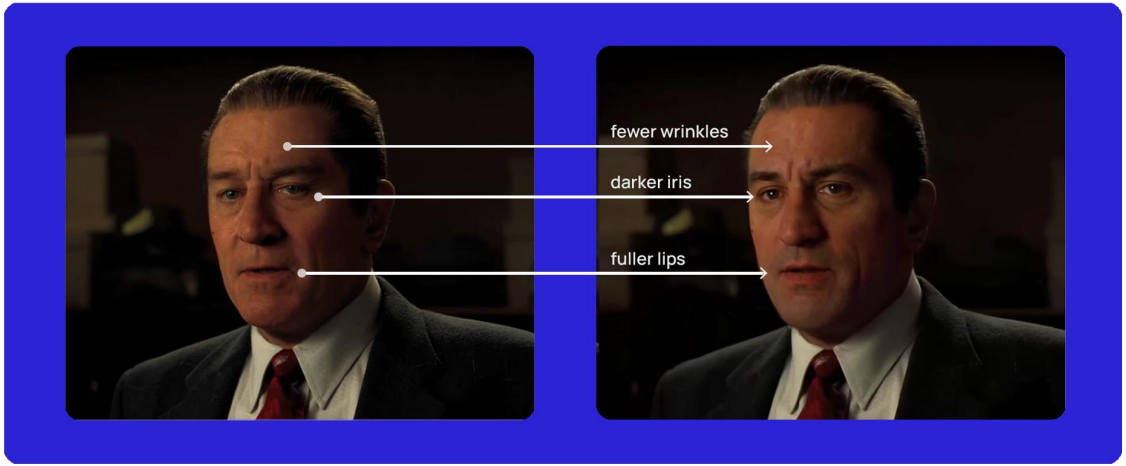
Quelle: https://cybersecuritynews.com/

AI & Deepfakes



Quelle: https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

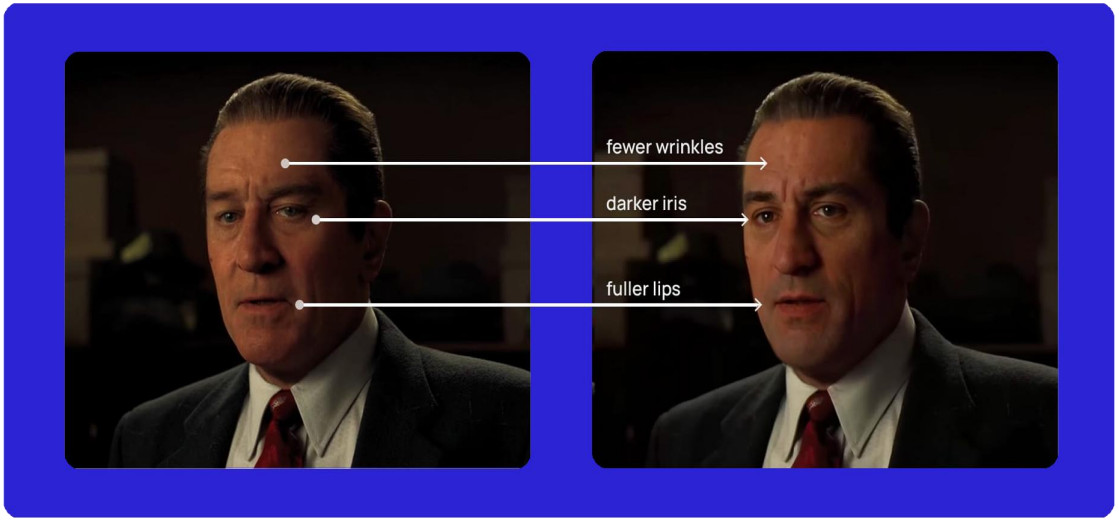
AI & Deepfakes



Fälschung von Videos/Audio zur Täuschung.

Quelle: https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

AI & Deepfakes



Quelle: https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

DNS Spoofing

Umleitung auf gefälschte Websites, um Daten abzufangen.

Quelle: https://cybersecuritynews.com/

Was ist DNS ?

Was ist DNS?

Domain **N**ame **S**ystem

Cyber Security Academy

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

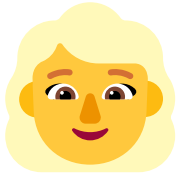
Was ist DNS?

Name	IP-Adresse
www.orf.at	184.231.10.114

Cyber Security Academy

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

Was ist DNS?



Name

IP-Adresse

www.orf.at

184.231.10.114

Cyber Security Academy

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

Live Demo 

DNS Spoofing

Jetzt seid Ihr dran! 

Praxisübung - Phishing Research

Ablauf ⏩

- Durchsuche deinen eigenen E-Mail-Account (auch den Spam-Ordner) nach verdächtigen Mails.

Dokumentation 📄

- Merkmale, warum denkst du, es handelt sich um eine Phishing Mail?

Zeit & Format 🕐

- 10 min Recherche
- 5 min Präsentation

Exkurs – Betrugswarnungen

WKO

Kontakt Anmelden

Transforma... Digitalisierung Nachhaltigkeit Startups Creative Industries Innovation Kärnten

Aktuelle Betrugswarnungen für Unternehmen

Übersicht irreführend gestalteter Aussendungen, Betrugsversuchen, Phishing...

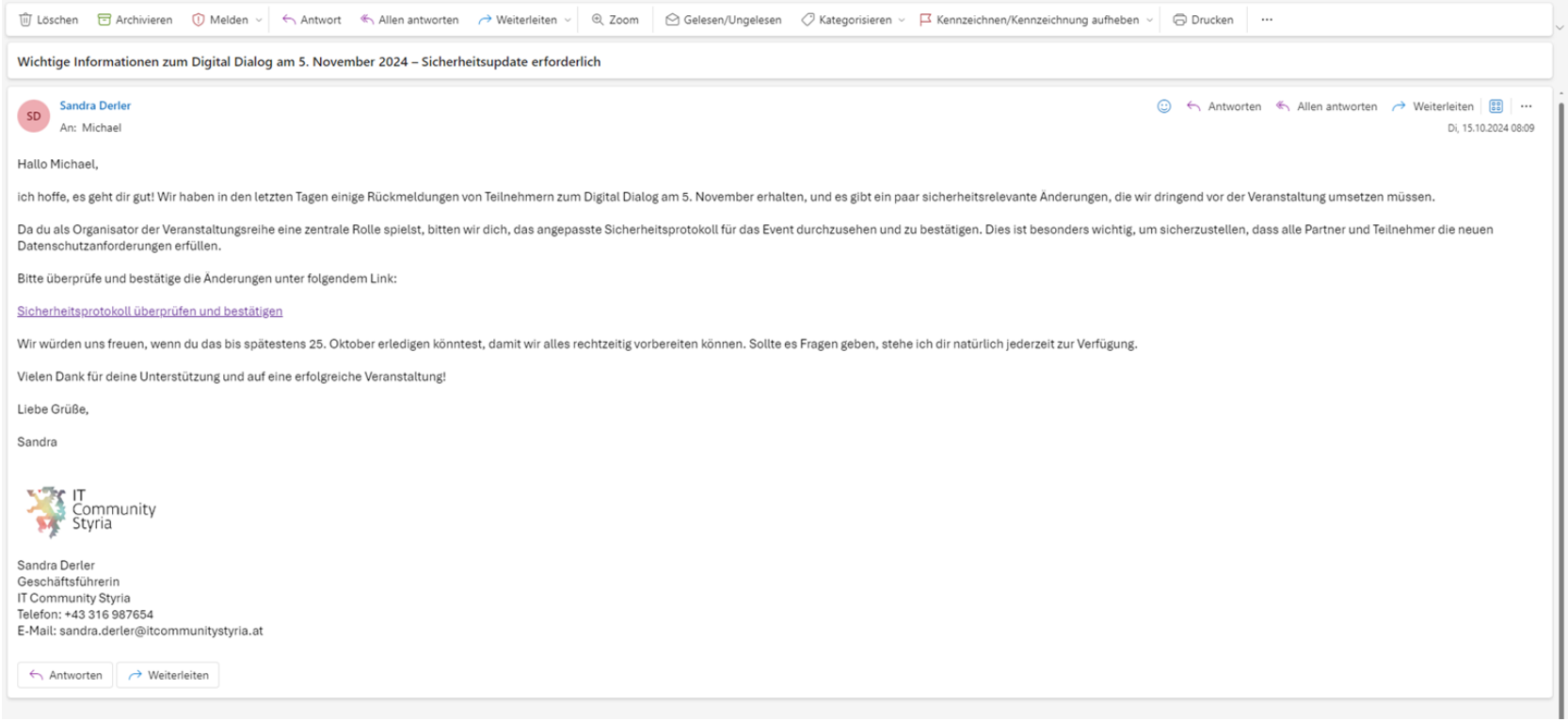
Lesedauer: 3 Minuten

© christianchan | stock.adobe.com

17.01.2023

Zeit für ein Quiz! 

Beispiel Phishing Mail - Digital Dialog



Löschen | Archivieren | Melden | Antwort | Allen antworten | Weiterleiten | Zoom | Gelesen/Ungelesen | Kategorisieren | Kennzeichnen/Kennzeichnung aufheben | Drucken | ...

Wichtige Informationen zum Digital Dialog am 5. November 2024 – Sicherheitsupdate erforderlich

SD **Sandra Derler**
An: Michael

Antworten | Allen antworten | Weiterleiten

Di, 15.10.2024 08:09

Hallo Michael,

ich hoffe, es geht dir gut! Wir haben in den letzten Tagen einige Rückmeldungen von Teilnehmern zum Digital Dialog am 5. November erhalten, und es gibt ein paar sicherheitsrelevante Änderungen, die wir dringend vor der Veranstaltung umsetzen müssen.

Da du als Organisator der Veranstaltungsreihe eine zentrale Rolle spielst, bitten wir dich, das angepasste Sicherheitsprotokoll für das Event durchzusehen und zu bestätigen. Dies ist besonders wichtig, um sicherzustellen, dass alle Partner und Teilnehmer die neuen Datenschutzanforderungen erfüllen.

Bitte überprüfe und bestätige die Änderungen unter folgendem Link:

Sicherheitsprotokoll überprüfen und bestätigen

Wir würden uns freuen, wenn du das bis spätestens 25. Oktober erledigen könntest, damit wir alles rechtzeitig vorbereiten können. Sollte es Fragen geben, stehe ich dir natürlich jederzeit zur Verfügung.

Vielen Dank für deine Unterstützung und auf eine erfolgreiche Veranstaltung!

