BENUTZBARE SICHERHEIT

Authentifizierung und Passwörter
… oder wie ich meine Zugänge sicherer machen sollte

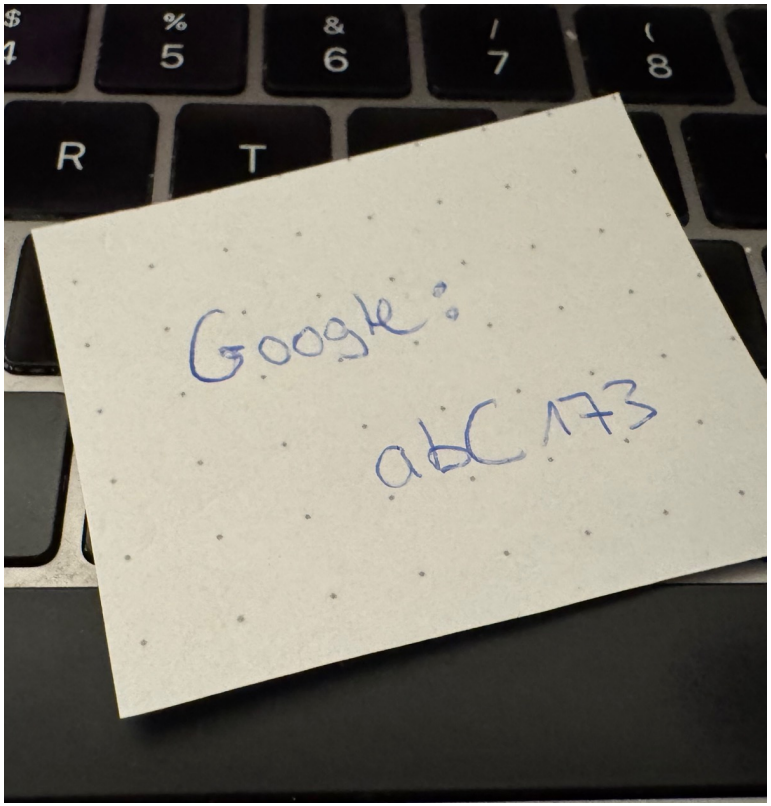
Foto von FlyD auf Unsplash

Prof. Dr. Bastian Pfleging – Professur für Ubiquitous Computing & Smart Systems – Institut für Informatik
bastian.pfleging@informatik.tu-freiberg.de

Sicherheit in der analogen Welt – und in der digitalen Welt?

Generiertes Bild (ChatGPT)

Foto von Calvin Hanson auf Unsplash



heise online

Abmelden | Mein Account Suchen

heise+ IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

Künstliche Intelligenz Windows Energie ePA für alle Raumfahrt Podcasts

heise online > Security > Cyber-Angriff: IT der TU Freiberg weitreichend lahmgelegt

Cyber-Angriff: IT der TU Freiberg weitreichend lahmgelegt

Ein Cyber-Angriff auf die IT der TU Freiberg in Sachsen führt zu weitreichenden Einschränkungen. Zum Wochenende hat die Uni die Internetverbindungen gekappt.

166

(Bild: Black_Kira/Shutterstock.com)

24.01.2023, 21:43 Uhr Lesezeit: 3 Min. | Security

Von Dirk Knop

An der sächsischen TU Freiberg sind in der vergangenen Woche Cyberkriminelle eingebrochen. Zum Wochenende haben die Mitarbeiter des Uni-Rechenzentrums

Security Newsletter

https://www.heise.de/news/Cyber-Angriff-IT-der-TU-Freiberg-weitreichend-lahmgelegt-7469937.html

Ausgewählte Prinzipien der IT-Sicherheit

Vertraulichkeit:

Daten nur durch autorisierte Personen / Systeme einsehbar

Integrität:

