GUARDING YOUR GATEWAYS: A USER'S GUIDE TO BASIC CYBERSECURITY

Workshop #1

JML Coding School GmbH

FAKTEN

- Kurszeiten:
  - Donnerstag 07.03.2024
    08:00 - 12:00
  - Freitag 08.03.2024
    08:00 - 12:00

- Location: Lakeside Science & Technology Park

- Follow-Up Workshops':
  Advanced & Expert Themen - https://www.dih-sued.at/

WER BIN ICH

- Lukas Stattmann
- Ausbildung
  - HTL Villach Schwerpunkt: Netzwerk- und Medientechnik
  - BSc Business Informatics
  - MSc Software Engineering
- Laufbahn
  - Fullstack Developer - Gentics Software (APA IT)
    Focus: Frontend & Backend Development
  - Tech Projektmanagement - Web&Söhne GmbH
    Focus: Architekturkonzepe / OPS / Security & PM
  - Managing Director - Coding School Wörthersee
    Workshops im Bereich Web / PM / AI / Security / uvm.

WER SEID IHR

- Hintergrund
  - Job / Aufgabenbereiche
  - Erfahrungen im Bereich der IT-Security?

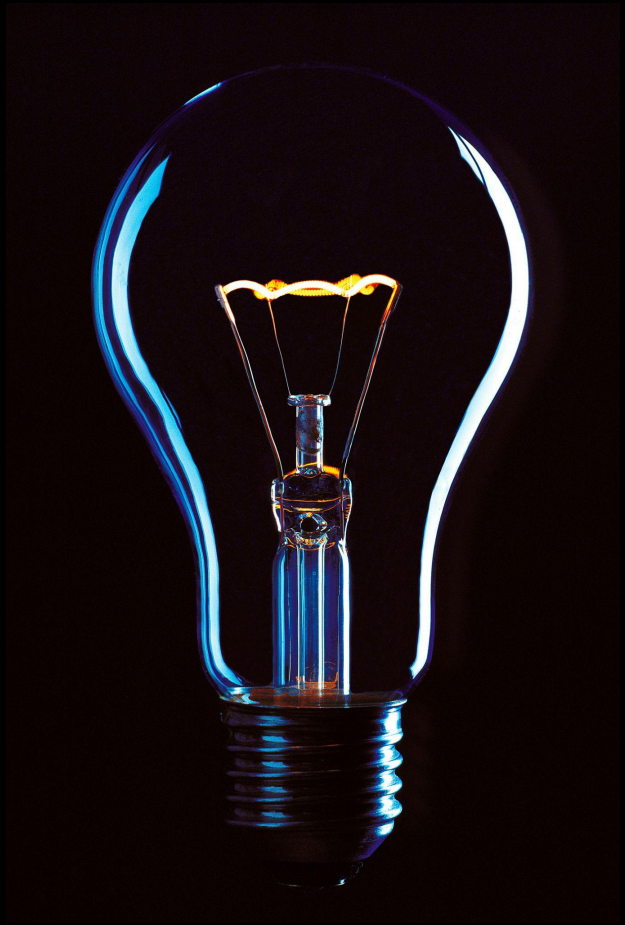
    (Privat als auch Unternehmen)
  - Erfahrungen im Software-Engineering Bereich?
- Vorstellungen & Erwartungen
- Nach diesem Workshop will ich in der Lage sein, ...

INHALT

- Phishing-Prävention
- Sicheres Surfen im Internet
- Sicherer Umgang mit Dateien
- Passwortsicherheit
- Grundlagen der Netzwerksicherheit

CYBERSECURITY

WAS VERSTEHST DU UNTER CYBER SECURITY?

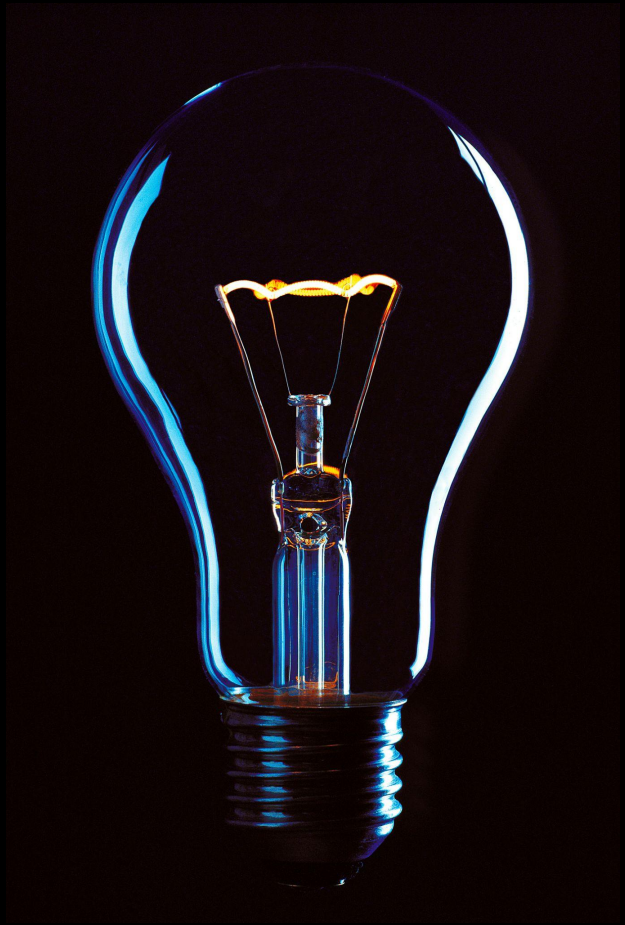


PHISHING PRÄVENTION

GRUNDBEGRIFFE

- Phishing
  - Identität einer bekannten Plattform
  - DHL / Banken / ...
- Spoofing
  - Identität einer konkreten Person
  - Vorgetäuschte E-Mail einer bekannten Person
- Social Engineering
  - Psychologie und soziale Interaktion
  - Telefonanrufe