Liebe Grüße,

Sandra

IT Community Styria

Sandra Derler
Geschäftsführerin
IT Community Styria
Telefon: +43 316 987654
E-Mail: sandra.derler@itcommunitystyria.at

Antworten | Weiterleiten

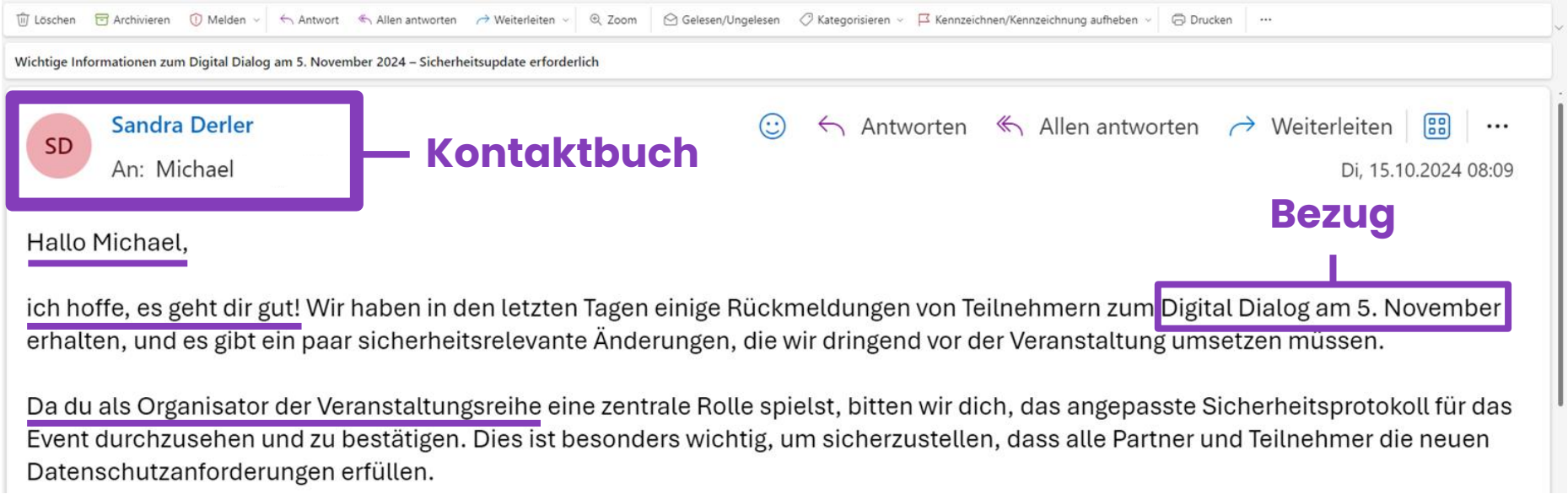
Cyber Security Academy

Beispiel Phishing Mail – Der Einstieg

Wichtige Informationen zum Digital Dialog am 5. November 2024 – Sicherheitsupdate erforderlich

Dringlichkeit und Kontext

Beispiel Phishing Mail - Vertrauen aufbauen



Persönlicher Ton

Beispiel Phishing Mail - Handlungsaufforderung

Bitte überprüfe und bestätige die Änderungen unter folgendem Link:

Sicherheitsprotokoll überprüfen und bestätigen

Call-to-Action als Hyperlink

Wir würden uns freuen, wenn du das bis spätestens 25. Oktober erledigen könntest, damit wir alles rechtzeitig vorbereiten können. Sollte es Fragen geben, stehe ich dir natürlich jederzeit zur Verfügung.

Deadline

Vielen Dank für deine Unterstützung und auf eine erfolgreiche Veranstaltung!

Versicherung

Liebe Grüße,

Sandra

Beispiel Phishing Mail – Signatur

Liebe Grüße,

Sandra

Antworten Weiterleiten

Multi Channel Phishing

Gefälschte Telefonnummer in Signatur für telefonische Bestätigung

Diskussion! 

Lernziele 🚀

- Was sind die wichtigsten Arten von Cyberangriffen?
- Was ist Phishing und wie funktioniert es?
- Wie erkenne ich Cyberangriffe?

Inhalte 📦

Cyberangriffe

Digitale Identitäten

Incident Response

Datenschutz

Inhalte 📦

Cyberangriffe

Digitale Identitäten

Incident Response

Datenschutz

Digitale Identitäten 

und wie ihr sicher mit Daten umgeht

Lernziele 🚀

- Was ist eine digitale Identität?
- Warum ist Passwortsicherheit wichtig?
- Wie verwende ich meinen Browser richtig?

Was ist eine digitale Identität?

Digitale Identität - Ausweiskontrolle

Zu schnell unterwegs gewesen?

Quelle: https://www.okta.com/identity-101/digital-identity

Was denkt ihr, wie viele Personen in der EU besitzen eine digitale Identität?

91%

besitzen eine digitale Identität in Europa (2024)

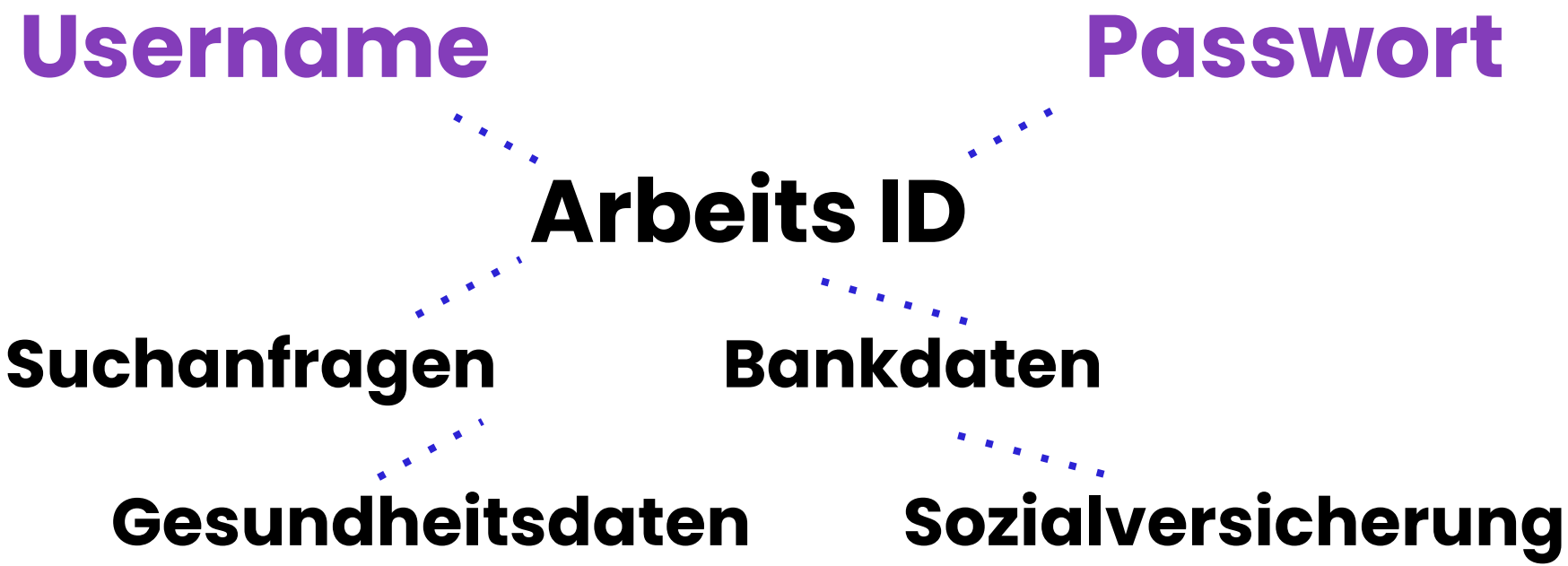
Quelle: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ifp_iu/default/table?lang=en

Digitale Identität – Ausweis im Internet

Informationen, die online existieren und eine Person, ein Unternehmen oder eine Organisation identifizieren

Quelle: https://www.okta.com/identity-101/digital-identity

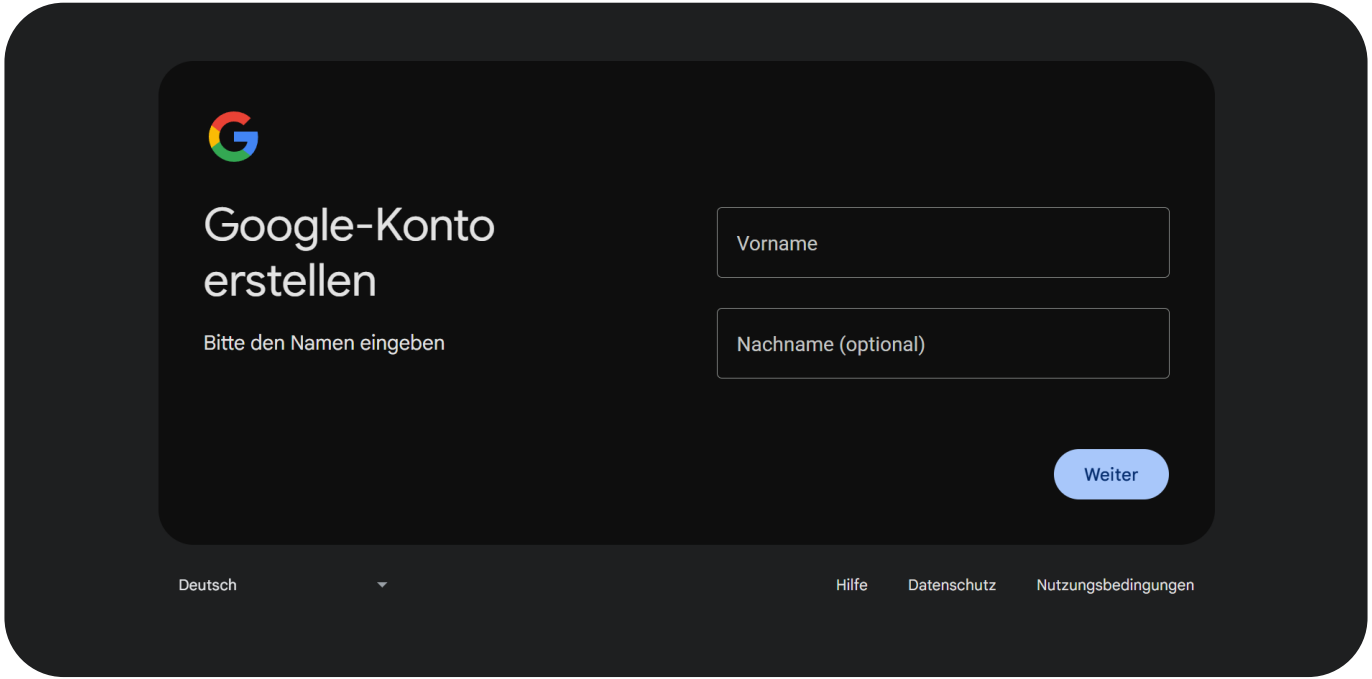
Digitale Identität – Beispiele



Quelle: https://www.okta.com/identity-101/digital-identity

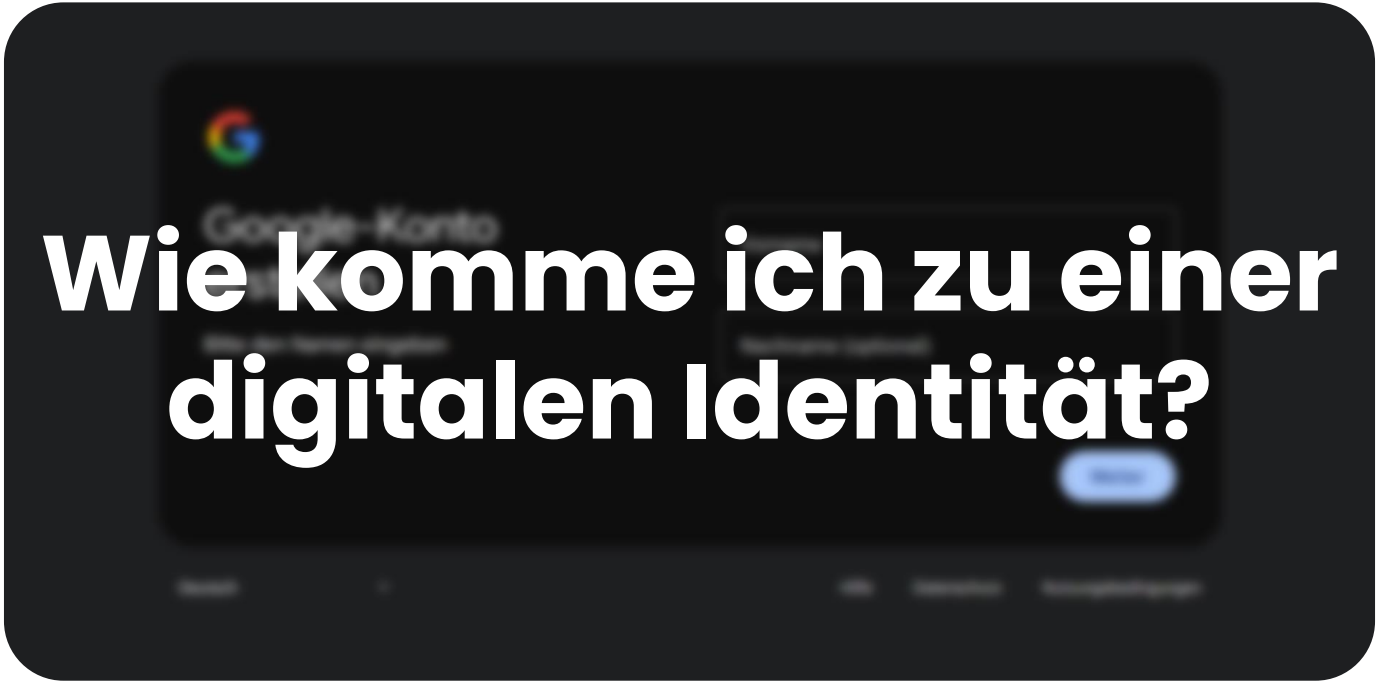
Verwaltet ihr im Unternehmen digitale Identitäten?