Schutz vor unbefugten Veränderungen

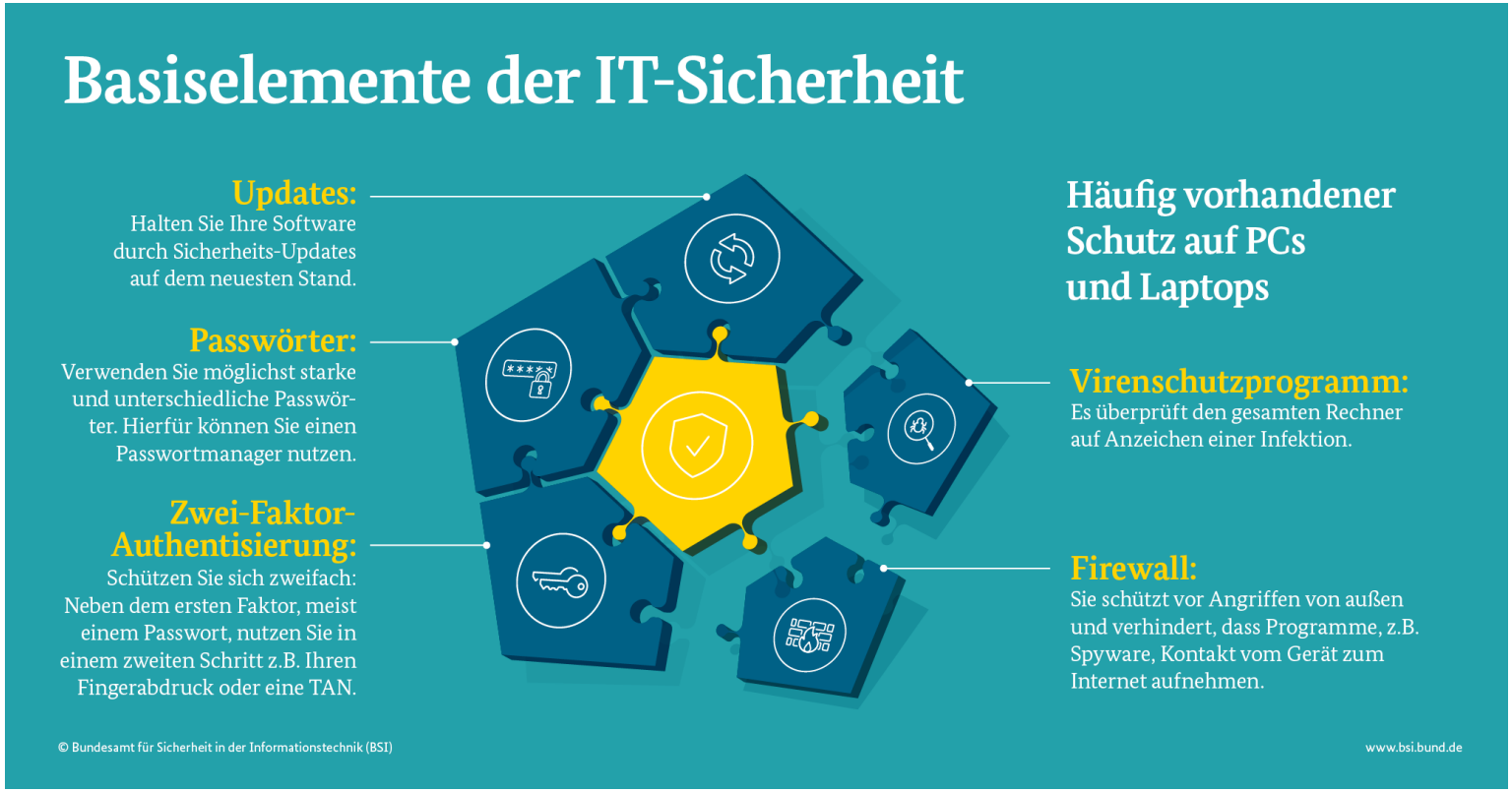
Zugriffskontrolle

Zugriff auf Daten / Systeme nur durch autorisierte Personen / Systeme

Verfügbarkeit:

Zuverlässige Systeme, die jederzeit verfügbar sind

IT-Sicherheit für Anwender:innen



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

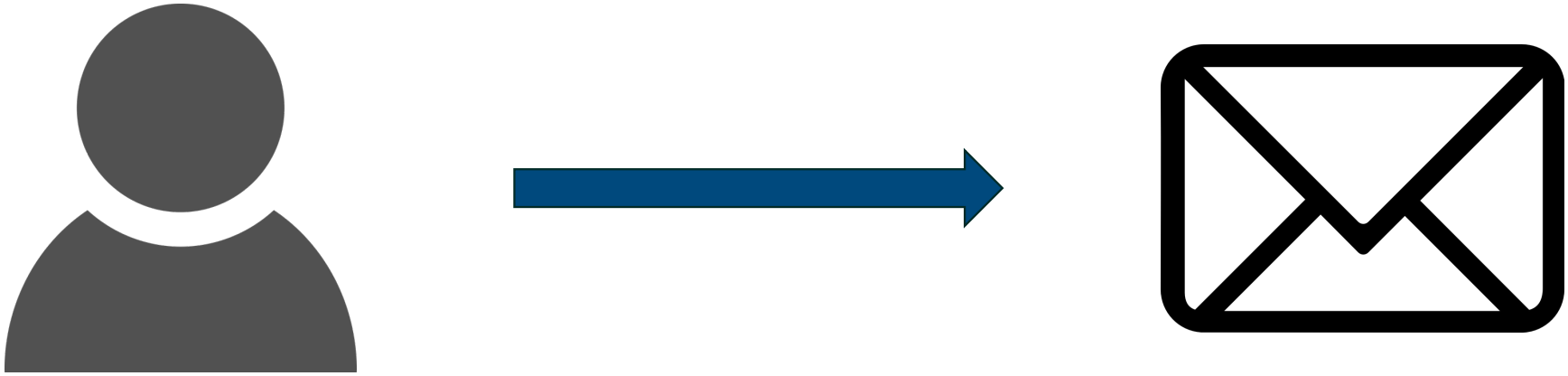
Authentifizierung / Authentisierung

- Nachweis, dass ein Benutzer tatsächlich der ist, für den er sich ausgibt
- Identitätsprüfung anhand bestimmter Merkmale / Nachweise

Wissensbasiert	Besitzbasiert	Biometrisch
Passwörter	Einmalpasswörter per App, SMS, E-Mail	Fingerabdruck
PINs	Hardware-Token	Gesichtserkennung
Graphische Muster	Smartcards	Iris-Scan
Sicherheitsfragen	Digitale Zertifikate	Stimmerkennung, Nutzerverhalten
… was der Nutzer weiß	**… was der Nutzer besitzt**	**… was der Nutzer ist**