SUCHE IN DEINEM E-MAIL POSTFACH NACH VORHANDENEN PHISHING & SPOOFING MAILS

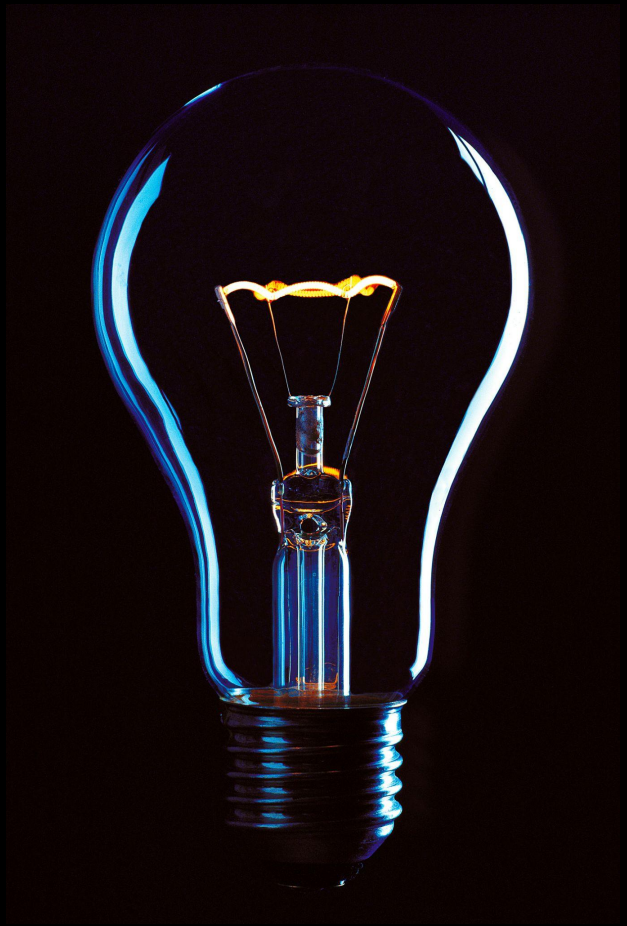


BEISPIEL: KURSINFO

MAILS ERKENNEN & ANALYSIEREN

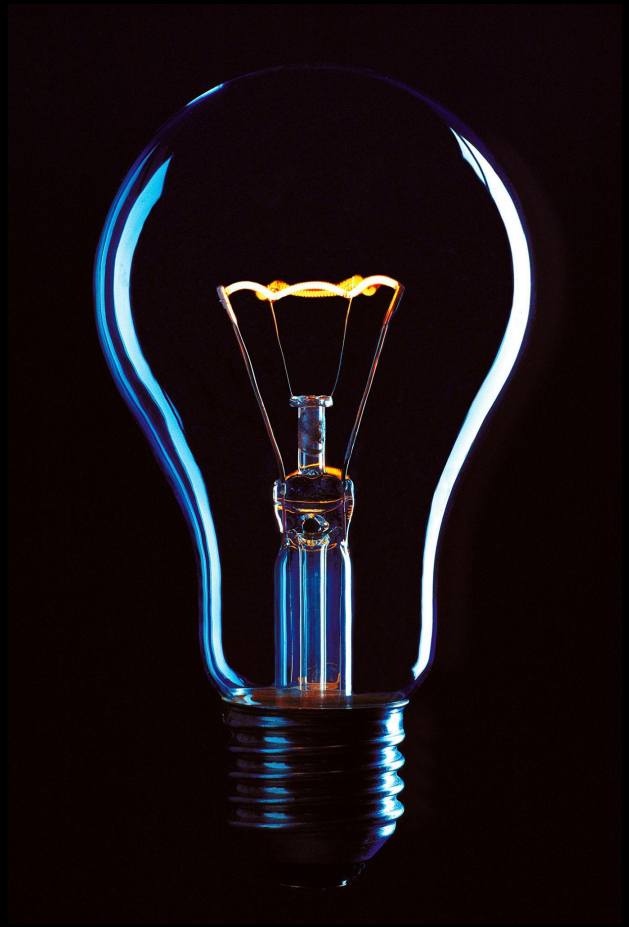
- Absenderadresse prüfen
- Grammatik und Rechtschreibung
- Verdächtige Links
- Dringende Handlungsaufrufe
- Aufforderung zur Weitergabe sensibler Informationen
- Designs / Logos
- Dokumente im Anhang

WIE EINFACH IST SPOOFING?



BEISPIEL: SPOOFING

WIE KANN MAN SICH ALS UNTERNEHMEN VOR SPOOFING SCHÜTZEN?



SCHUTZ VOR SPOOFING

- SPF

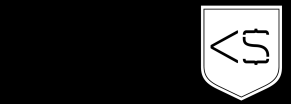
  Sender **P**olicy **F**ramework
- DKIM