Digitale Identität – Registrierung



Quelle: https://www.okta.com/identity-101/digital-identity

Digitale Identität – Registrierung



Quelle: https://www.okta.com/identity-101/digital-identity

Digitale Identität - Ausweiskontrolle im Internet

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Digitale Identität – Ausweiskontrolle im Internet

1 Authentication
2 Authorization
3 Accounting

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Digitale Identität – Ausweiskontrolle im Internet

1

Authentication

Beweise, dass du DU bist

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Digitale Identität – Ausweiskontrolle im Internet

2

Authorization

Was du machen darfst

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Digitale Identität – Ausweiskontrolle im Internet

3

Accounting

Protokoll, was machst du

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Digitale Identität – Ausweiskontrolle im Internet

Authentication - Beweise, dass du DU bist

Authorization - Was du machen darfst

Accounting - Protokoll, was machst du

Quelle: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting

Jetzt seid Ihr dran! 

Praxisübung - Digitale Identitäten

Ablauf ⏩

- Versuche herauszufinden, welche digitale Identitäten von dir im Arbeitsumfeld existieren

Tipps 💡

- Beginne mit den Authentifizierungs Anbietern (Google, Microsoft usw.)

Dokumentation 📃

- Erstelle eine Mindmap mit allen dig. Identitäten.

Zeit & Format 🕐

- 20 min Recherche
- 5 min Diskussion

Digitale Identitäten - Wo liegt das Problem?

80% der Cyber Angriffe starten mit dem Passwort

191 Passwörter hat ein Angestellter im Durschnitt

34% der Accounts werden mit MFA geschützt (<100 Mitarbeiter)

Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Welche Merkmale hat ein sicheres Passwort ?

Digitale Identitäten - Passwortsicherheit

- Keine persönlichen Informationen*
- Keine Wörter aus dem Wörterbuch
- Zahlen, Symbole & Groß- und Kleinbuchstaben (min. 12 Zeichen)
- Passwörter nicht wiederverwenden!

Quelle: https://www.okta.com/de/identity-101/password-vs-passphrase/

*im Volltext

Woher weiss ich, dass mein Passwort sicher ist?

Woher weiss ich, dass mein Passwort sicher ist?

Testen

UoP22lawdme3tWJH1#7jBRWcdg**d%P&%z

Tolles Passwort!

- Ihr Passwort hält Angriffen von Hackern stand.
- Ihr Passwort taucht in keiner Datenbank mit kompromittierten Passwörtern auf.

Ihr Passwort kann mit einer Bruteforce-Attacke geknackt werden – mit einem normalen Heim-PC in etwa.....

10000+ Jahrhunderte

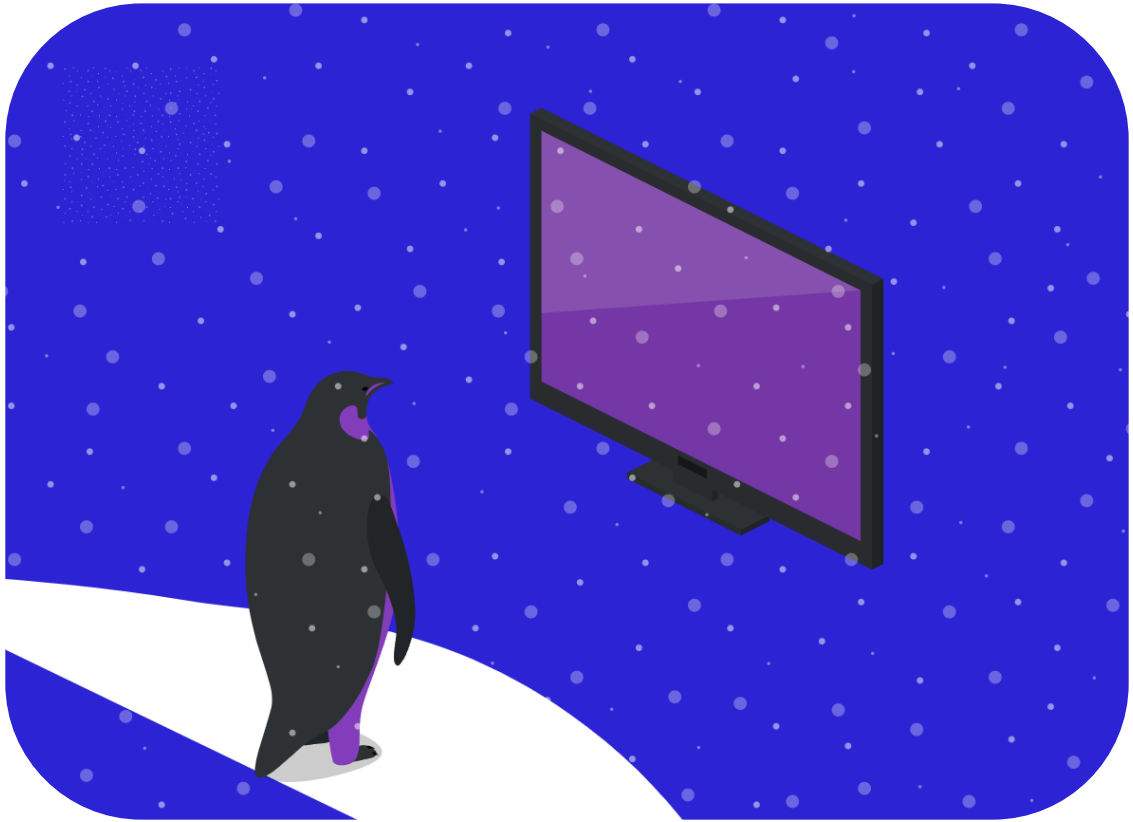
In dieser Zeit können Sie die Antwort auf die Frage "nach dem Leben, dem Universum und dem ganzen Rest" finden.

Wie merkt man sich ein sicheres Passwort?

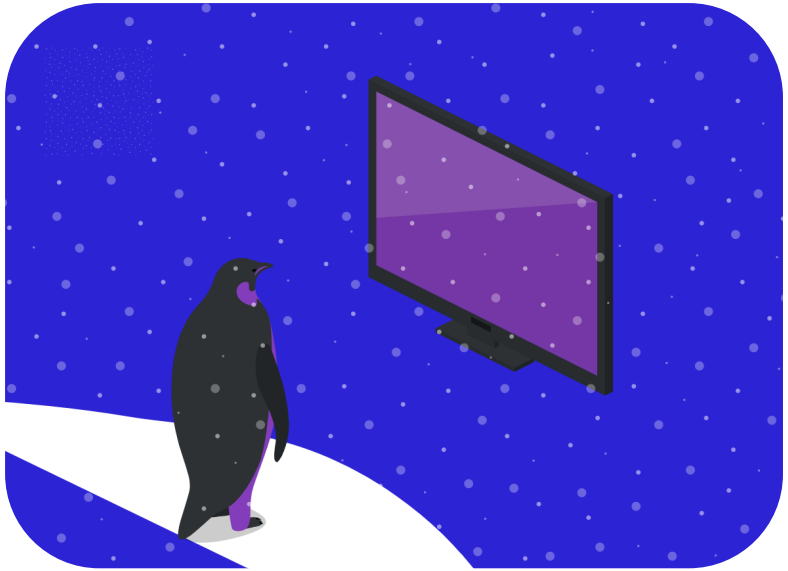
10000+ Jahrhunderte

In dieser Zeit können Sie die Antwort auf die Frage "nach dem Leben, dem Universum und dem ganzen Rest" finden.

