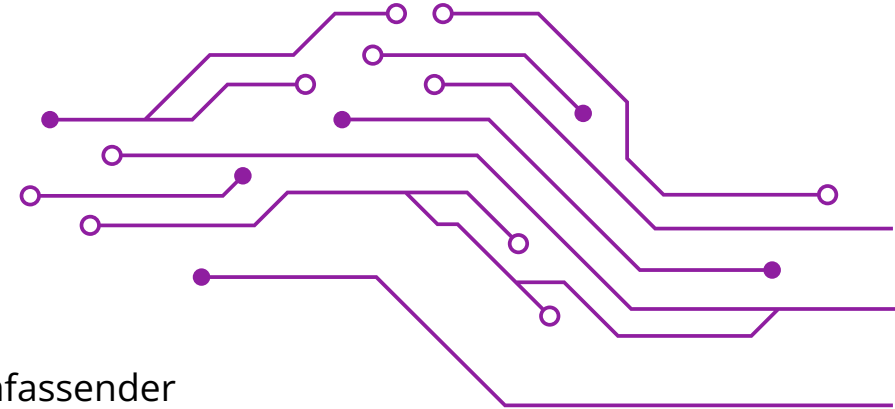
Cybersicherheit – Grundlagen



Eine Nachhaltige Digitalisierung gelingt nur mit umfassender Weitsicht!

15.01.2025 | Cecilia und Jona Sander

Agenda

- Was ist Cybersicherheit
- Wichtigkeit Cybersicherheit
- Cyberangriffe
- Wie schützen wir unsere Daten
  - physisch
  - digital
- Was tun wenn es doch passiert ist?

Agenda

- Was ist Cybersicherheit
- Wichtigkeit Cybersicherheit
- Cyberangriffe
- Wie schützen wir unsere Daten
  - physisch
  - digital
- Was tun wenn es doch passiert ist?

Agenda

- Was ist Cybersicherheit
- Wichtigkeit Cybersicherheit
- Cyberangriffe
- Wie schützen wir unsere Daten
  - physisch
  - digital
- Was tun wenn es doch passiert ist?

Agenda

- Was ist Cybersicherheit
- Wichtigkeit Cybersicherheit
- Cyberangriffe
- Wie schützen wir unsere Daten
  - physisch
  - digital
- Was tun wenn es doch passiert ist?

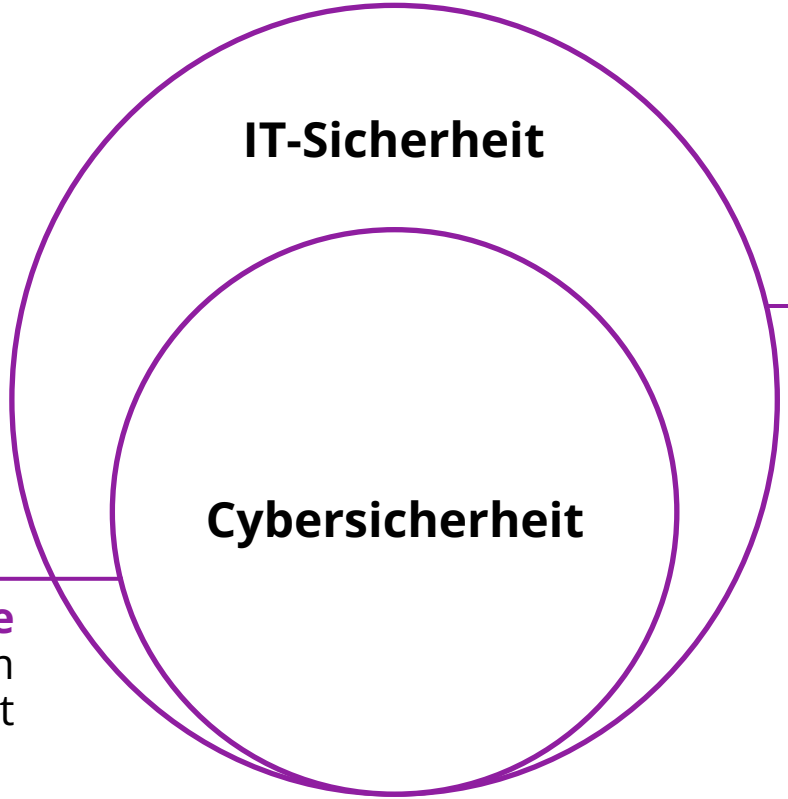
Agenda

- Was ist Cybersicherheit
- Wichtigkeit Cybersicherheit
- Cyberangriffe
- Wie schützen wir unsere Daten
  - physisch
  - digital
- Was tun wenn es doch passiert ist?