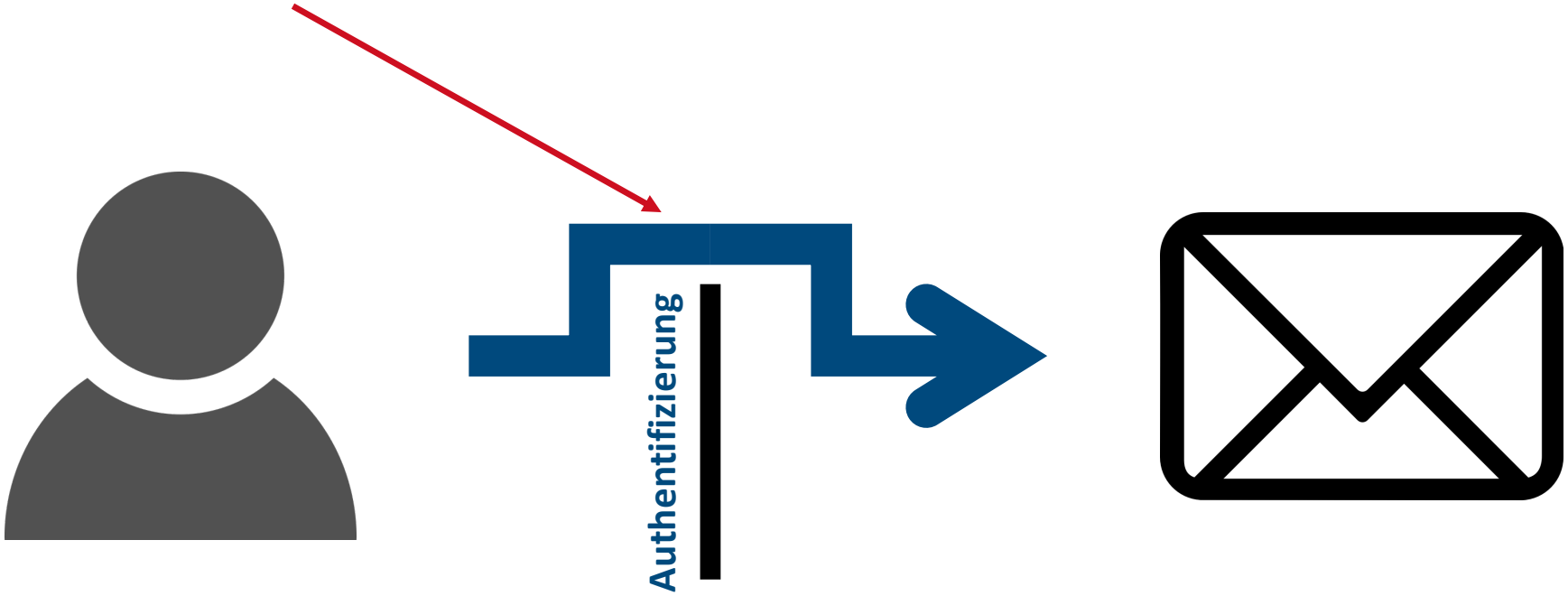
Ziele der Nutzenden

Aufgaben erledigen



Ziele von Sicherheitsexpert:innen

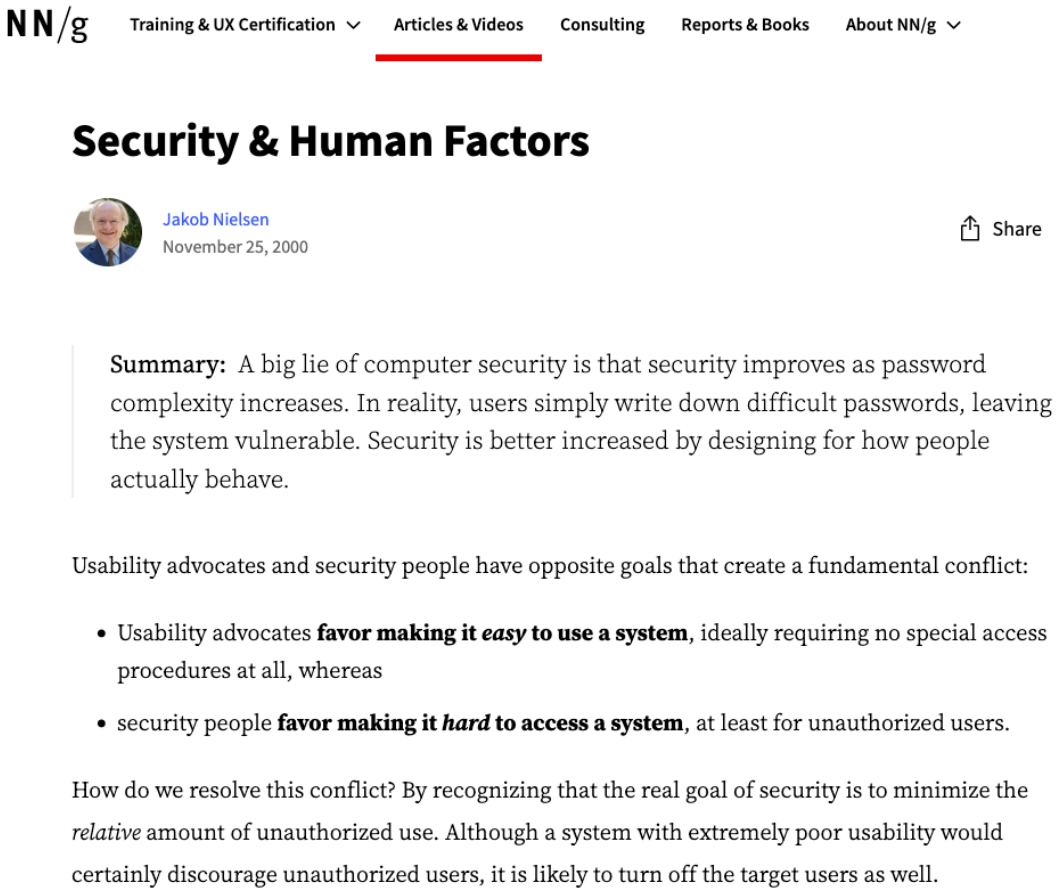
System absichern



Sicherheit und der Faktor Mensch

„A big lie of computer security is that security improves as password complexity increases. In reality, users simply write down difficult passwords, leaving the system vulnerable. Security is better increased by designing for how people actually behave.”