Cyber Security Academy

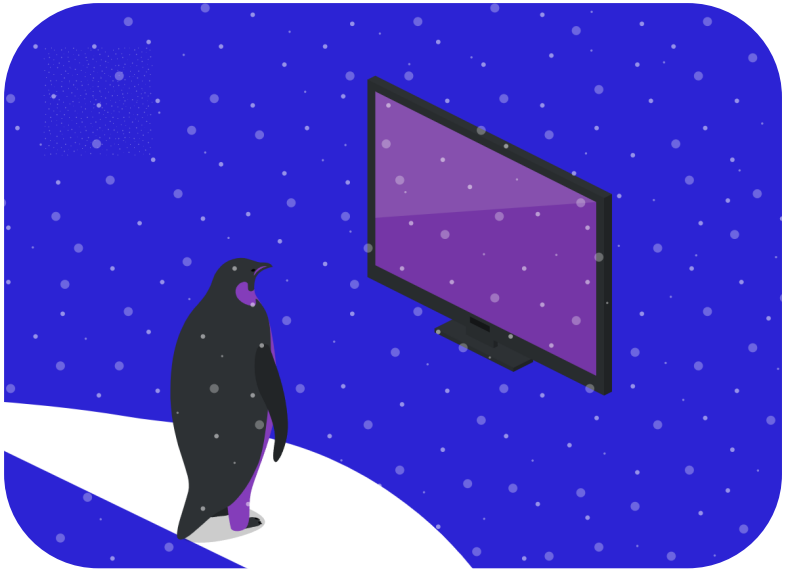


1. Objekte im Bild



Pinguin-Fernsehen-Schnee

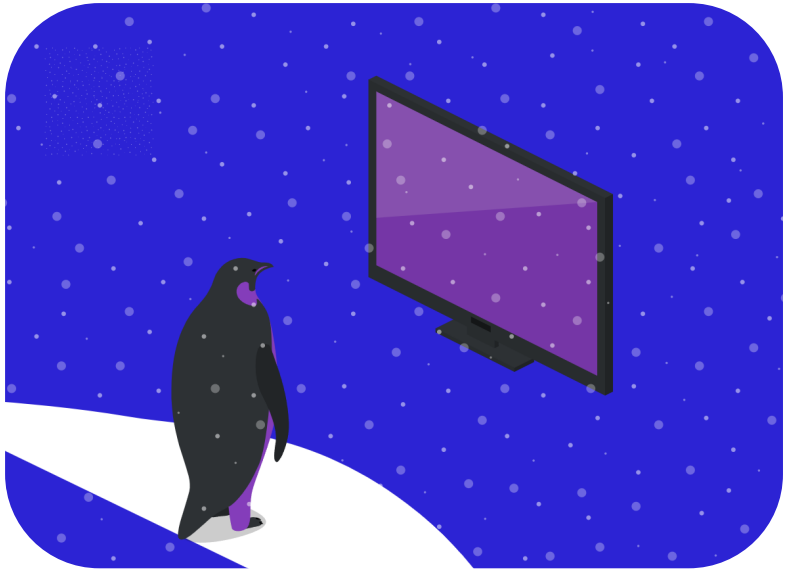
2. Schreibweise



pinguin-Fernsehen-schnee

3. Zahl

z.B älteste Pinguin der Welt



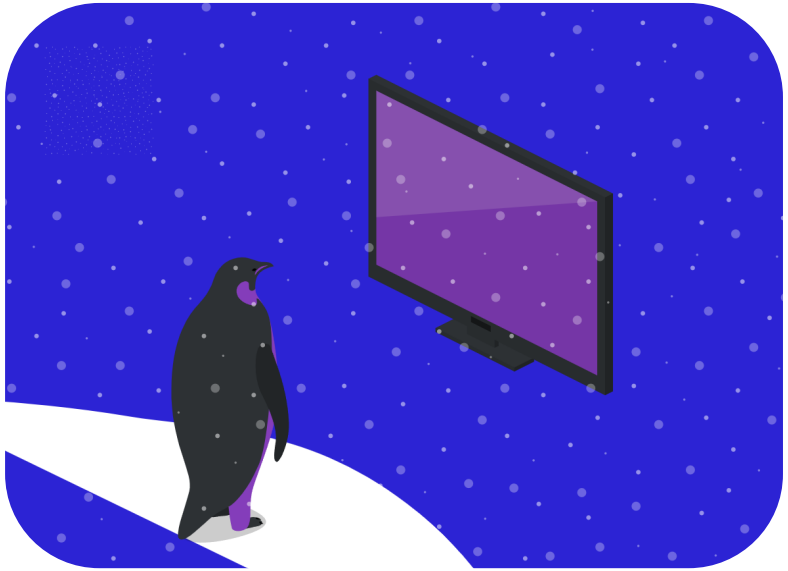
pinguin-Fernsehen-schnee

OMA

46

3. Zahl

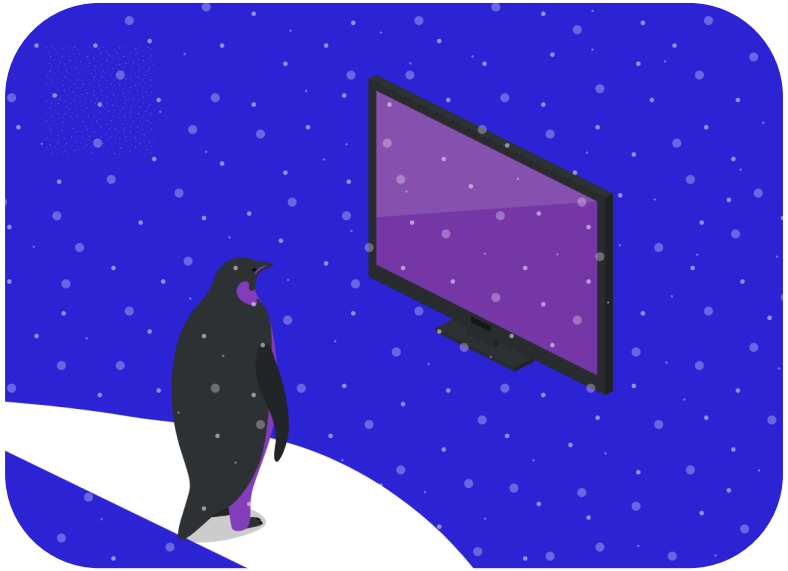
z.B älteste Pinguin der Welt



pinguin-Fernsehen-schnee-46

4. Sonderzeichen

z.B wo findet das statt?



pinguin-Fernsehen-schnee-46@Südpol

Wie machen wir das jetzt für unsere ganzen Identitäten?

Beruflich anders als privat?

Digitale Identitäten – Passwortmanagement

- Verwalten von Passwörtern & anderen sensiblen Daten
- Kein Merken von Passwörtern Notwendig
  - Daher starke Passwörter möglich
  - Überwachung von “Kompromittierung ”
- Unkomplizierte Verwendung
- Gibt 3 Varianten von Passwortsafes
  - Lokale Installation
  - Online Managed Installation
  - Self Hosted Installation

Passwortmanager – Überblick

Lokale „Installation“

KeePass

KeePassXC

All in One Managed

NordPass

KEEPER
Cybersecurity Starts Here

1Password

bitwarden

Online Hosted & Managed

Self-Hosted Installation

Vaultwarden

bitwarden

Community Edition

Free Tier

Free Tier mit Aufwand

Cyber Security Academy

Live Demo 

Sauberes Passwortmanagement
Methoden für neuen Account

Digitale Identitäten – Passwortsicherheit Recap

- Keine persönlichen Informationen*
- Keine Wörter aus dem Wörterbuch
- Zahlen, Symbole & Groß- und Kleinbuchstaben (min. 12 Zeichen)
- Passwörter nicht wiederverwenden!

Hand aufs Herz

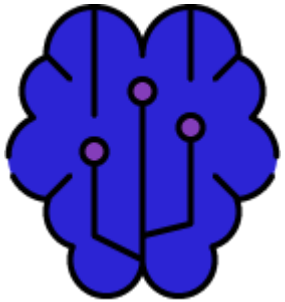
Bei wem von euch ist das Master Passwort nicht nach den Kriterien?

Cyber Security Academy

Quelle: https://www.okta.com/de/identity-101/password-vs-passphrase/

*im Volltext

Digitale Identitäten - Passwortsicherheit



Social Engineering

Bruteforce Attacke

Digitale Identitäten - Passwortsicherheit

Wie schützen wir uns dagegen?

Social Engineering

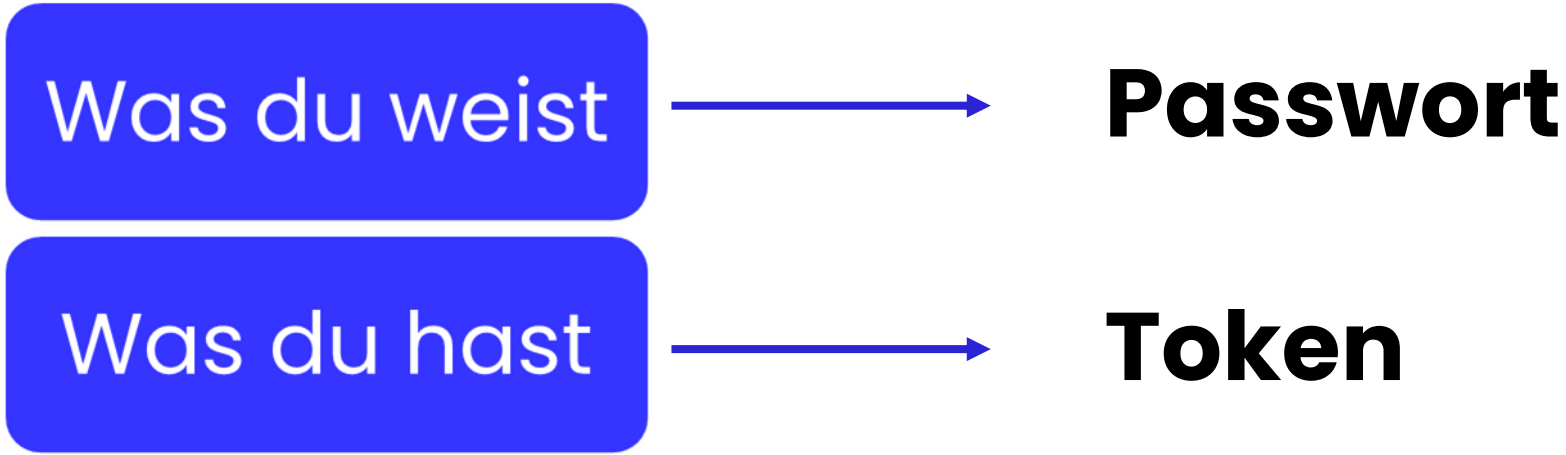
Bruteforce Attacke

Multi Factor Authentication

Passwort

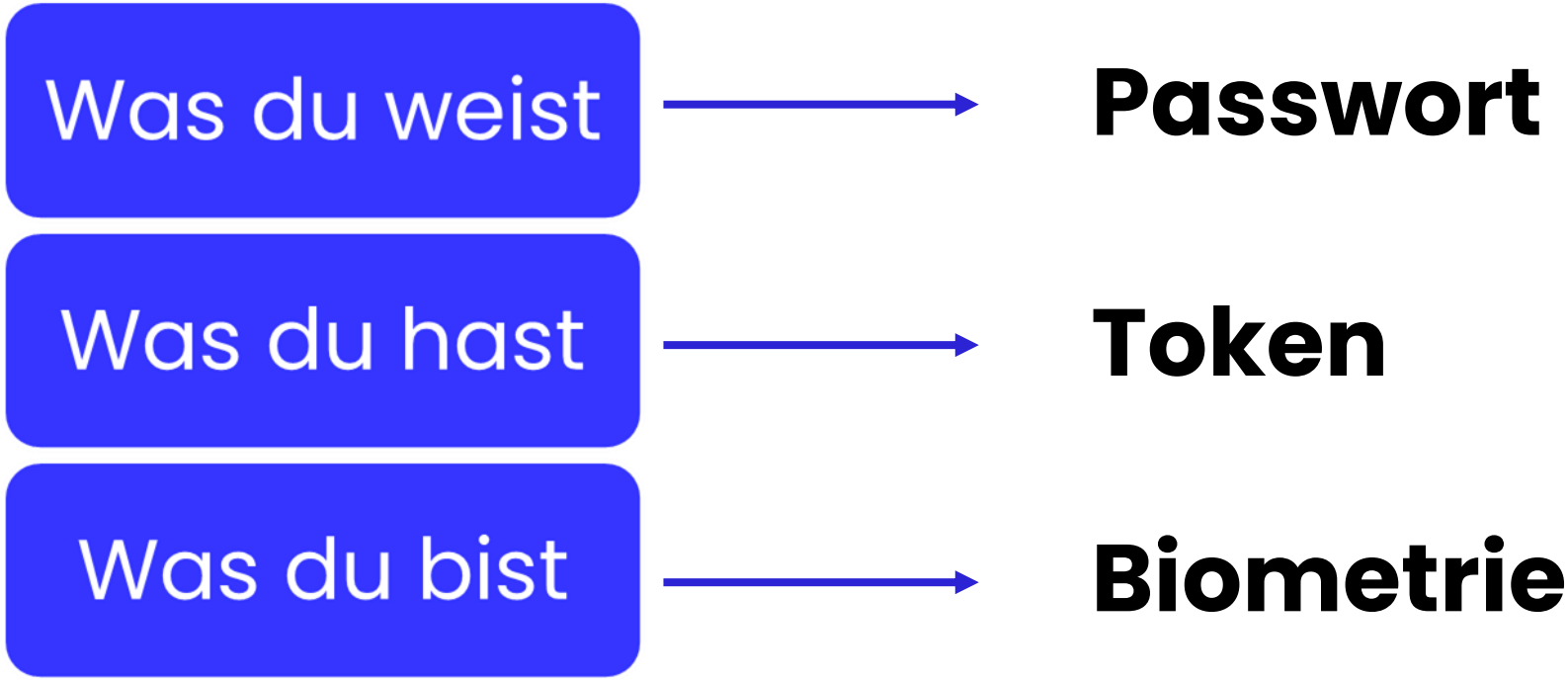
Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Multi Factor Authentication