Cybersicherheit – Was ist das genau?

Cybersicherheit = IT-Sicherheit

Unterschiede und Überschneidungen



Ganzheitlicher Ansatz: **physische** (z. B. verschlossene Serverräume) als auch **digitale** (z. B. Passwörter) Daten

spezifisch auf **digitale** Bedrohungen aus dem Internet

Cybersicherheit leicht erklärt

Cybersicherheit ist der Schutz von

- Daten,
- Privatsphäre
- Geschäftsprozessen
- und Menschen vor digitalen Bedrohungen.

Cybersicherheit betrifft uns alle

206 Mrd. Euro Schaden durch Cyberangriffe (Deutschland, 2023)

Betroffen: Konzerne, Kommunen, kleine Betriebe – und jede private Person

Schadsoftware: Verschlüsselt Daten & fordert Lösegeld

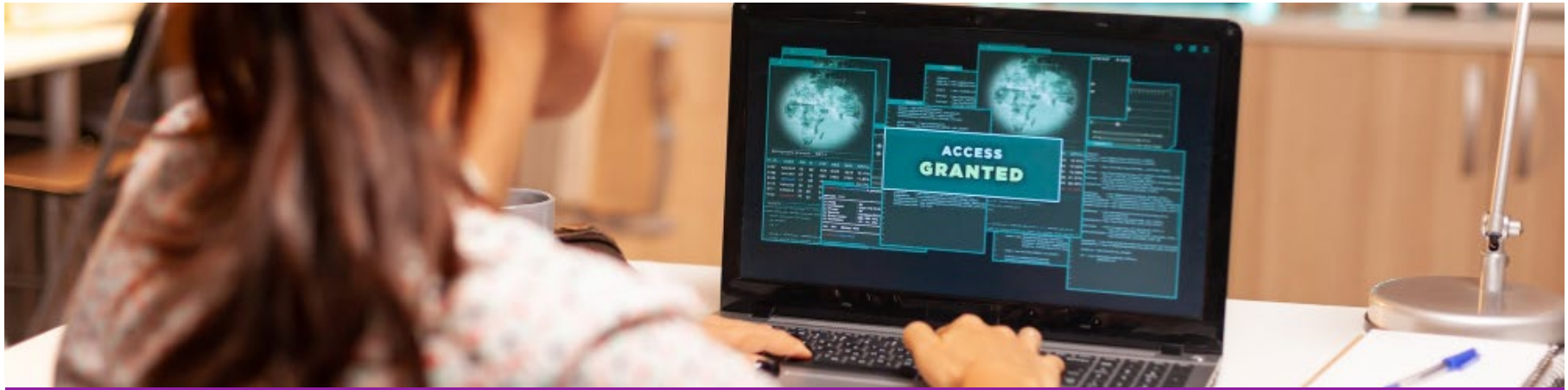
Was gilt es zu schützen?

Daten, Privatsphäre & Prozesse schützen

- Bankkonten
- Fotos
- Messenger
- ...

Quelle: BSI (Bundesamt für Sicherheit in der Informations-technik) Lagebericht2024.pdf

Zahlen zum Malware-Anstieg



2023 haben Sicherheitsexperten weltweit durchschnittlich **309.000 neue Schadprogramm-Varianten pro Tag** entdeckt, was einem **Anstieg von 26 %** im Vergleich zum Vorjahr entspricht.

Quelle: Lagebericht des BSIs „Lagebericht2024.pdf“

Warum ist Cybersicherheit wichtig?