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

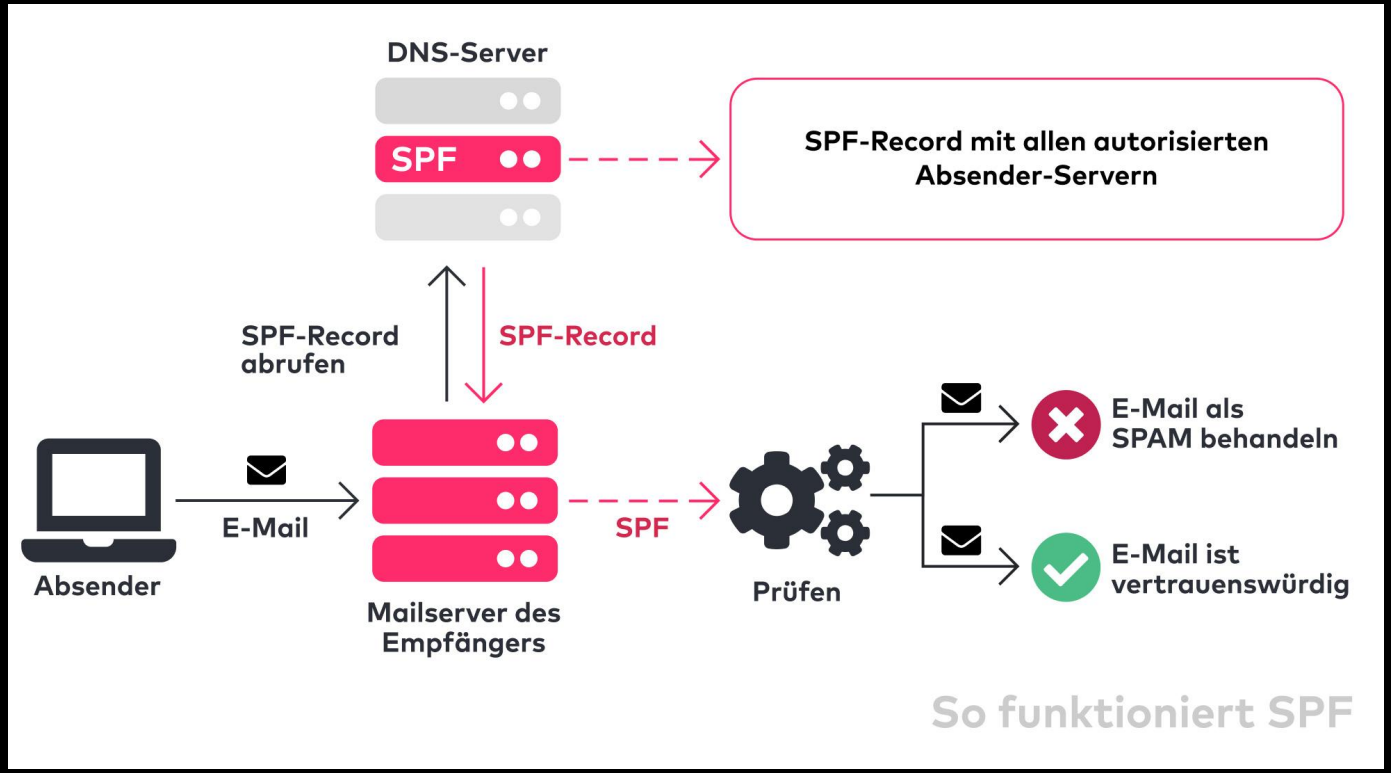
  Domain-based **M**essage **A**uthentication, **R**eporting, and **C**onformance

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

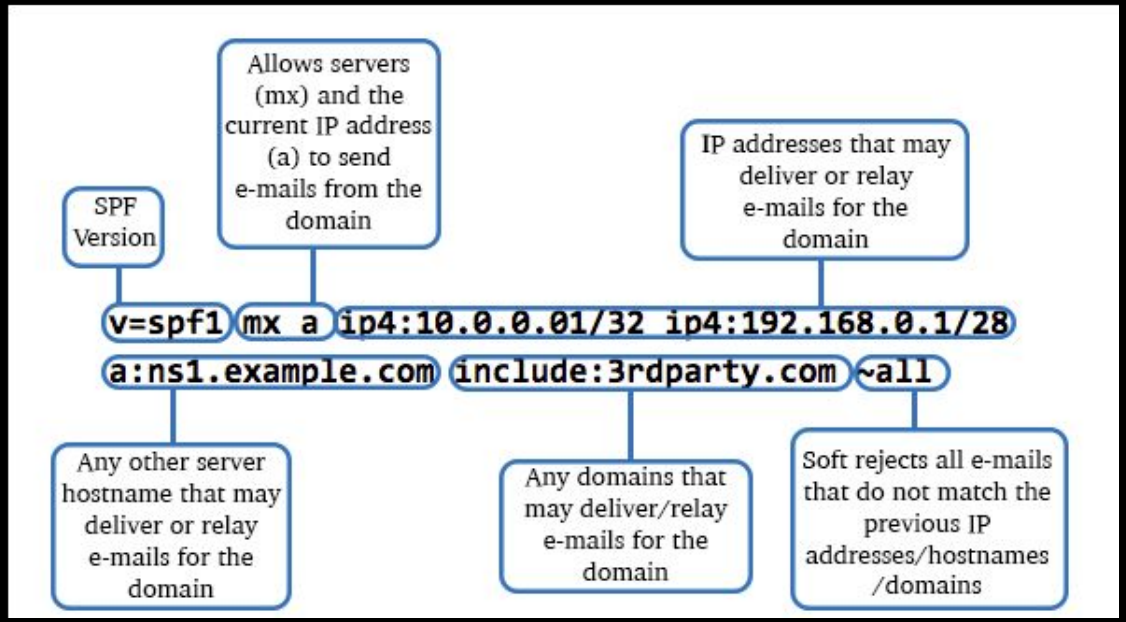


SPF II



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

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
```

SPF IIII

SPF existiert & stimmt mit Absender überein

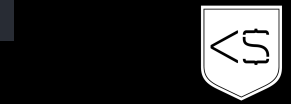
```
X-Received-SPF: pass ( mx04.ispgateway.de: domain of sender-domain.tld designates Sender-Server-IP as permitted sender )
```

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 )
```