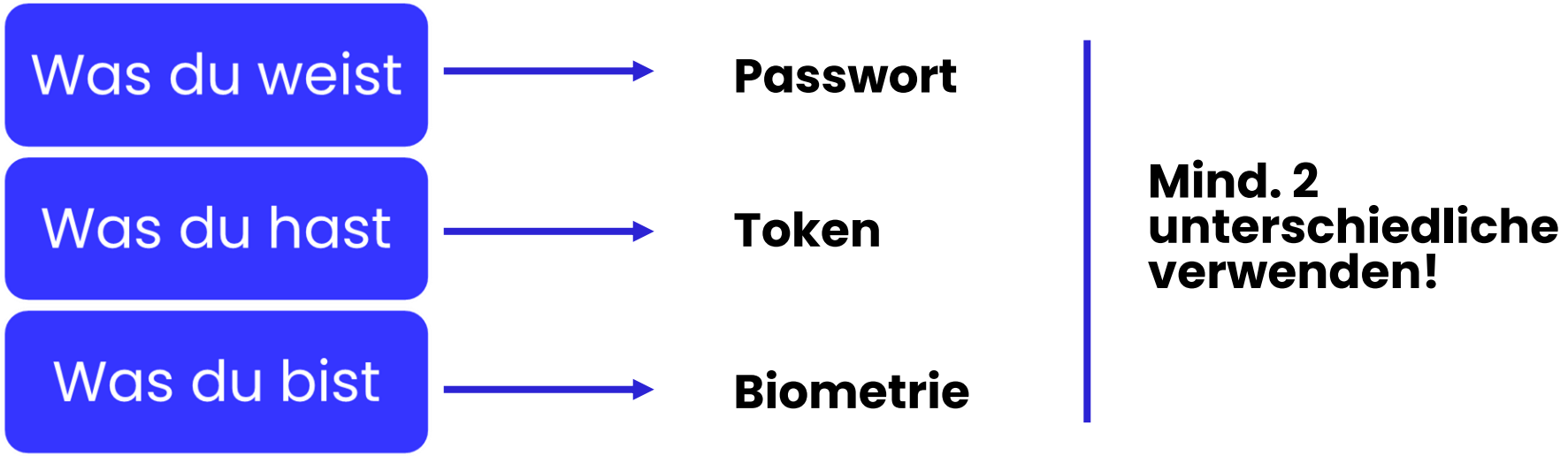
Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Multi Factor Authentication



Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Multi Factor Authentication



Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Jetzt seid Ihr dran! 

Praxisübung - Multi Factor Authentication

Ablauf ⏩

- Anhand der gefundenen dig. Identitäten, aktiviert MFA - wo es möglich ist

Dokumentation 📃

- Liste mit MFA Accounts

Tipps 💡

- Beginnt mit den Social media Accounts
  → Vor allem LinkedIn

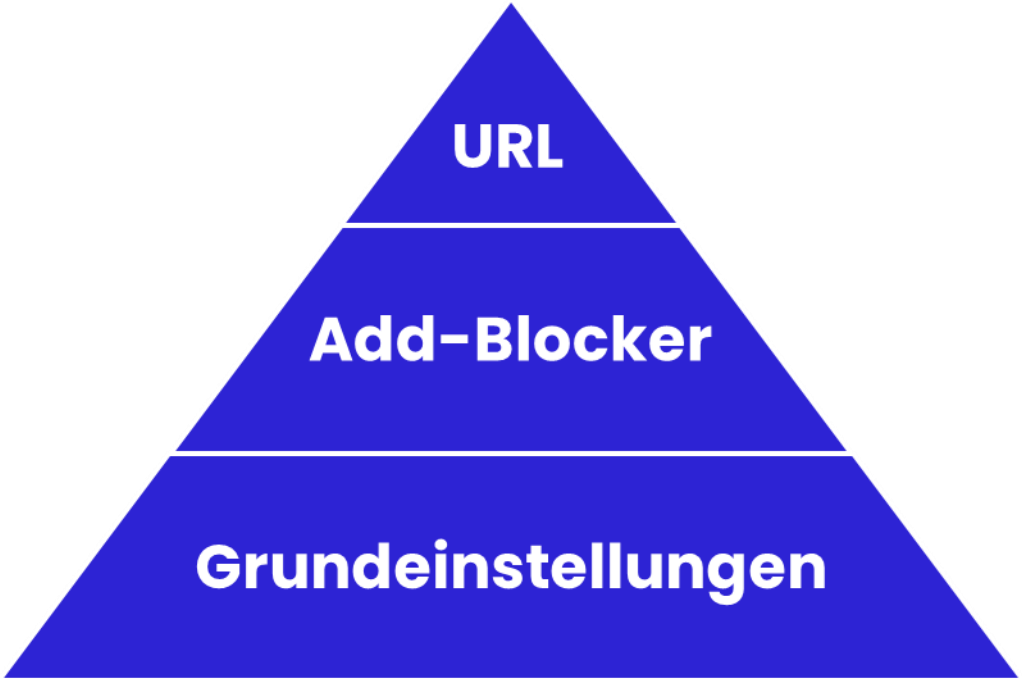
Zeit & Format 🕛

- 20 min Recherche
- 5 min Diskussion

Safe Browsing 🌐

Auf was achtet ihr beim Verwenden des Browsers?

Safe Browsing



Live Demo 

Safe Browsing

Lernziele 🚀

- Was ist eine digitale Identität?
- Warum ist Passwortsicherheit wichtig?
- Wie verwende ich meinen Browser richtig?

Inhalte 📦

Cyberangriffe

Digitale Identitäten

Incident Response

Datenschutz

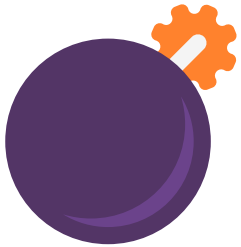
Incident Response  

Das wichtigste im Überblick

Lernziele 🚀

- Was sollte ich machen wenn ich einen Incident **wahrnehme**?
- Welchen **Prozess** gibt es für einen Incident?
- Was benötigt ihr täglich zum **Arbeiten**?

Richtiges Verhalten 



Was würdet ihr jetzt tun?

Was tun bei einem Angriff/Verdacht?

- Öffnen von Links/Anhängen vermeiden
- Ändern von Passwörtern inkl. Account Logout
- Internet-verbindung Trennen

Verhalten

Was tun bei einem Angriff/Verdacht?

Meldung

- Mitarbeiter:innen verständigen
- Nichts weiterleiten an andere
- Stakeholder und ggf. Behörden verständigen

Was tun bei einem Angriff/Verdacht?

Verhalten

- Öffnen von Links/Anhängen vermeiden
- Ändern von Passwörtern inkl. Account Logout
- Internet-verbindung Trennen

Meldung

- Mitarbeiter:innen verständigen
- Nichts weiterleiten an andere
- Stakeholder und ggf. Behörden verständigen

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Security Einstellungen an Systemen prüfen

Falls notwendig Backups einspielen

Datenschutz Meldung falls notwendig

Nacharbeit

Regulärer Prozess eines Incidents 🔁

Incident Response Prozess

Incident

Ruhe bewahren

Meldung an relevante Beteiligte

IT-Manager, GF, Dep., Stakeholder etc.

Logs von Servern, Apps und Devices

Sammeln und filtern von Infos

Hilfe anfordern

SOS

Expert:innen, Stakeholder?

IT-Manager, GF

Entscheidung treffen

Incident lösen & Aufräumen

MA, GF, IT, Stakeholder

Cyber Security Academy

Jetzt seid Ihr dran! 

Praxisübung - Business Continuity

Ablauf ⏩

- Überlegt euch, was ihr täglich zum Arbeiten benötigt. Hardware, Software und sonstige digitalen Assets.

Tipps 💡

- Geht einen normalen Arbeitstag durch und überlegt euch was ihr braucht.

Dokumentation 📃

- Auflistung der Assets
- Klassifizierung nach Kritikalität

Zeit & Format 🕐

- 20 min
- 5 min Diskussion

Lernziele 🚀

- Was sollte ich machen wenn ich einen Incident **wahrnehme**?
- Welchen **Prozess** gibt es für einen Incident?
- Was benötigt ihr täglich zum **Arbeiten**?



Inhalte 📦

Cyberangriffe

Digitale Identitäten

Incident Response

Datenschutz

Zeit für ein Quiz! 

Datenschutz 🔒

ein grober Überblick

Lernziele 🚀

- Was ist Datenschutz?*
- Was sind personenbezogene Daten und Datenverarbeitung?*
- Was versteht man unter den Betroffenenrechten?*

*Laut Datenschutz Grundverordnung der Europäischen Union

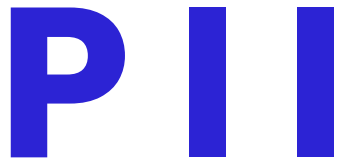
Was versteht ihr unter dem Begriff Datenschutz?

Datenschutz Grundverordnung (DSGVO)

Was ist Datenschutz laut DSGVO ?

Schutz von
personenbezogenen Daten

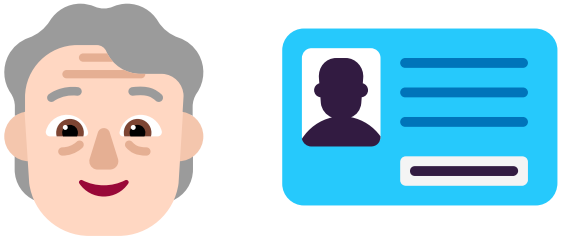
Was sind personenbezogene Daten (PII) ?



Was sind personenbezogene Daten (PII) ?

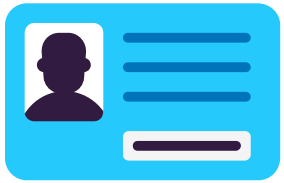
Personally **I**dentifiable **I**nformation

Was sind personenbezogene Daten (PII) ?



alle Informationen, die sich auf identifizierbare Person beziehen

Was sind personenbezogene Daten (PII) ?



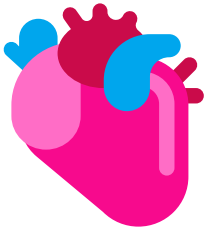
Name

Adresse

Telefonnummer

E-Mail-Adresse

Geburtsdatum



Gesundheitsdaten

Was ist Datenverarbeitung laut DSGVO?

Datenverarbeitung im Sinne der DSGVO bedeutet jegliche Erhebung, Speicherung, Nutzung oder Weitergabe personenbezogener Daten (PII).

Quelle: https://www.wko.at/datenschutz/eu-dsgvo-wichtige-begriffsbestimmungen

Was ist Datenverarbeitung laut DSGVO?

kurz gesagt...

Irgendwas mit PII tun

Gilt die DSGVO auch für mein Unternehmen? 🙈

Gilt die DSGVO auch für mein Unternehmen?

kurz gesagt...

JA!

Gilt die DSGVO auch für mein Unternehmen?

Die DSGVO gilt…

- für **alle** Unternehmen in der **EU**.
- **inhaltlich**, wenn „personenbezogene Daten (**PII**)“ vorliegen und diese „verarbeitet“ werden.

Quelle: https://europa.eu/youreurope/business/dealing-with-customers/data-protection

Was ist das Minimum, das ich tun sollte? 🔽

Was ist das Minimum, das ich tun sollte?

Die Betroffenenrechte einhalten

Jetzt seid Ihr dran! 

Praxisübung - Datenanfrage

Ablauf ⏩

- Stellt eine Auskunftsanfrage über eure persönlichen Daten an das Unternehmen eurer Wahl.