https://www.nngroup.com/articles/security-and-human-factors/



NN/g Training & UX Certification Articles & Videos Consulting Reports & Books About NN/g

Security & Human Factors

Jakob Nielsen
November 25, 2000

Share

Summary: A big lie of computer security is that security improves as password complexity increases. In reality, users simply write down difficult passwords, leaving the system vulnerable. Security is better increased by designing for how people actually behave.

Usability advocates and security people have opposite goals that create a fundamental conflict:

- Usability advocates **favor making it *easy* to use a system**, ideally requiring no special access procedures at all, whereas
- security people **favor making it *hard* to access a system**, at least for unauthorized users.

How do we resolve this conflict? By recognizing that the real goal of security is to minimize the *relative* amount of unauthorized use. Although a system with extremely poor usability would certainly discourage unauthorized users, it is likely to turn off the target users as well.

Übereinstimmende Prioritäten?

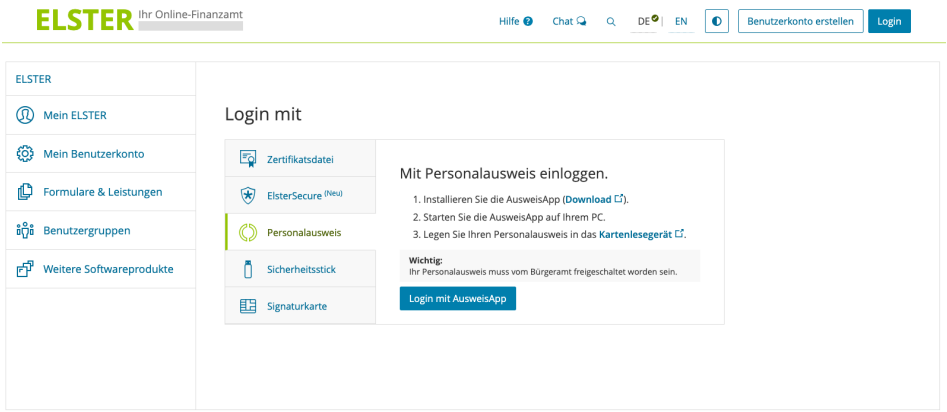
2-Faktor-Authentifizierung nutzen, nur über VPN!

Sicherheitsexpert:innen

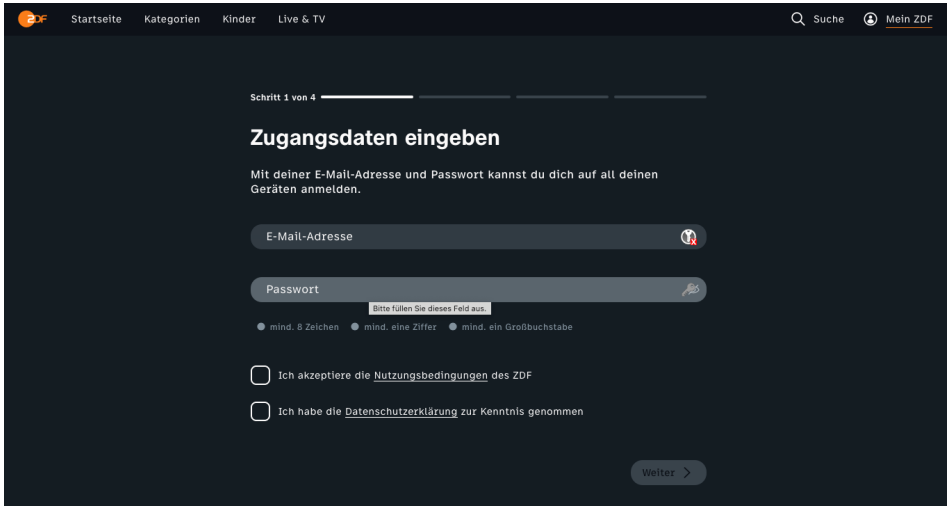
Ich nehme eine einfach PIN, um sie nicht zu vergessen.