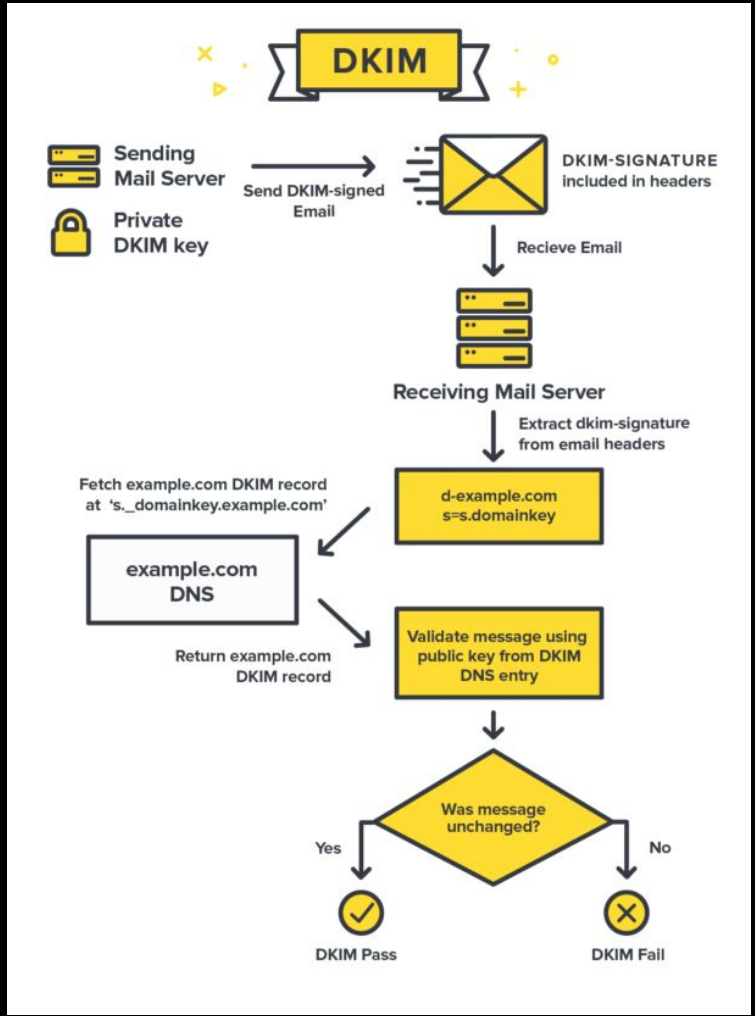
SPF existiert nicht

```
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

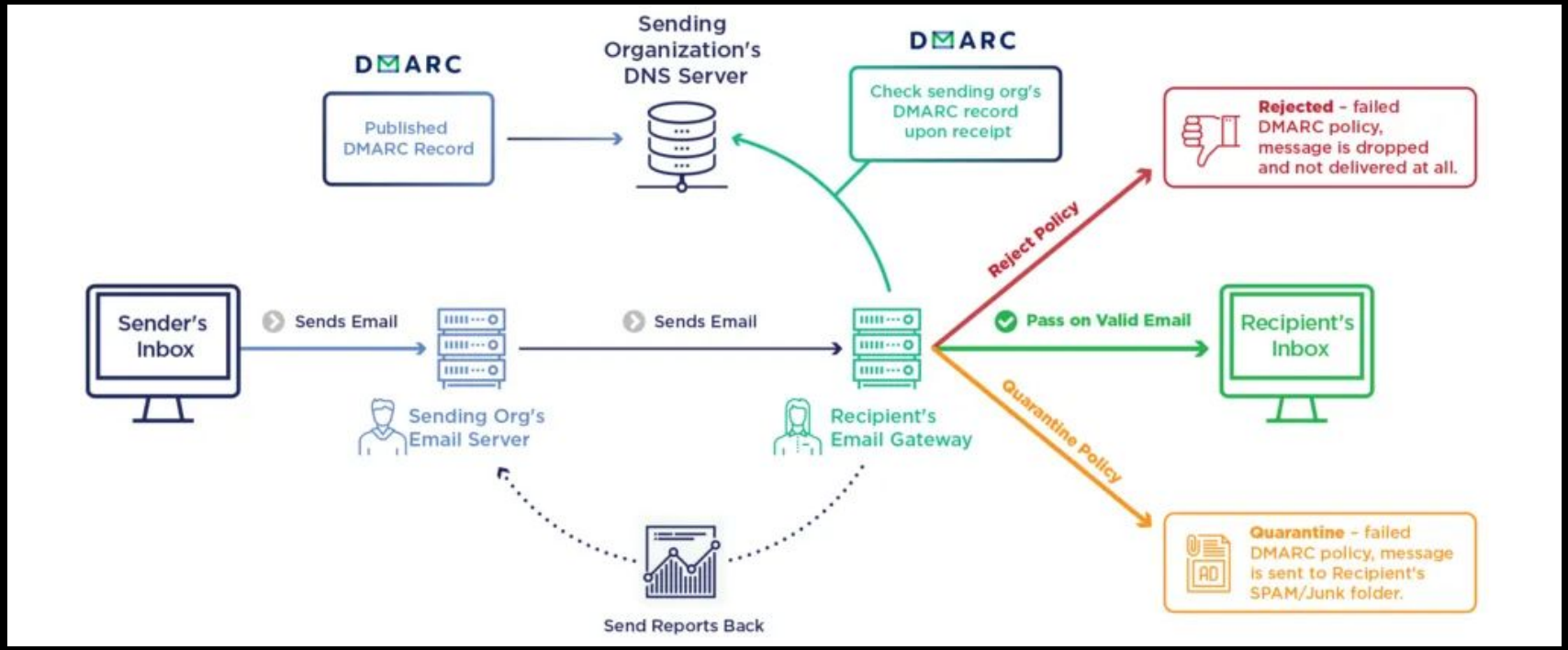
a= Algorithmus, der zur Berechnung der digitalen Signatur / Erzeugung des Hashes des E-Mail-Textes verwendet wird

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

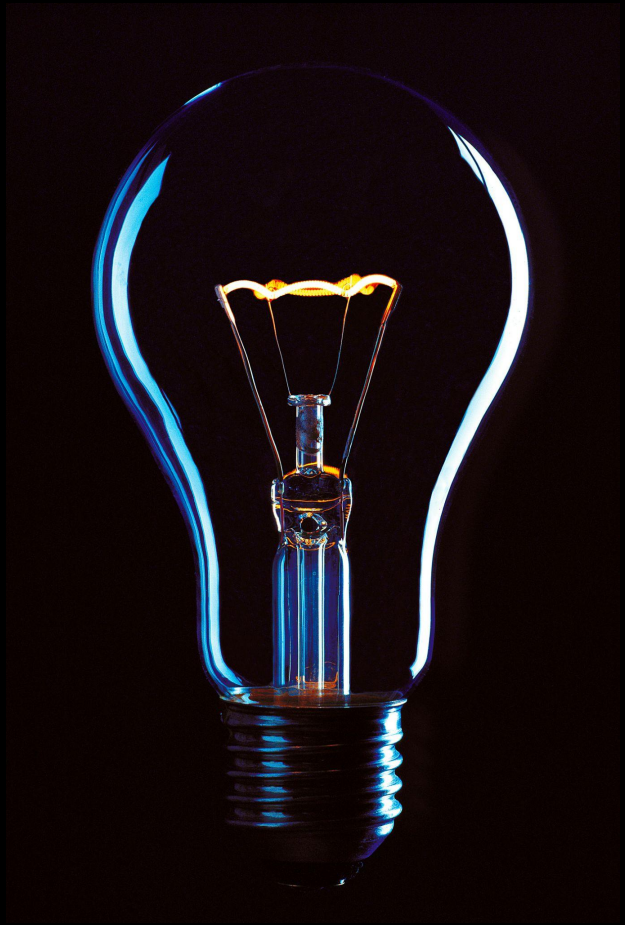
- Domain-Spoofing: Fälschen von Unternehmensdomain für legitime E-Mails
- E-Mail-Spoofing: Fälschung von E-Mails
- Business E-Mail Compromise (BEC): Management fordert Geld / Daten
- Impostor E-Mails: Betrüger geben sich als jemand anders aus
- Phishing-E-Mails: Installation von Malware / Zugangsdaten 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

ACTIONS BEI VERDACHT / ANGRIFF

- Öffnen von Links / Anhängen vermeiden
- Ändern von Passwörtern
- Melden von verdächtigen E-Mails
  - An Admin / Zuständige Person oder Abteilung kommunizieren
  - Andere MitarbeiterInnen warnen
  - **Mail nicht weiterleiten!**
- Malware Scan & verdächtige Daten löschen
- Falls notwendig Backup einspielen
- Sicherheitseinstellungen prüfen / beobachten

SICHERES SURFEN IM INTERNET