Tipps 💡

- Ihr wollt eine schnelle Antwort? Sendet die Anfrage an Google oÄ., die haben den Prozess automatisiert

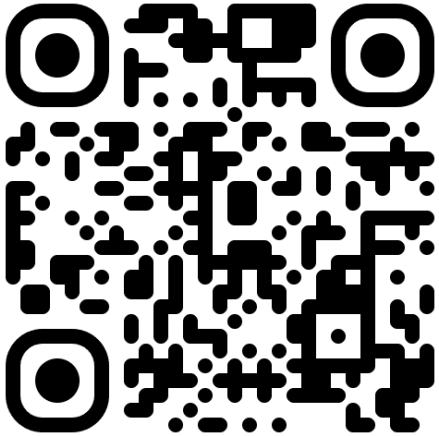
Dokumentation 📃

- Bestägigung von Datenanfragen.de

Zeit & Format 🕐

- 10 min Anfrage stellen

Praxisübung - Datenanfrage



www.datenanfragen.de

Was sind die Betroffenenrechte laut DSGVO?

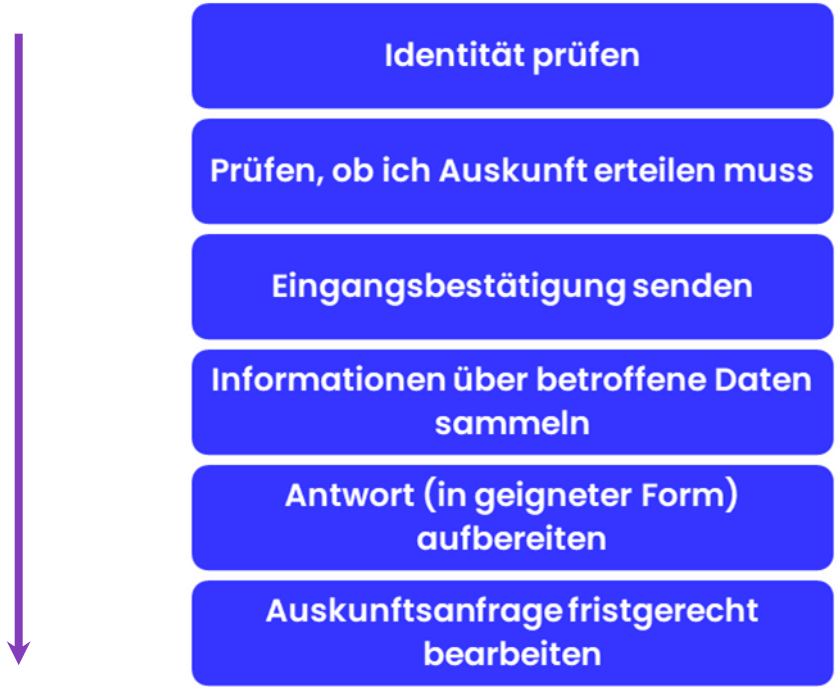
- Recht auf Information
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Einschränkung
- Recht auf Widerspruch
- Recht auf Löschung
- Recht auf Datenübertragbarkeit

Was muss ich als Unternehmen machen?

Auskunftsanfrage fristgerecht beantworten

1 Monat

Auskunftsanfrage – der Prozess



Was ist für euch wichtig?

Anfrage rechtzeitig an zuständige Person weitergeben!

Lernziele 🚀

- Was ist Datenschutz?*
- Was sind personenbezogene Daten und Datenverarbeitung?*
- Was versteht man unter den Betroffenenrechten?*

*Laut Datenschutz Grundverordnung der Europäischen Union

Jetzt seid Ihr dran! 

Praxisübung - Detektivarbeit 🔍

Ablauf ⏩

- Versucht möglichst viel über euch und den eure Firma im Internet herauszufinden
- Überlegt euch wie diese Daten missbraucht werden können

Dokumentation 📄

- Notiert die relevantesten Informationen und zugehörigen Quellen

Zeit & Format 🕐

- 20 min Recherche
- 5 min Diskussion

Was könnte ein Hacker 🦹 jetzt damit Anfangen?

Live Lookup – Lakeside Park

Recap 

mit den Highlights aus dem Kurs

Cyberangriffe 🤺

Cyberangriffe sind allgegenwärtig

Phishing Mails können täuschend echt aussehen, überlegt zwei mal vor dem Öffnen eines links

Achtet darauf, wo ihr eure Daten ablegt

Digitale Identitäten 

Verwendete sichere Passwörter, vor allem bei dem Masterpasswort

Aktiviert MFA, wo es möglich ist

Löscht inaktive Accounts, sowie zugehörige Credentials aus dem Safe

Incident Response 💥♻️

Wenn wirklich ein Incident passiert bewahrt Ruhe, keine unüberlegten Handlungen

Meldet den Vorfall an die zuständige Person

Verwendet dafür einen sicheren Kanal

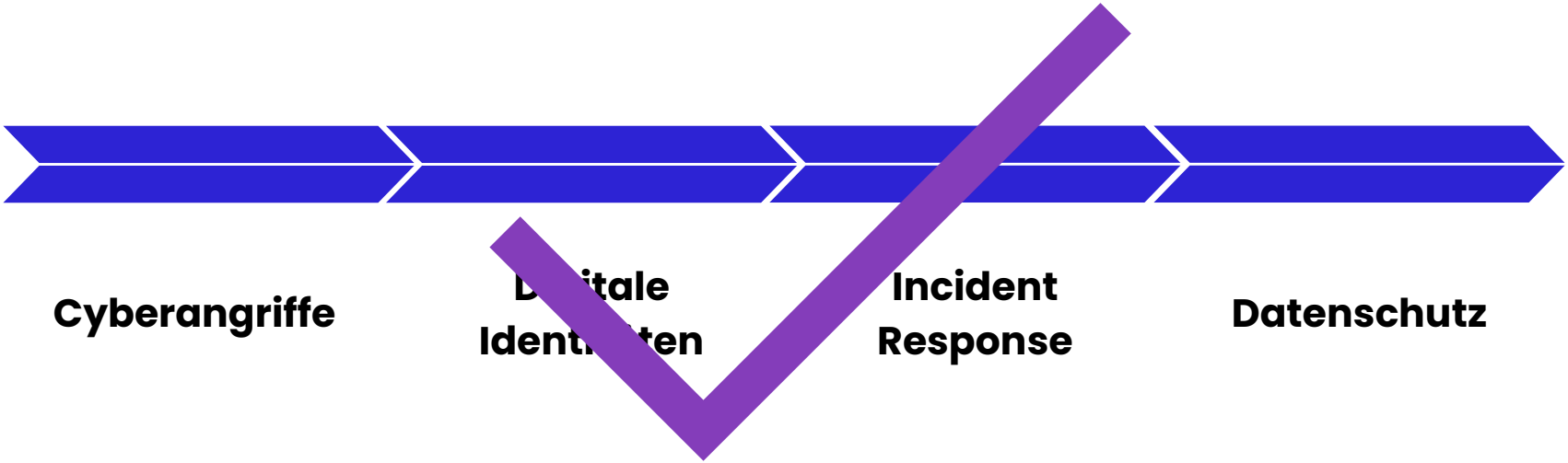
Datenschutz 🔒

Jedes Unternehmen in der EU muss die DSGVO einhalten, bei Verstoß muss man Strafe bezahlen

Minimiert wenn möglich die Erhebung von PII

Achtet auf Auskunftsanfragen, die müssen binnen einem Monat korrekt bearbeitet werden

Inhalte 📦



Habt ihr noch Fragen? 🚀

Zusatzinhalte ➕

Zusatzinformationen und noch wichtige Themen

WIE KANN MAN SICH ALS UNTERNEHMEN VOR SPOOFING SCHÜTZEN?

Cyber Security Academy

SCHUTZ VOR SPOOFING

- SPF

  Sender **P**olicy **F**ramework
- DKIM

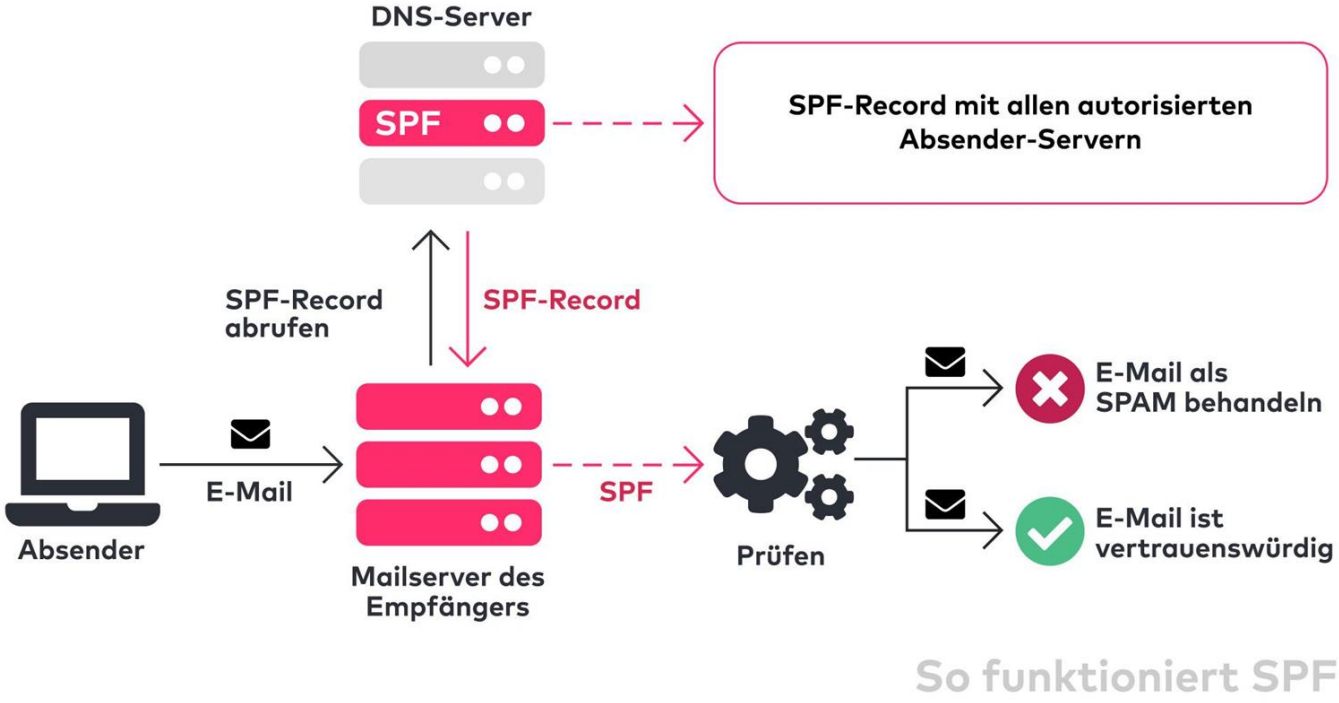
  Domain**K**eys **I**dentified **M**ail
- DMARC

  Domain-based **M**essage **A**uthentication, **R**eporting, and **C**onformance

SPF

- Sender Policy Framework
- Verhindert das Fälschen von Absenderadressen
- Festlegen, aus welchen Bereichen Mails versendet werden
  - IP-Adresse
  - Netzwerkbereiche
- Kann aus Mail-Header ausgelesen werden
- Wird über TXT Eintrag festgelegt