Schutz sensibler Daten

Gesetzliche Vorgaben & Compliance

Vertrauen bei Kunden & Partnern erhalten

Wirtschaftsspionage abwehren

Kosten und Reputations-schäden vermeiden

Risiken kennen und richtig reagieren

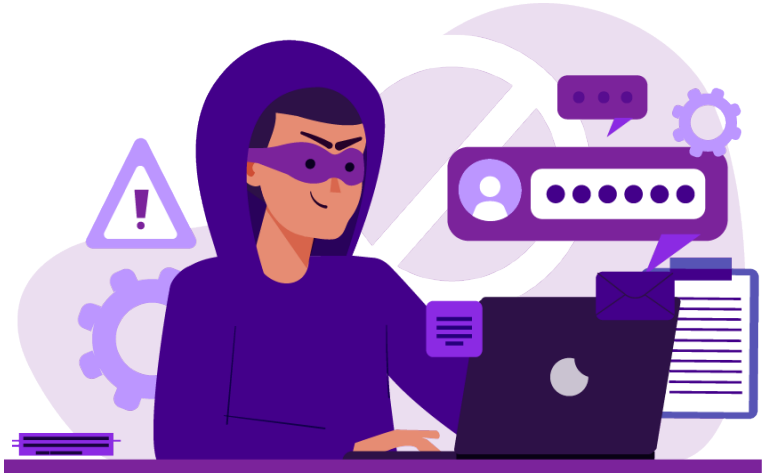
Betriebsfähigkeit sicherstellen

Was ist ein Cyberangriff?

Ein Cyberangriff ist eine gezielte Attacke auf Computer oder Computernetzwerke.

Die Folge:

- Störung von Betriebsabläufen,
- der Abfluss von Informationen,
- die Verweigerung von Zugängen sowie die Manipulation,
- Beschädigung oder Zerstörung von Hardware, Daten, Netzwerken oder technischen Systemen.



Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Phishing

Kriminelle versenden gefälschte E-Mails, SMS oder Chat-Nachrichten, die vertrauenswürdig wirken sollen.

Ziel:
Erahnen oder Abgreifen von Zugangsdaten, Kreditkarteninformationen oder anderen sensiblen Daten.

35,3 % sind Phishing-Angriffe

Phishing

Wie viele Phishing-Mails werden pro Jahr weltweit verschickt?

A 1 Million

B 3 Milliarden

C 3 Billionen

D 10 Milliarden

Phishing

Wie viele Phishing-Mails werden pro Jahr weltweit verschickt?