AUF WAS ACHTEST DU AKTUELL BEIM SURFEN?



SAFE BROWSING

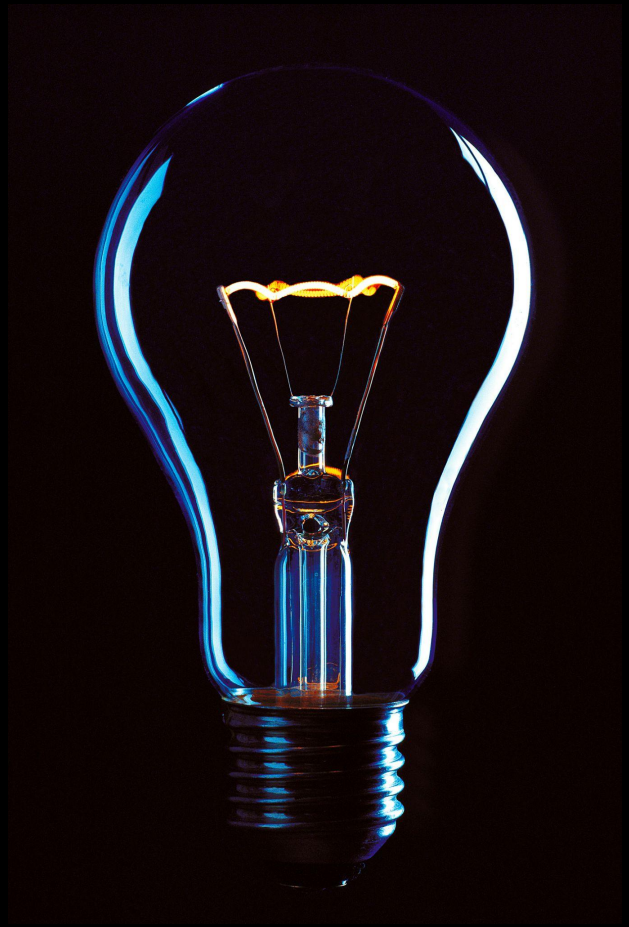
- Grundeinstellungen → Chrome / Firefox / Safari
- Anonymes Surfen
  - Ad-Blocker
  - Cookie Blocker
- Angabe von persönlichen Daten
  - URL Checken
  - Verschlüsselte Übertragung
  - Nur notwendige Daten angeben (Fotos / Dokumente / etc.)
- Scam Seiten & Pop-ups
  - Eigenartige Meldungen
  - Senden von Fehlerberichten
- Unterschiedliche Passwörter verwenden

SAFE BROWSING II

- Regelmäßige Logout durchführen
  - Immer Abmelden z.B. bei Online Bankings
- Herunterladen von Dokumenten
  - Dokumente & Endungen prüfen
  - Ungewollt geladene Dateien löschen und nicht öffnen
- Onlinekäufe
  - Onlineshop & URL auf Echtheit prüfen
  - Nur notwendige Daten weitergeben → z.B. Willhaben Chat: Telefonnummer
  - Zahlungsanbieter mit Käuferschutz verwenden → PayPal, PayLivery, ...

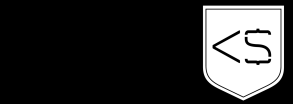
LIVE DEMO:
BROWSER / GOOGLE LOGIN / AD-BLOCKER

KENNST DU TOOLS, UM WEBSEITEN ZU PRÜFEN?



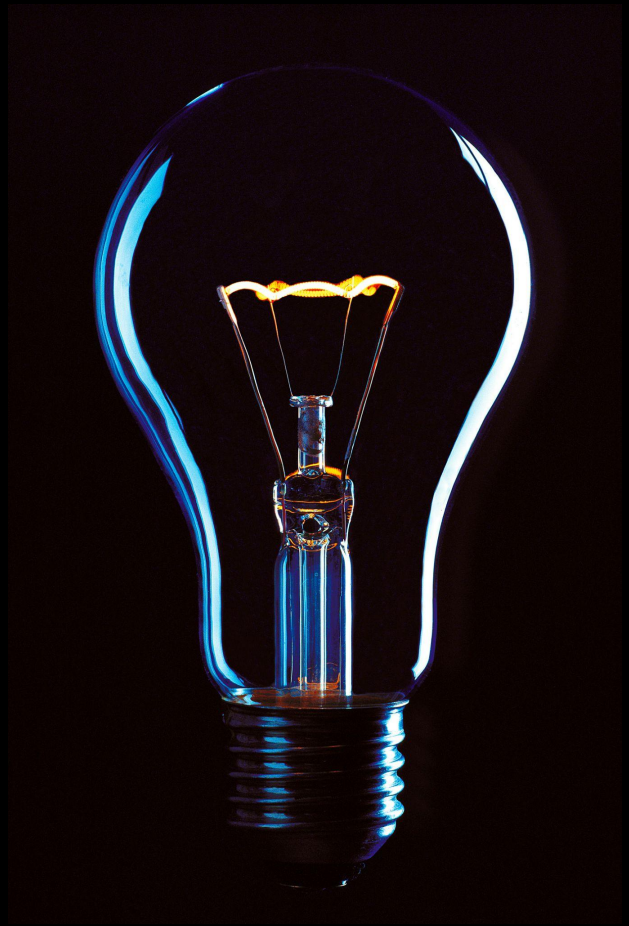
TOOLS

- 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/

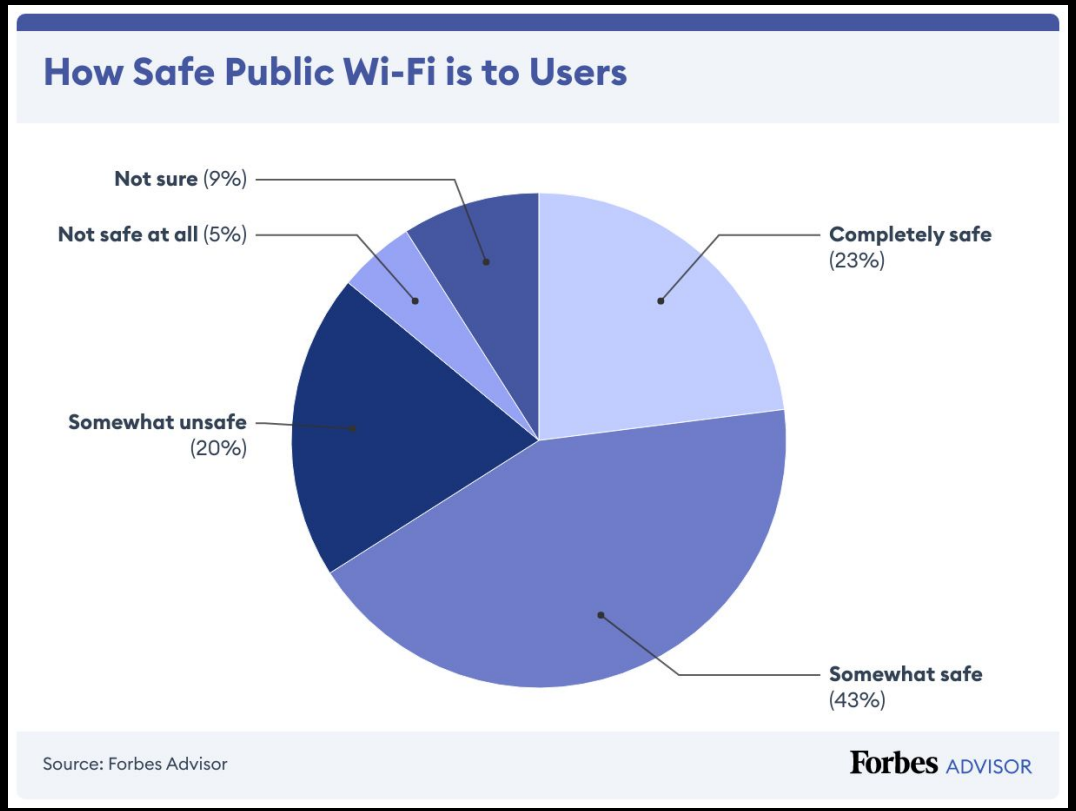