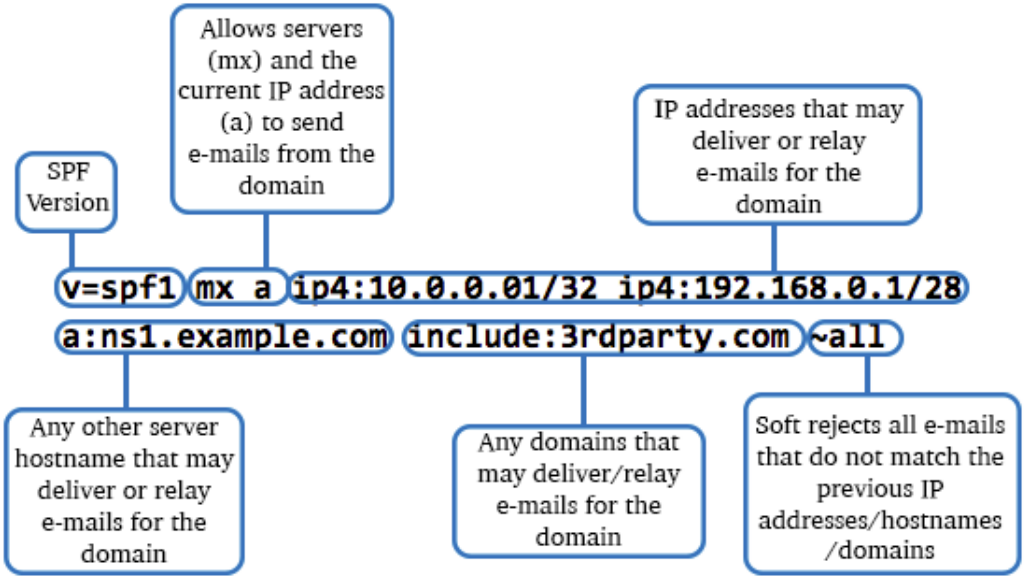
SPF II



Quelle: https://www.spf-record.de/

Cyber Security Academy

SPF III



Quelle: https://www.pair.com/support/kb/what-is-an-spf

Beispiel

```
v=spf1 include:spf.w4ymail.at include:_spf.google.com ~all
```

Cyber Security Academy

SPF IIII

SPF existiert & stimmt mit Absender überein

```
X-Received-SPF: pass ( mx04.ispgateway.de: domain of sender-domain.tld designates Sender-Server-IP as permitted sender )
```

SPF existiert & stimmt nicht mit Absender überein

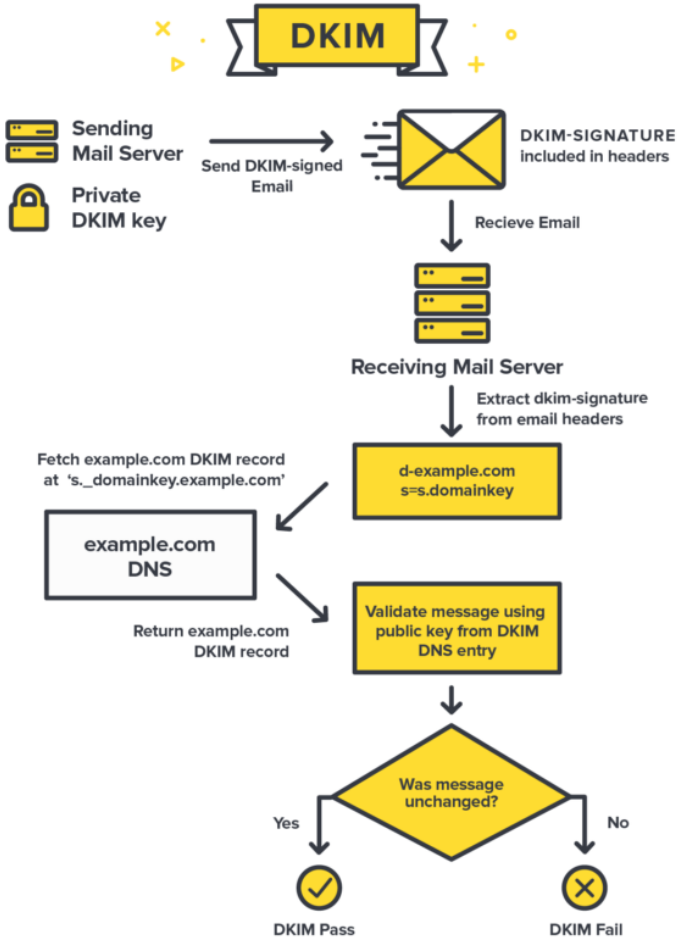
```
X-Received-SPF: fail ( mx02.ispgateway.de: domain of sender-domain.tld does not designate Sender-Server-IP as permitted sender )
```

SPF existiert nicht

```
X-Received-SPF: none ( mx15.ispgateway.de: domain of sender-domain.tld does not provide an SPF record )
```

DKIM

- DomainKeys Identified Mail
- Methode zur E-Mail Authentifizierung
- Verifizierung mittels Public & Private Key
- Kann aus Mail-Header ausgelesen werden
- Wird über TXT Eintrag festgelegt



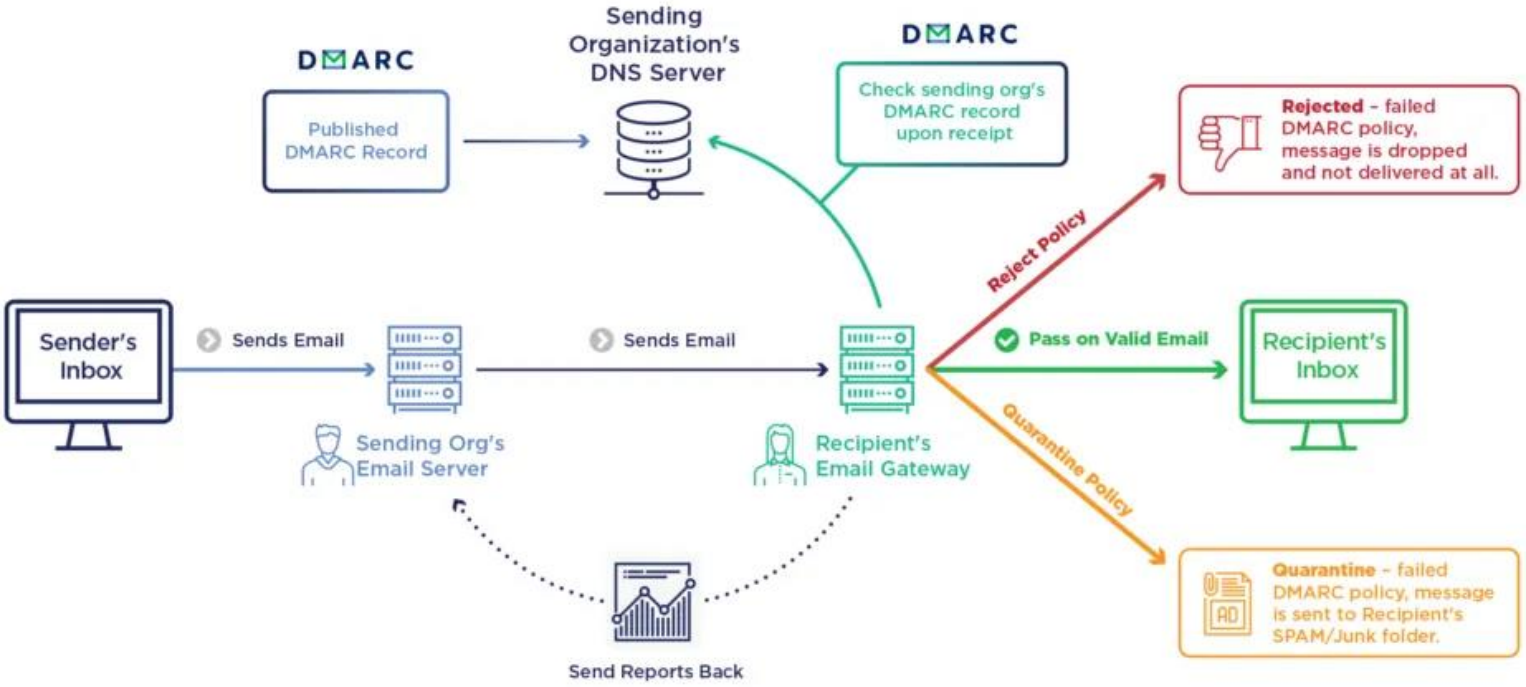
Quelle: https://www.duocircle.com/resources/what-is-dkim

DKIM II

```
v=1; a=rsa-sha256;
        d=example.com;
      bh=uMixy0BsCqhbru4fqPZQdeZY5Pq865sNAnOAxNgUS0s=;
  b=LiIvJeRyqMo0gngiCygwpiKphJjYezb5kXBKCNj8DqRVcCk7obK6OUg4o+EufEbB
tRYQfQhgIkx5m70IqA6dP+DBZUcsJyS9C+vm2xRK7qyHi2hUFpYS5pkeiNVoQk/Wk4w
ZG4tu/g+OA49mS7VX+64FXr79MPwOMRRmJ3lNwJU=
```

v= DKIM Version
a= Algorithmus, der zur Berechnung der digitalen Signatur / Erzeugung des Hashes des E-Mail-Textes verwendet wird
d= Domainname des Absenders.
bh= Hash des E-Mail-Textes
b= Digitale Signatur → aus h und bh erzeugt & mit dem privaten Schlüssel signiert

DMARC



Quelle: https://emailauth.io/what-is-dmarc

DMARC II

```
v=DMARC1; p=none; rua=mailto:dmarc-reports@mydomain.com
```

p=none → Mails werden überwacht, jedoch keine Maßnahmen

p=quarantine → Unautorisierte Mails gehen in den Spam-Ordner

p=reject → Unautorisierte Mails werden nicht zugestellt

SPF / DKIM / DMARC - SCHÜTZEN VOR

- Domain-Spoofing: Fälschen von Unternehmensdomain für legitime E-Mails
- E-Mail-Spoofing: Fälschung von E-Mails
- Business E-Mail Compromise (BEC): Management fordert Geld / Daten
- Impostor E-Mails: Betrüger geben sich als jemand anders aus
- Phishing-E-Mails: Installation von Malware / Zugangsdaten Weitergabe.
- Consumer-Phishing: E-Mails an Kunden → Datendiebstahl
- Partner-Spoofing: Fälschung von Geschäfts-E-Mails zur Zahlungsmanipulation
- Whaling: Fälschung von E-Mails an leitende Mitarbeiter für finanziellen Gewinn

SICHERES SURFEN IM INTERNET

KENNST DU TOOLS, UM WEBSEITEN ZU PRÜFEN?