A 1 Million

B 3 Milliarden

C 3 Billionen

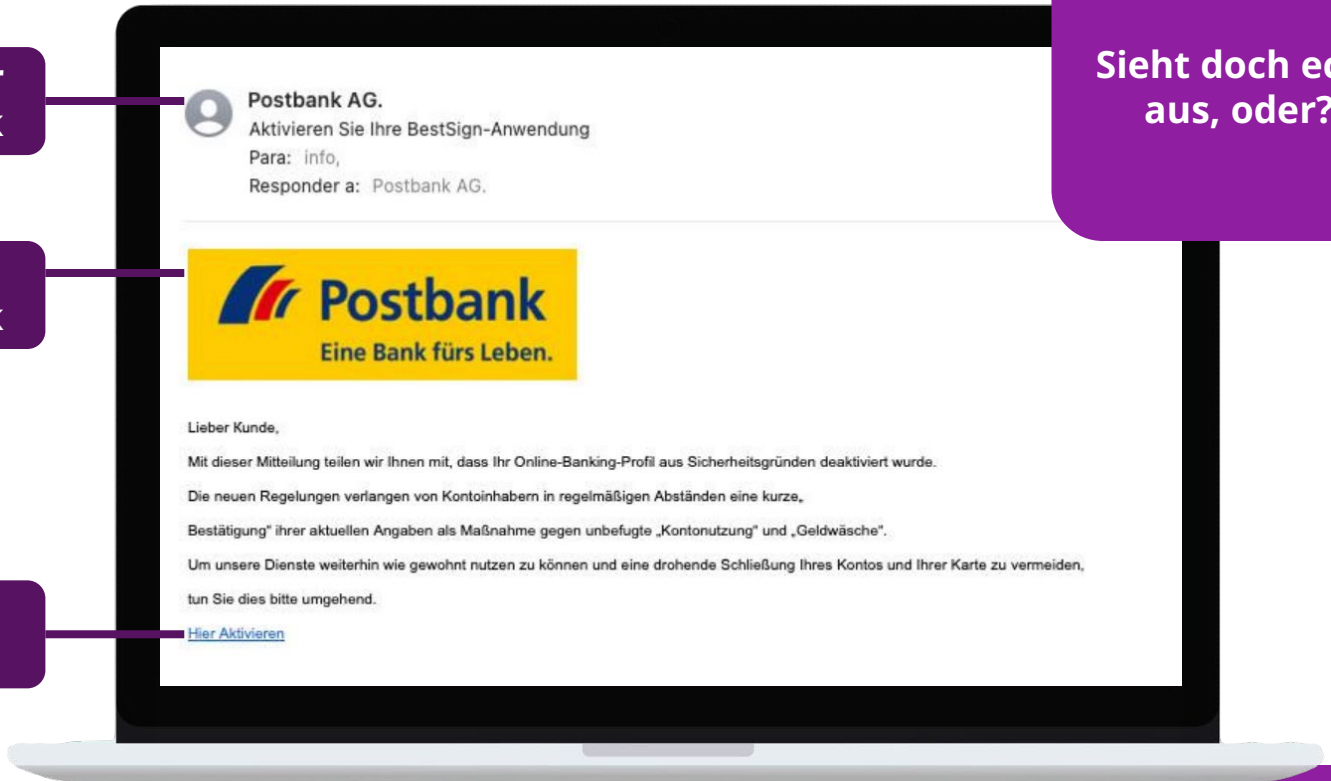
D 10 Milliarden

Phishing – Woran erkennen?

Absender Postbank

Logo Postbank

Link



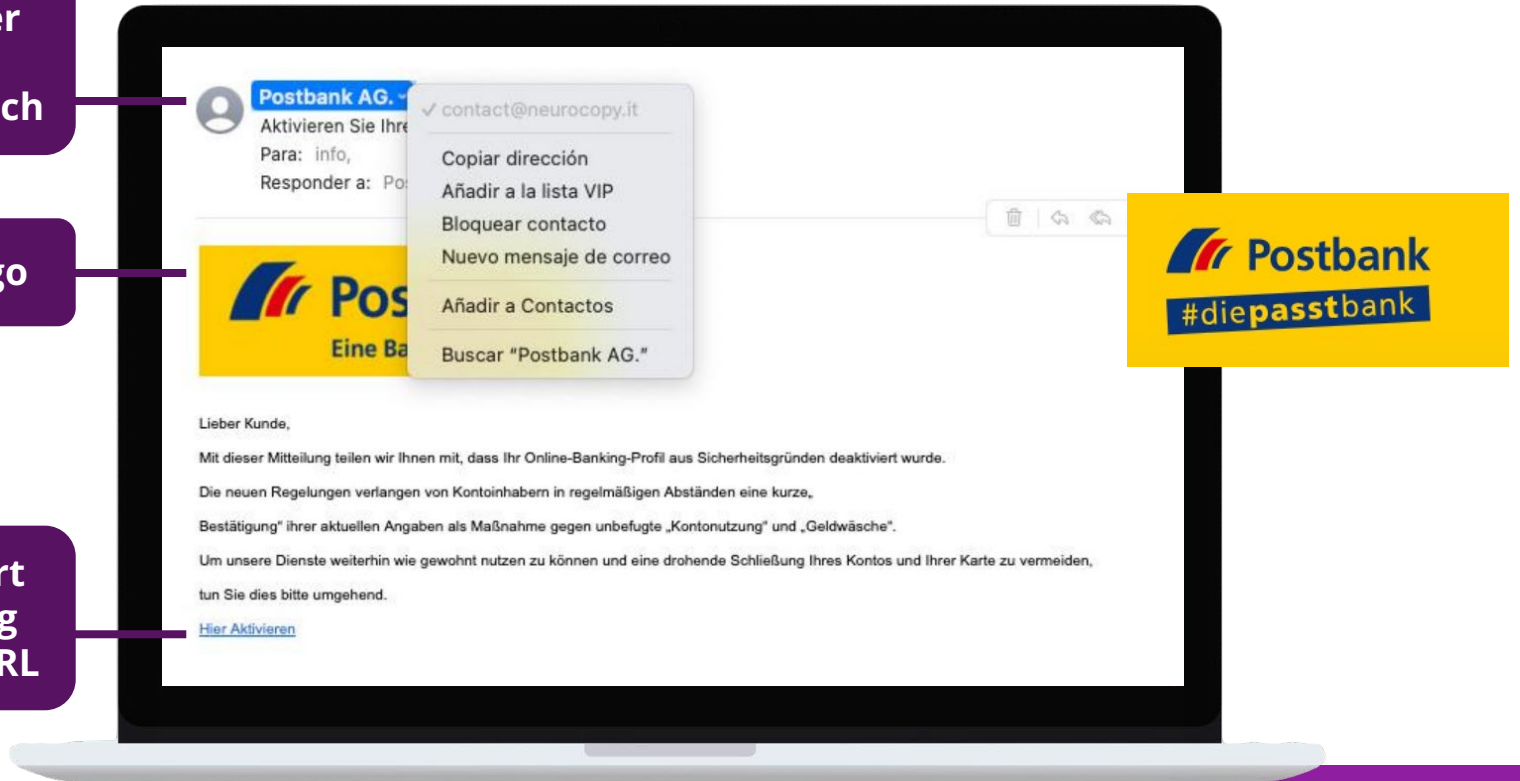
Sieht doch echt aus, oder?