Nutzende

Unterschiedliche Situationen – unterschiedliche Anforderungen



https://www.elster.de/eportal/login/npa



https://www.zdf.de/mein-zdf/registrierung

Je größer der mögliche Schaden, desto stärker sollte das Passwort gewählt werden.

Die am häufigsten genutzten PINs und Passwörter

123456
123456789
qwerty
password
1234567
12345678
12345
iloveyou
111111
123123
abc123
qwerty123
1q2w3e4r

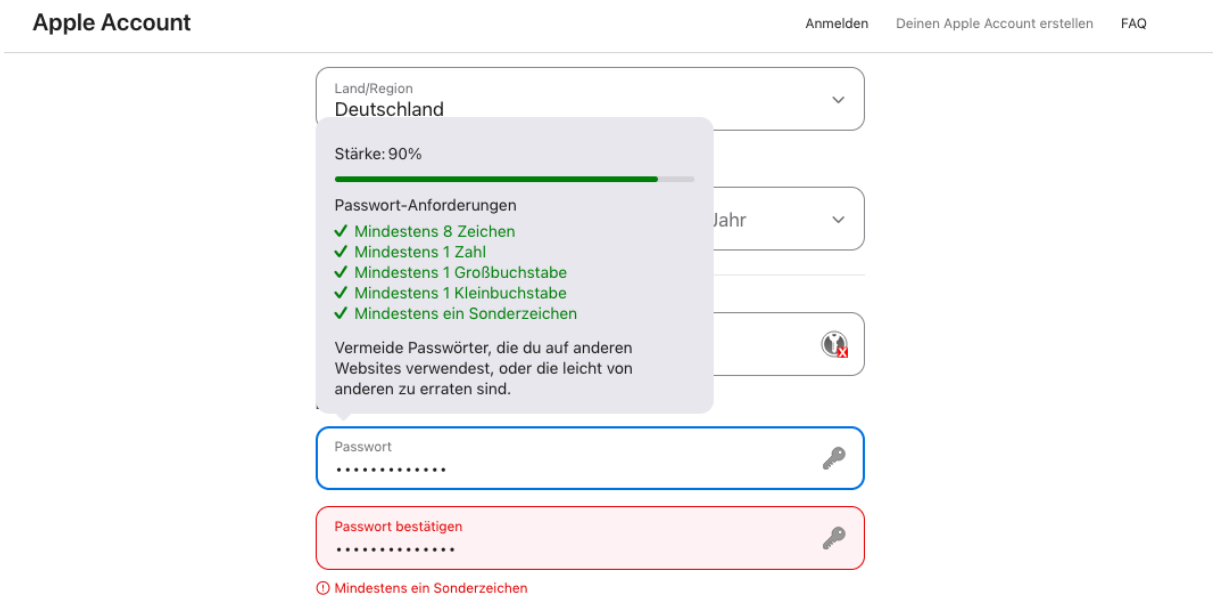
admin
qwertyuiop
654321
555555
lovely
7777777
welcome
888888
princess
dragon
password1
123qwe

1234
1111
0000
1212
7777
1004
2000
4444
2222
6969

https://gizmodo.com/its-time-to-nervously-mock-the-50-worst-passwords-of-th-1840514905