Cyber Security Academy

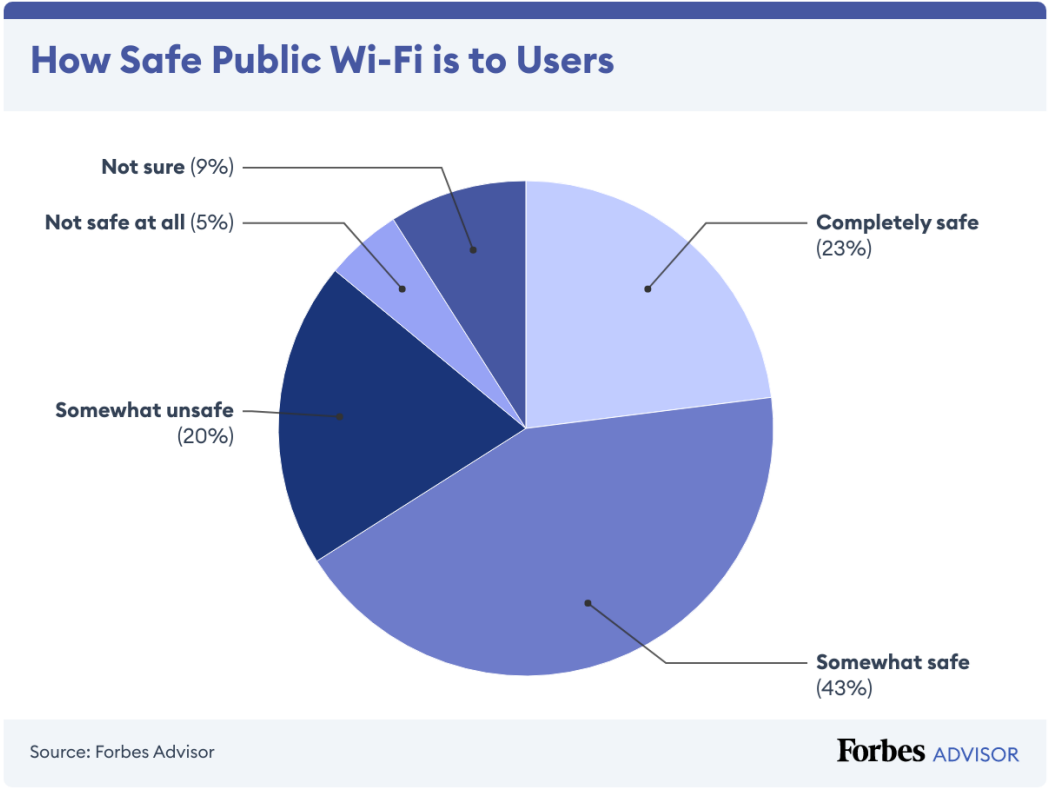
TOOLS

- Google Safe Browsing: https://developers.google.com/safe-browsing
- VirusTotal: https://www.virustotal.com/gui/home/upload
- URLVoid: https://www.urlvoid.com/
- Sucuri SiteCheck: https://sitecheck.sucuri.net/
- Mozilla Observatory: https://observatory.mozilla.org/
- Qualys SSL Labs: https://www.ssllabs.com/ssltest/
- OpenDNS PhishTank: https://www.phishtank.com/
- Clickjacker: https://clickjacker.io/

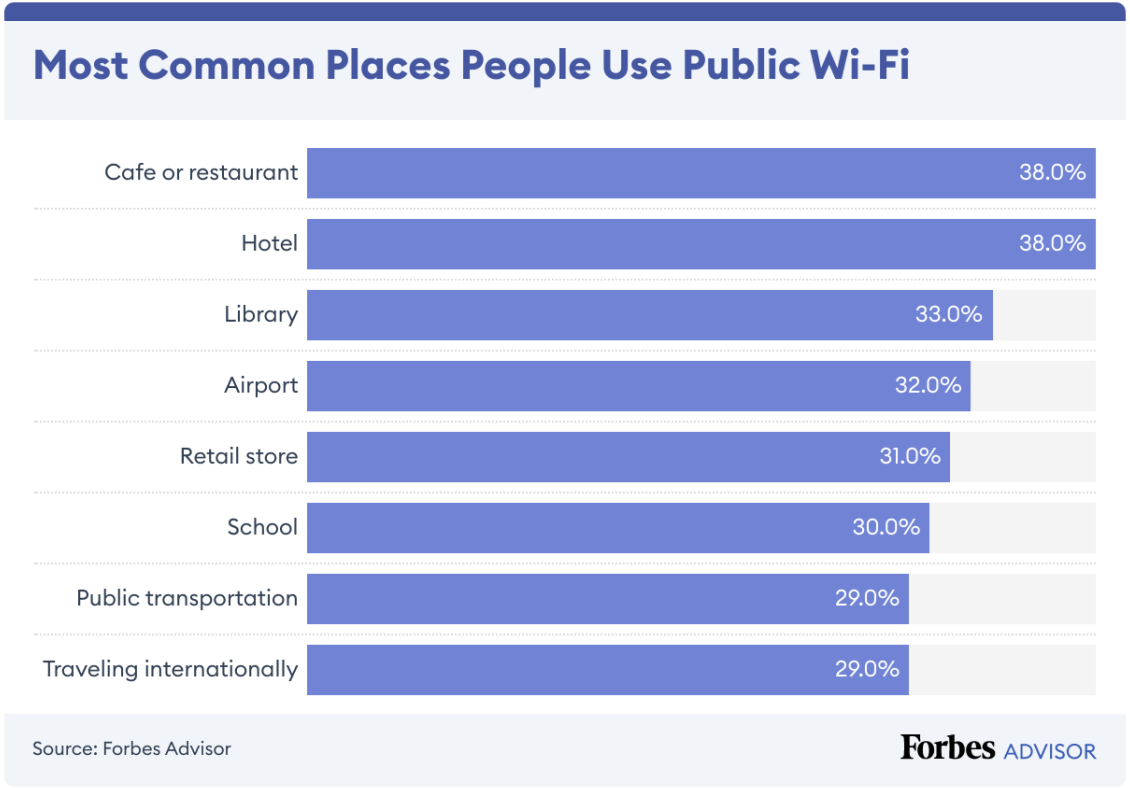
ÖFFENTLICHE NETZWERKE

WIE SICHER SIND ÖFFENTLICHE NETZWERKE?

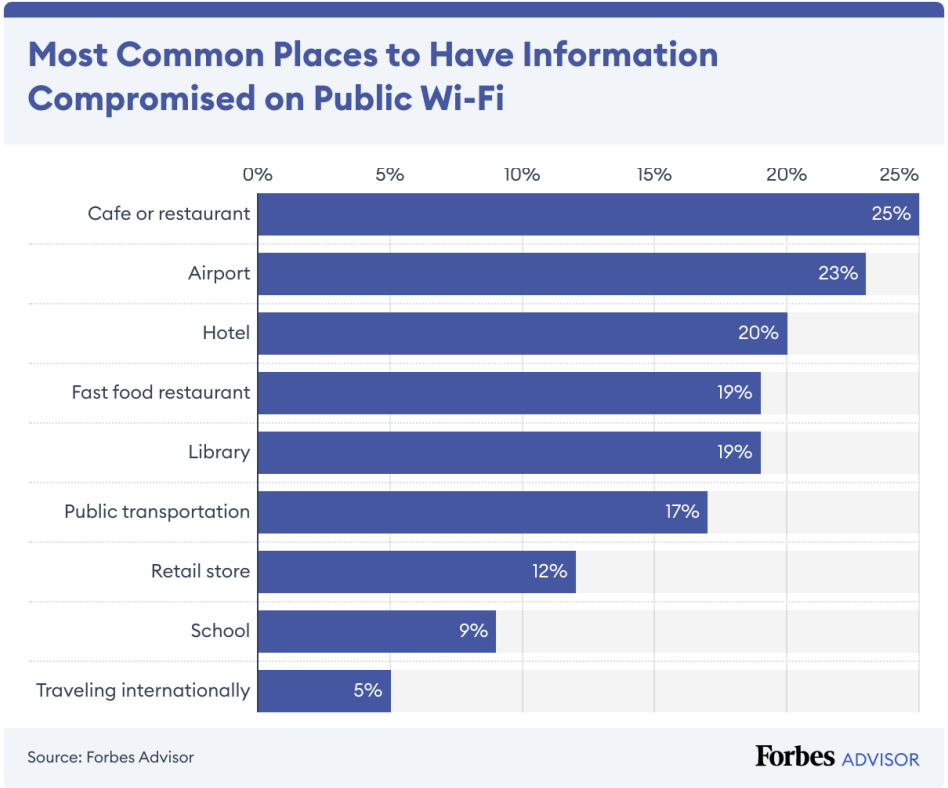
ÖFFENTLICHE NETZWERKE



ÖFFENTLICHE NETZWERKE II



ÖFFENTLICHE NETZWERKE III



ÖFFENTLICHE NETZWERKE IIII

- Cyberstalking
  - Kriminelle überwachen Aktivitäten
  - Browsing Verhalten / Browserverlauf
- Identitätsdiebstahl
  - Sammeln von Anmeldedaten & Passwörter
  - Finanzdaten
- Malware über Router ausspielen
  - DNS resolution auf Fake Seiten
  - Captive Portal mit Schadeware

ÖFFENTLICHE NETZWERKE IIIII

- Automatisches verbinden mit öffentlichem WLAN deaktivieren
- Persönlichen Hotspot verwenden
- Wenn du verbunden bist:
  - Applikationen im Hintergrund beenden
    - z.B. Cloud Syncs, etc
    - Daten werden nicht übertragen und können auch nicht weitergegeben werden
  - Keine persönlichen Daten weitergeben
    - Login bei Banken / Gesundheits Datenbanken / Anmeldungen / ...
  - VPN Benutzen
    - Deine Verbindung wird verschlüsselt
    - z.B. NordVPN

SICHERER UMGANG MIT DATEIEN

AUF WAS ACHTEST DU IN BEZUG AUF DEINE DATEN?

Cyber Security Academy

ARBEITSGERÄTE / BÜRO

- Authentifizierung bei PC / Laptop / Tablets / Telefon / ...
  - Immer sperren, wenn Platz verlassen wird
  - Autolock aktivieren (1 - 3 Minuten)
  - Unbefugter Zugriff kann zu Datenleak führen
- WLAN
  - Sicheres Passwort & WPA3 Verschlüsselung
  - WLAN der MitarbeiterInnen nicht an Kunden weitergeben
  - Potenzieller Zugriff auf NAS / Interne im Netzwerk erreichbare Dokumente
- Positionierung von Monitoren & Informationen
  - Einsehen von Daten / Passwörtern durch Glastüren

DEMO: DATEN LEAK BROWSER COOKIES

FIREWALL & ANTIVIRUS

- Daten am PC / Laptop verschlüsselt speichern
  - Mac - FileVault
  - Microsoft BitLocker
  - Linux - VeraCrypt
- Firewall aktivieren & konfigurieren
- Antivirus
  - Microsoft Defender
  - Avast Antivirus

DATENSICHERHEIT

- Sensible Daten
  - Share über Passwortmanager
  - OneTime Sends
    - https://dead-drop.me/
    - Achtung: Selfhosted Tools am besten (https://github.com/FlowMo7/dead-drop)
- Cloud Links
  - Dokumente & Dateien
  - Zugriff auf User einschränken
  - Keine öffentlichen Links
- Interne Daten
  - Über VPN zugänglich machen

DATENSICHERHEIT II

- Regelmäßige Schulungen / Awareness schaffen
- Regelmäßige Backups erstellen
  - Auf anderen Systemen
  - Nicht öffentlich zugänglich aufbewahren
  - Verschlüsseln

BEISPIEL: SCREEN LOCK

GRUNDLAGEN DER NETZWERKSICHERHEIT

KONFIGURATION

- Standard Anmeldedaten ändern
  - Router
  - admin / admin1234
- WiFi Protection → mindestens WPA2
- Sicheres Passwort wählen
  - Siehe Passwortsicherheit
  - Vermeiden, dass Nachbarn / Externe das PW erraten können
- Achtung bei externen Geräten
  - Staubsaugerroboter, Backrohr
  - Haben coole Integration, und können von extern bedient werden
  - Hersteller schauen sich aber auch oft an, was im Netzwerk passiert & berichten nach Hause
  - Eigenes Subnetz / VLAN / Gastzugang → Entkapseln vom eigentlichen Traffic

KONFIGURATION II

- Falls Standard Router mit wenig Funktionen
  - Standard Router im Bridge Modus verwenden
  - Router mit mehr Möglichkeiten installieren → z.B. UniFi Dream Router
- Eigener NAS (Network Attached Storage)
  - Im besten Fall nicht nach von außerhalb zugänglich
  - Backup aller wichtigen Daten und Konfigurationen
  - Wenn öffentliche Dienste
    - Nur Protokolle, die auch benötigt werden
    - So wenig wie möglich freigeben

KONFIGURATION III

- Firmware und Betriebssysteme aktuell halten
- Router Firewall
  - Aktivieren und Sicherheitseinstellungen erweitern
  - Traffic prüfen
    - Welche Protokolle werden verwendet?
    - Was passiert z.B. wenn ich nicht zu Hause bin?
- Regelmäßig prüfen, welche Geräte in meinem Netzwerk sind

Feedback