Phishing – Woran erkennen?

Absender nicht authentisch

Altes Logo

Link führt auf völlig andere URL



Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Ransomware

Schadsoftware, die Daten verschlüsselt **und** ein Lösegeld verlangt.

Häufig werden Unternehmen, Behörden, Krankenhäuser oder Privatpersonen angegriffen, um hohe Zahlungen zu erzwingen.

Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Distributed Denial of Service (DDoS)

Angreifer überfluten einen Server oder Onlinedienst mit massiven Anfragen, sodass das System überlastet und legitime Nutzer keinen Zugriff mehr haben.

Oft genutzt, um Webseiten oder Netzwerke lahmzulegen.

Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Malware (malicious [bösartig] **software)**

Oberbegriff für Viren, Würmer, Trojaner, Spyware etc.

Wird häufig per E-Mail-Anhang, Download oder infizierten Websites verbreitet.

Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Spyware / Keylogger

Spezielle Schadprogramme, die Tastatureingaben mitlesen oder umfassend Aktivitäten auf dem System aufzeichnen.

Ziel ist das Ausspionieren von Passwörtern, PINs und anderen vertraulichen Daten.

Achtung, Cyberfallen! Angriffe auf einen Blick.

- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Social Engineering

Psychologische Manipulation von Menschen, um an vertrauliche Informationen zu gelangen.

Kann telefonisch (**Vishing** - Voice Phishing), **Phishing** (Mail), per SMS (**Smishing**), QR-Codes (**Quiching**), über Social Media oder über persönliche Kontakte erfolgen.

Social Engineering

Das war ja nur gespielt ....

Die Geschichte hat sich genauso abgespielt.
Namen und Getränke abgeändert.

- Vertrauen aufbauen
- Persönliche Details entlocken
- Sich Zugang verschaffen

Achtung, Cyberfallen! Angriffe auf einen Blick.

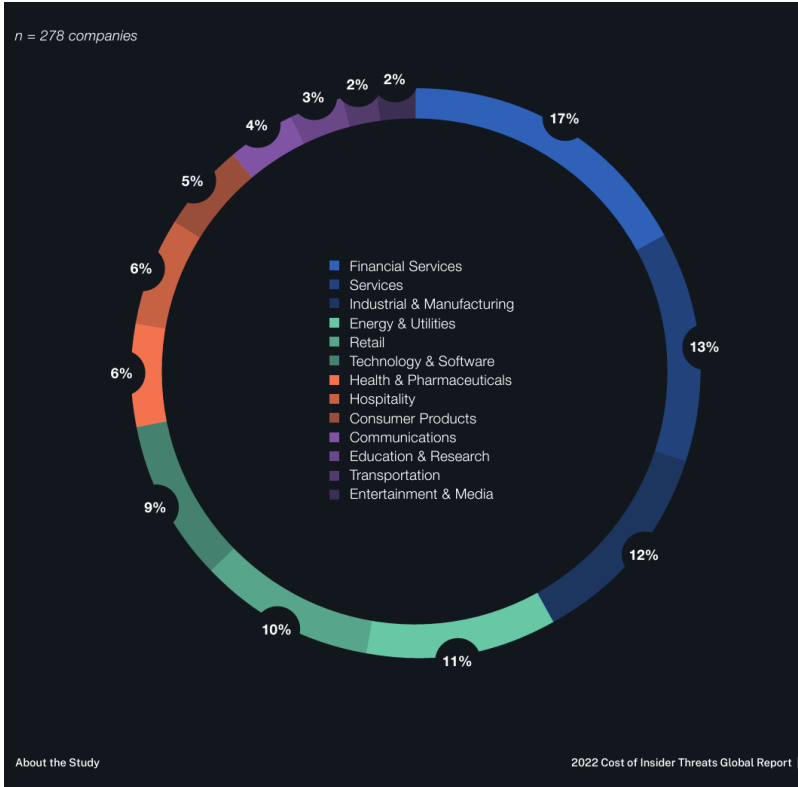
- Phishing
- Ransomware
- DDoS
- Malware
- Spyware/Keylogger
- Social Engineering
- Insider Threats

Insider Threats

Angriffe oder Datenlecks durch eigene Mitarbeiter oder nahestehende Personen.