ÖFFENTLICHE NETZWERKE

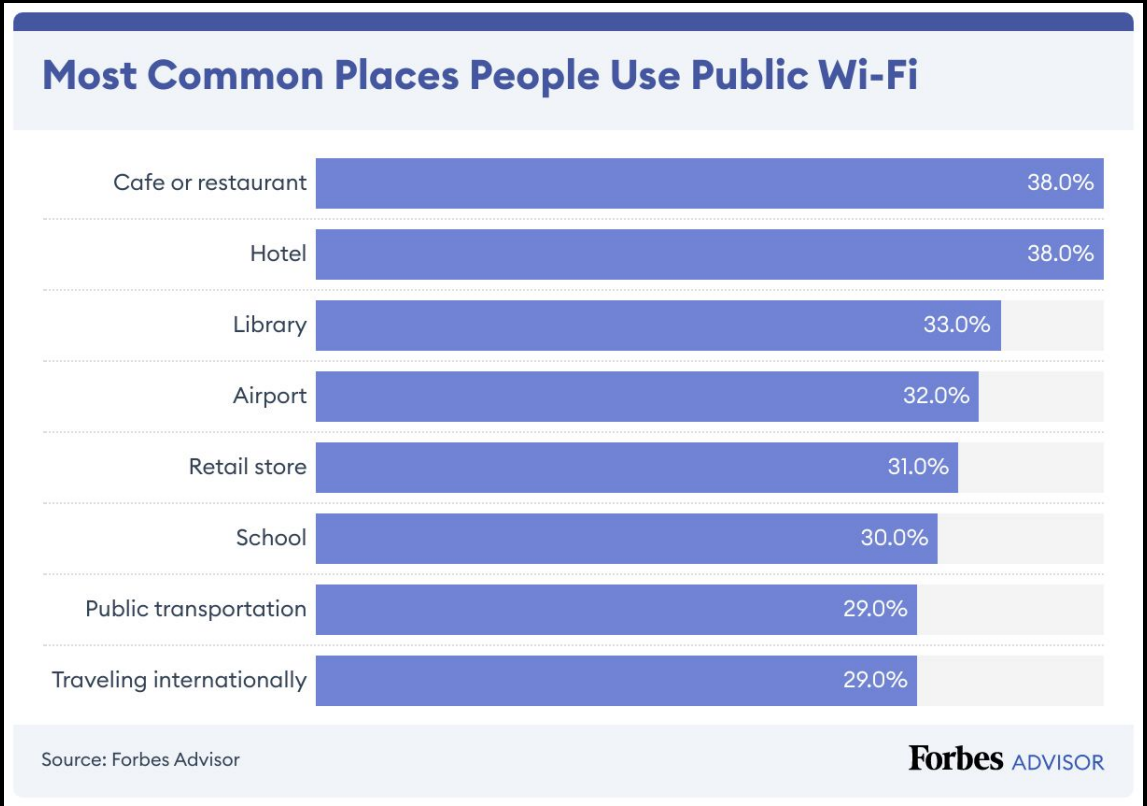
WIE SICHER SIND ÖFFENTLICHE NETZWERKE?



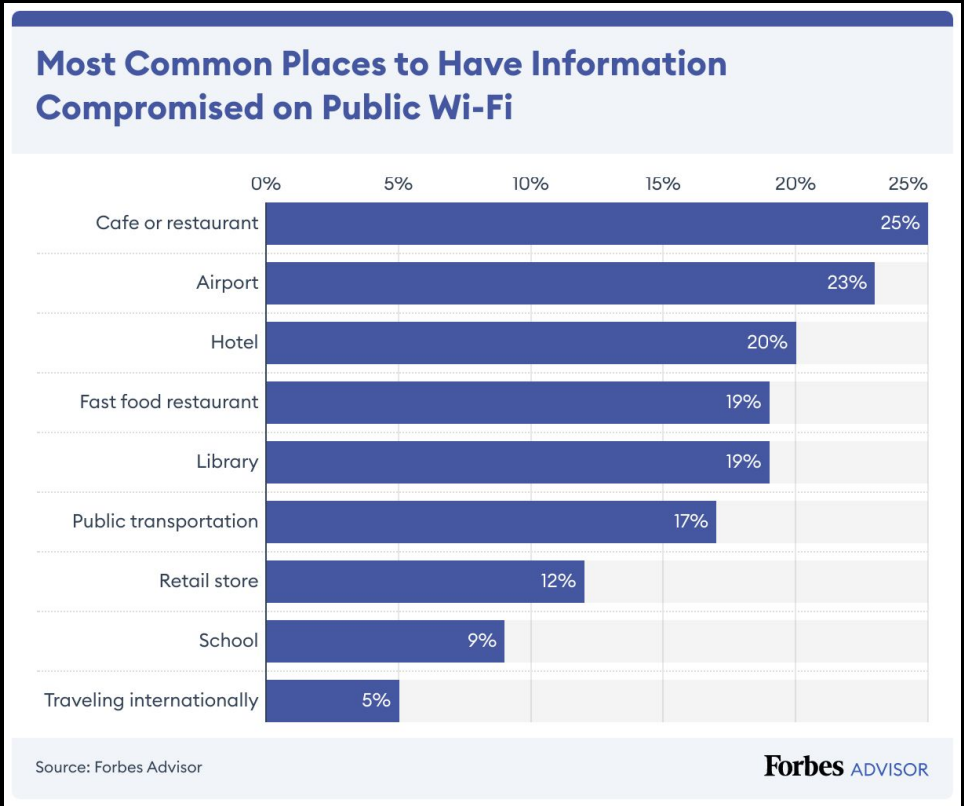
ÖFFENTLICHE NETZWERKE



ÖFFENTLICHE NETZWERKE II



ÖFFENTLICHE NETZWERKE III



ÖFFENTLICHE NETZWERKE IIII

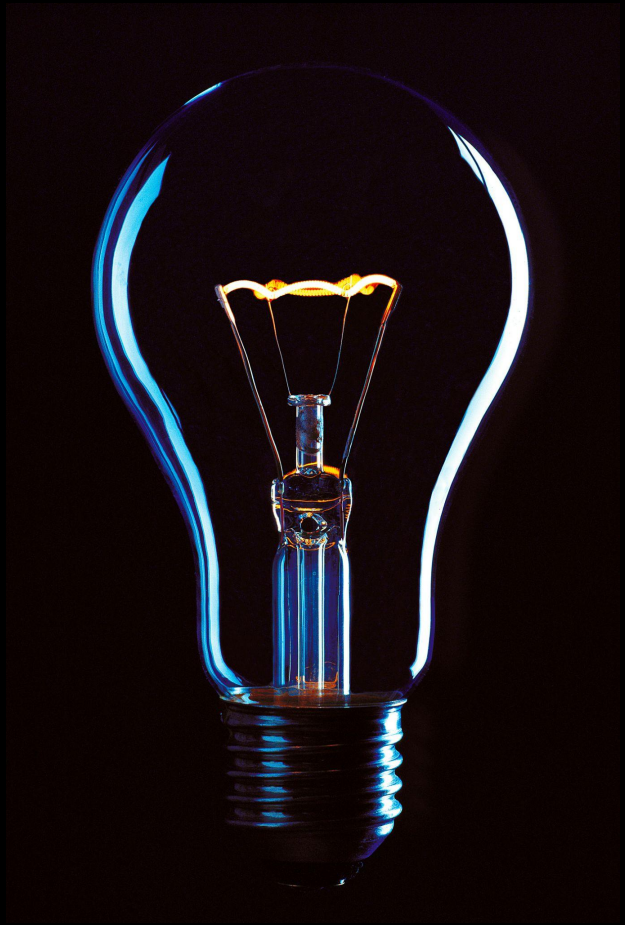
- Cyberstalking
  - Kriminelle überwachen Aktivitäten
  - Browsing Verhalten / Browserverlauf
- Identitätsdiebstahl
  - Sammeln von Anmeldedaten & Passwörter
  - Finanzdaten
- Malware über Router ausspielen
  - DNS routing auf Fake Seiten - automatische Downloads von Dateien bei Aufruf
  - Bei gelungener Infektion → Zugriff auf Daten nicht nur im öffentlichen Netzwerk

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?



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

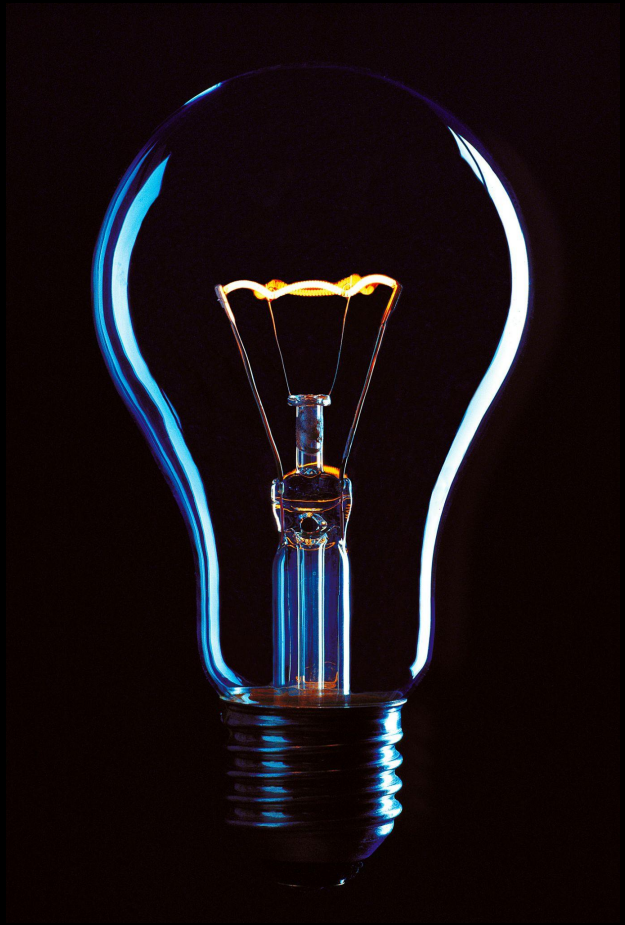
ACTIONS BEI VERDACHT / ANGRIFF

- Öffnen von Links / Anhängen vermeiden
- Ändern von Passwörtern
- Melden von verdächtigen Daten
  - An Admin / Zuständige Person oder Abteilung kommunizieren
  - Andere MitarbeiterInnen warnen
  - **Daten nicht weiterleiten!**
- Malware Scan & verdächtige Daten löschen
- Falls notwendig Backup einspielen