Kann **absichtlich** (z. B. bei Unzufriedenheit) oder **fahrlässig** (keine Sicherheitsregeln beachtet) passieren.

Wie viel Prozent machen Bedrohungen von innen aus?



Wie viel Prozent machen Bedrohungen von innen aus?

56%

Fahrlässig oder unvorsichtig

23%

böswillig

Quelle: [Ponemon Cost of Insider Threats Global Report 2022]

Wie wir uns und unsere Daten im digitalen Alltag schützen können.

Passwortsicherheit

Längere Passwörter sind sicherer als komplizierte kurze – Mythos oder Wahrheit?

Welches Passwort ist am sichersten?

A Password123

B !dF9s7gH!

C IchLiebeKartoffeln2024

Passwortsicherheit

Längere Passwörter sind sicherer als komplizierte kurze – Mythos oder Wahrheit?

Welches Passwort ist am sichersten?

A Password123

B !dF9s7gH!

C IchLiebeKartoffeln2024

Passwortsicherheit – Brute-Force-Angriff

Ein **Brute-Force-Angriff** ist eine Methode, bei der ein Angreifer alle möglichen Kombinationen von Zeichen ausprobiert, um ein Passwort zu erraten.

Es ist ein **"Raten mit System",** das so lange dauert, bis das richtige Passwort gefunden wird.

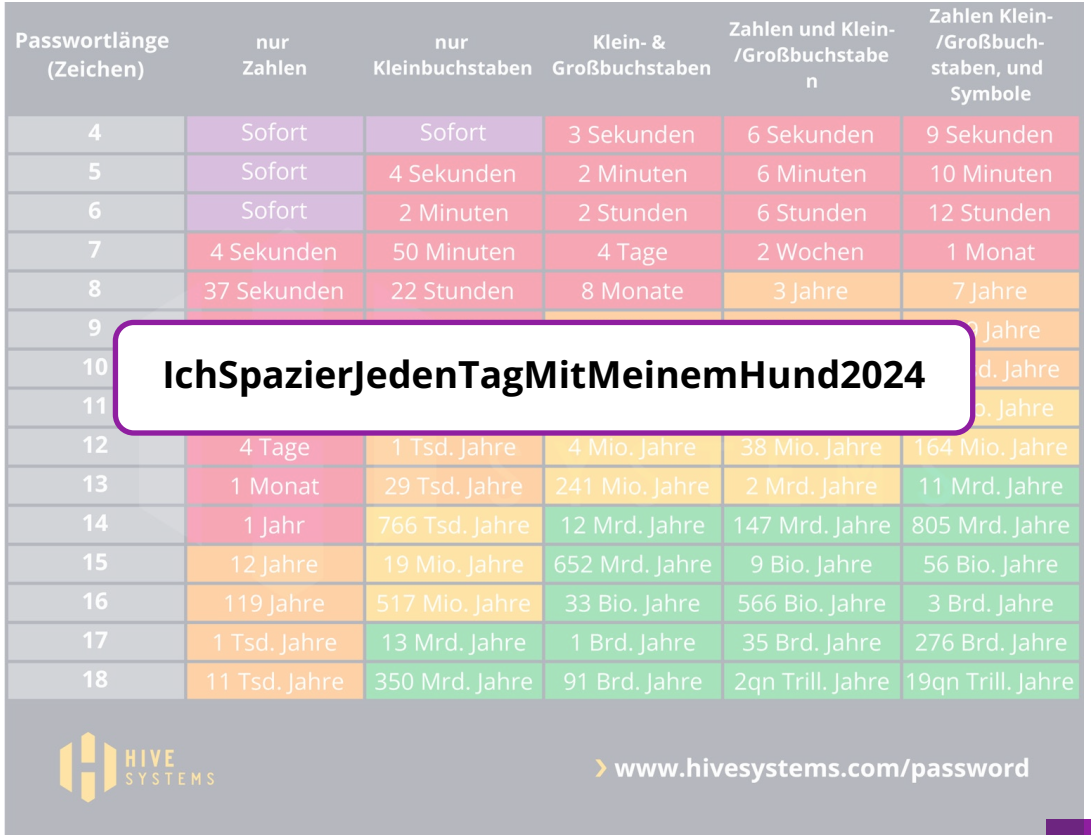
Länge statt Sonderzeichen-Wahn

Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein-/Großbuchstaben	Zahlen Klein-/Großbuch-staben, und Symbole
4	Sofort	Sofort	3 Sekunden	6 Sekunden	9 Sekunden
5	Sofort	4 Sekunden	2 Minuten	6 Minuten	10 Minuten
6	Sofort	2 Minuten	2 Stunden	6 Stunden	12 Stunden
7	4 Sekunden	50 Minuten	4 Tage	2 Wochen	1 Monat
8	37 Sekunden	22 Stunden	8 Monate	3 Jahre	7 Jahre
9	6 Minuten	3 Wochen	33 Jahre	161 Jahre	479 Jahre
10	1 Stunde	2 Jahre	1 Tsd. Jahre	9 Tsd. Jahre	33 Tsd. Jahre
11	10 Stunden	44 Jahre	89 Tsd. Jahre	618 Tsd. Jahre	2 Mio. Jahre
12	4 Tage	1 Tsd. Jahre	4 Mio. Jahre	38 Mio. Jahre	164 Mio. Jahre
13	1 Monat	29 Tsd. Jahre	241 Mio. Jahre	2 Mrd. Jahre	11 Mrd. Jahre
14	1 Jahr	766 Tsd. Jahre	12 Mrd. Jahre	147 Mrd. Jahre	805 Mrd. Jahre
15	12 Jahre	19 Mio. Jahre	652 Mrd. Jahre	9 Bio. Jahre	56 Bio. Jahre
16	119 Jahre	517 Mio. Jahre	33 Bio. Jahre	566 Bio. Jahre	3 Brd. Jahre
17	1 Tsd. Jahre	13 Mrd. Jahre	1 Brd. Jahre	35 Brd. Jahre	276 Brd. Jahre
18	11 Tsd. Jahre	350 Mrd. Jahre	91 Brd. Jahre	2qn Trill. Jahre	19qn Trill. Jahre

HIVE SYSTEMS

› www.hivesystems.com/password

Länge statt Sonderzeichen-Wahn



Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein-/Großbuchstaben	Zahlen Klein-/Großbuch-staben, und Symbole
4	Sofort	Sofort	3 Sekunden	6 Sekunden	9 Sekunden
5	Sofort	4 Sekunden	2 Minuten	6 Minuten	10 Minuten
6	Sofort	2 Minuten	2 Stunden	6 Stunden	12 Stunden
7	4 Sekunden	50 Minuten	4 Tage	2 Wochen	1 Monat
8	37 Sekunden	22 Stunden	8 Monate	3 Jahre	7 Jahre
9					Jahre
10					d. Jahre
11					. Jahre
12	4 Tage	1 Tsd. Jahre	4 Mio. Jahre	38 Mio. Jahre	164 Mio. Jahre
13	1 Monat	29 Tsd. Jahre	241 Mio. Jahre	2 Mrd. Jahre	11 Mrd. Jahre
14	1 Jahr	766 Tsd. Jahre	12 Mrd. Jahre	147 Mrd. Jahre	805 Mrd. Jahre
15	12 Jahre	19 Mio. Jahre	652 Mrd. Jahre	9 Bio. Jahre	56 Bio. Jahre
16	119 Jahre	517 Mio. Jahre	33 Bio. Jahre	566 Bio. Jahre	3 Brd. Jahre
17	1 Tsd. Jahre	13 Mrd. Jahre	1 Brd. Jahre	35 Brd. Jahre	276 Brd. Jahre
18	11 Tsd. Jahre	350 Mrd. Jahre	91 Brd. Jahre	2qn Trill. Jahre	19qn Trill. Jahre

IchSpazierJedenTagMitMeinemHund2024

HIVE SYSTEMS

› www.hivesystems.com/password

Passkeys – Das Login der Zukunft

Passkeys sind kryptographische Schlüsselpaare, die den klassischen Login mit Benutzername/ Passwort ersetzen.

Funktionieren in Kombination mit z. B. Fingerabdruck, PIN oder Gesichtserkennung auf dem Gerät.

phishingsicher, einfacher, sicherer.

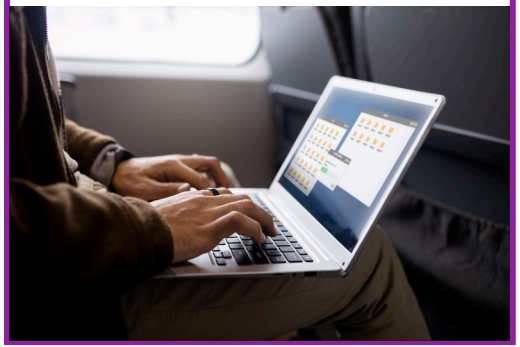
Wie wir uns und unsere Daten im analogen Alltag schützen können.