- Sicherheitseinstellungen prüfen / beobachten

BEISPIEL: SCREEN LOCK

PASSWORT SICHERHEIT / MULTI-FACTOR AUTHENTICATION (MFA)

WAS ZEICHNET EIN GUTES PASSWORT AUS?



PASSWORT SAFETY

- Keine persönlichen Informationen
  - Namen, Geburtstag, Benutzername, E-Mail-Adresse
  - Öffentlich verfügbar = Erraten des Passworts leichter
- Je länger, desto besser
  - Mindestens 12 Zeichen
  - zusätzliche Sicherheit mehr > 12
- Zahlen, Symbole & Groß- und Kleinbuchstaben
- Nicht ein Passwort für mehrere Accounts
- Wörter aus Wörterbuch meiden
- Passwortgenerator verwenden, z. B.: https://www.passwort-generator.at/
- 2FA aktivieren, wo möglich

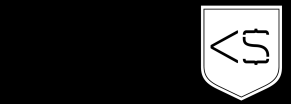
PASSWORT MANAGER

- Verwahren von Passwörtern & anderen sensiblen Daten
- Kein Merken von Passwörtern notwendig → können deshalb sehr komplex sein
- Unkomplizierte Verwendung
- Gibt auch Self-Hosted Lösungen
- Bekannte Tools
  - NordPass
  - 1Password
  - Bitwarden

Quelle: https://quicklaunch.io/two-factor-authentication-vs-multi-factor-authentication/

2FA

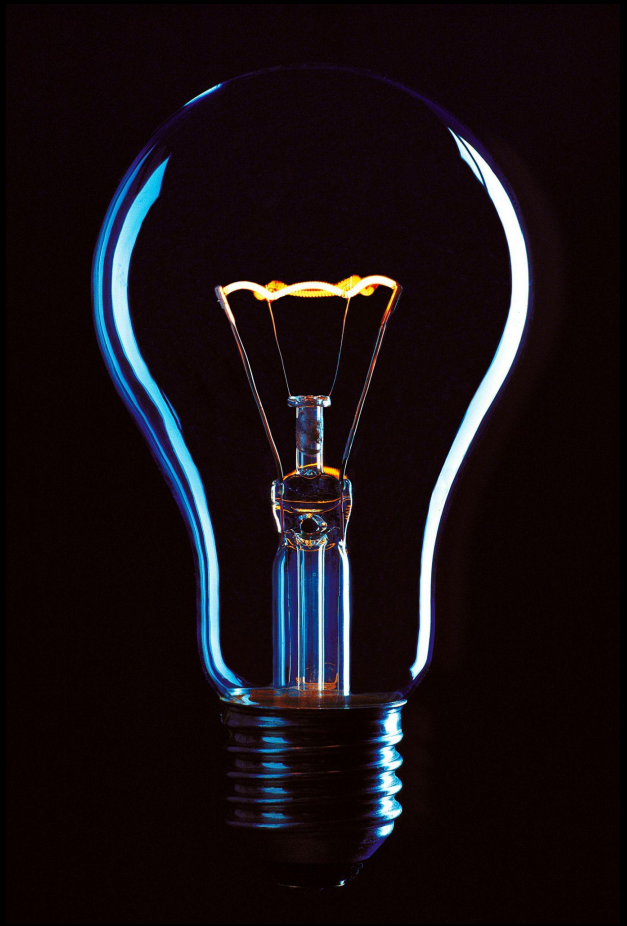
- Erhöhte Sicherheit
- Schutz vor Passwort Diebstahl
- Verschiedene Faktoren