Sichere Arbeitsumgebung

Sichere Arbeitsumgebung

Sicherheit außerhalb des Arbeitsplatzes

Im Zug, Café, usw. ...

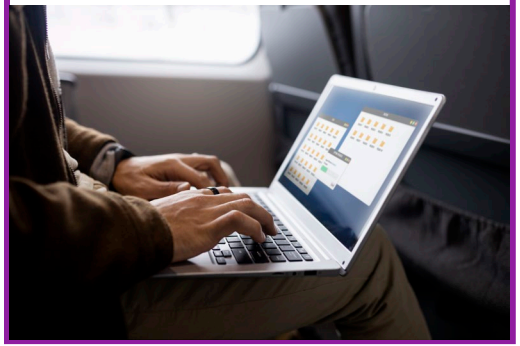


Gerätediebstahl

Im Homeoffice

Sicherheit außerhalb des Arbeitsplatzes

- Keine sensiblen Daten über **öffentliche WLANs** austauschen
- **VPN** nutzen
- Fake Netzwerke mit gleicher SSID

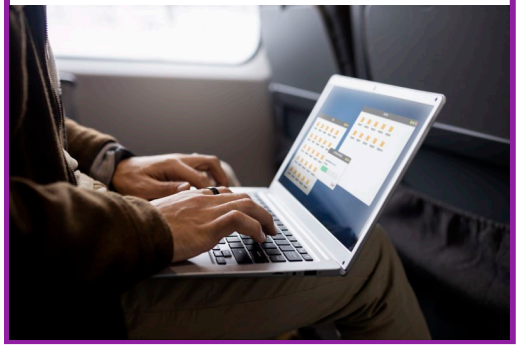


Gerätediebstahl

Im Homeoffice

Sicherheit außerhalb des Arbeitsplatzes

- Keine sensiblen Daten über **öffentliche WLANs** austauschen
- **VPN** nutzen
- Fake Netzwerke mit gleicher SSID

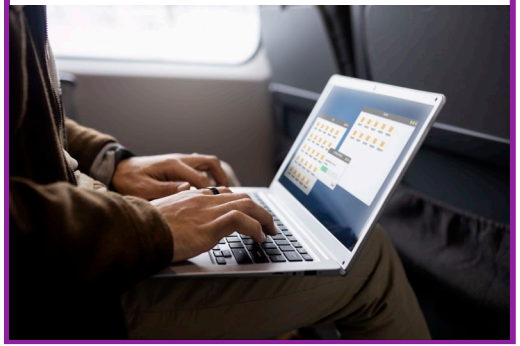


- Geräte verschlüsseln und mit starken Passwörtern schützen.
(z. B. Bitlocker)

Im Homeoffice

Sicherheit außerhalb des Arbeitsplatzes

- Keine sensiblen Daten über **öffentliche WLANs** austauschen
- **VPN** nutzen
- Fake Netzwerke mit gleicher SSID



- Geräte verschlüsseln und mit starken Passwörtern schützen.
(z. B. Bitlocker)

- Passwörter regelmäßig ändern
- Updates durchführen (Software, Router etc.)
- Separate Netzwerke für Gäste erstellen.

Verhalten bei IT-Sicherheitsvorfällen

Schritte im Ernstfall:

- ☑ IT informieren, nicht eigenmächtig „herumdoktern“
- ☑ Passwörter ändern, sofern sensible Bereiche betroffen sind
- ☑ Dokumentation (wer, was, wann)
- ☑ Ruhig bleiben und ggf. an interne Security-Richtlinien halten

Abschluss

Zusammenfassung:

- Ransomware & Phishing: Größte Bedrohungen laut BSI, besonders KMU gefährdet.
- Hinterfragen Sie sämtliche E-Mails
- Sind ihre Passwörter sicher und lang genug?
- Passkeys sind ein zukunftsfähiger, phishingsicherer Weg
- Achten Sie darauf, wem Sie bestimmte Informationen überlassen Stichwort: Social Engineering
- Halten Sie ihre Daten sicher, auf der Arbeit und auch außerhalb des Arbeitsplatzes
- Und wenn doch etwas passiert? Schnell und richtig reagieren

DANKE FÜR DIE AUFMERKSAMKEIT