  - SMS-Codes, mobile Authentifizierungs-Apps, Hardware-Token
  - biometrische Daten (Fingerabdrücke, Gesichtserkennung)
- Einfache Implementierung / Aktivierung
- Tools
  - Google Authenticator / Microsoft Authenticator
  - Kann auch durch diverse Passwortmanager abgebildet werden



- WAS SIND DEINE GÄNGIGSTEN APPLIKATIONEN BEI DENEN EIN PASSWORT BENÖTIGT WIRD?

- BEI WIEVIELEN HAST DU DASSELBE PASSWORT?

- BEI WIEVIELEN IST 2FA AKTIVIERT?



ACTIONS BEI VERDACHT / ANGRIFF

- Passwortänderung
  - Überall wo es verwendet wird
  - kann durch Passwortmanager eingesehen werden
- Prüfen auf Daten Leak
- Melden
  - An Admin / Zuständige Person oder Abteilung kommunizieren
  - Andere MitarbeiterInnen warnen
  - **Betroffene Personen informieren**
- Sicherheitseinstellungen prüfen / beobachten

GRUNDLAGEN DER NETZWERKSICHERHEIT

KONFIGURATION

- Standard Anmeldedaten ändern
  - Router
  - admin / admin1234
- Network Encryption → 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. Synology
- Eigener NAS (Network Attached Storage)
  - Im besten Fall nicht nach von außerhalb zugänglich
  - 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