https://www.bayern3.de/handy-pin-code-haeufig-selten

Passwortrichtlinien



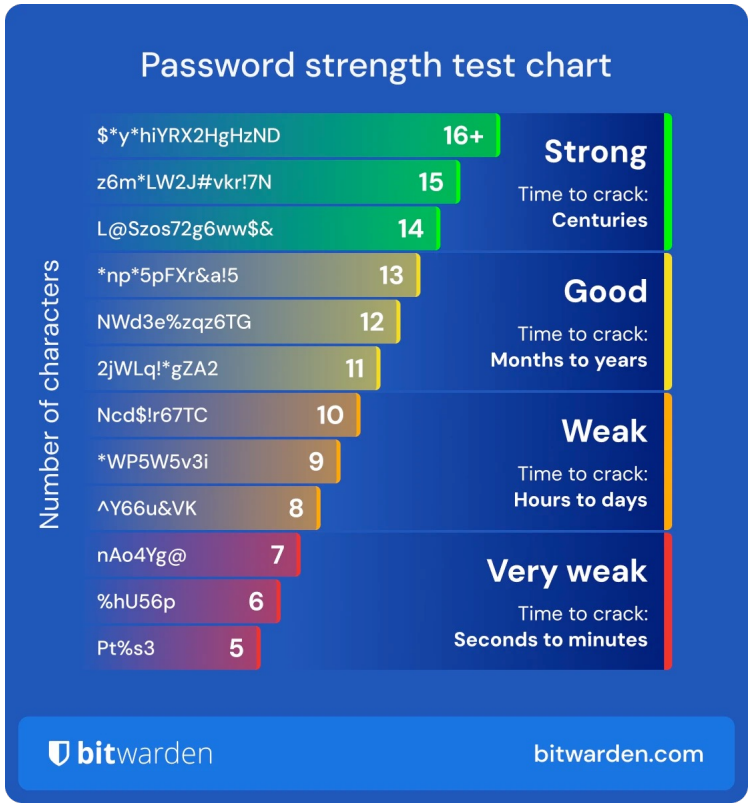
https://account.apple.com/account#

Was sind übliche Angriffsmethoden?

Was probiert ein Angreifer aus?

- Liste der am häufigsten verwendeten Passwörter
- Abgewandelte Ergänzungen und Ersetzungen („Fr3ib3rg!“)
- Raten / „Brute Force“
- Wissen über einen Account (Partner, Kind, Geburtsdatum, …)
- Kombinationen daraus

Wie lange dauert ein Angriff?



https://bitwarden.com/blog/how-long-should-my-password-be/

Was macht „gute“ Passwörter aus?

- Die besten Passwörter sind die, die man sich nicht merkt / merken kann (zufällige Zeichenfolgen)
- Je länger, desto besser
  - Kurz und komplex (Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen): mindestens 8, besser 12 Zeichen
  - Lang und weniger komplex: mindestens 25 Zeichen
- Möglichst alle verfügbaren Zeichen nutzen (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen)

Wichtig / bitte vermeiden:

- Jedes Passwort ist schwach, sobald es kompromittiert ist
- Vermeiden: Passwörter wiederverwenden
- Keine Namen von Familie / Freunden, Tieren, Stars, Geburtsdaten
- Keine gängigen Verfahren und Wiederholungsmuster (abc123) oder Tastaturmuster (asdfjklö)
- Ziffer oder Sonderzeichen am Anfang/Ende eines einfachen Passworts reicht nicht!

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Strategien

… besser als “einfache“ Passwörter, aber noch verbesserungswürdig

Selbst merken – kreativ sein!

Beispiel 1: Längeren (sehr individuellen!) Satz merken

- Daraus: jeder erste/fünfte/letzte Buchstabe
- Umwandlung bestimmter Buchstaben in Zahlen / Sonderzeichen (z.B. Leetspeak, https://de.wikipedia.org/wiki/Leetspeak)
- Alle Interpunktionen im Satz

Beispiel 2: Zufällig 6-8 Wörter aus dem Wörterbuch nehmen

- Wörter aneinander reihen
- Mit bestimmtem Zeichen verbinden

Empfehlungen

- Passwortmanager verwenden
  - Passwörter sicher & zufällig generieren und abspeichern
  - Praktische eingebaute Lösungen im Browser (Firefox, Chrome, Safari)
  - Separate Programme, z.B. KeepassXC, Bitwarden, …
  - Gut überlegen: Will ich die Daten in der Cloud haben?
  - Sichere “Ablage“ des Hauptpassworts
  - Backup der Daten haben (z.B. wenn ich das Telefon verliere)
- 2-Faktor-Authentisierung (2FA) aktivieren
  - 2FA: Neben Wissen wird etwas von einem Gerät im Besitz abgefragt (→ nur das Passwort reicht nicht für Angriff)
  - Häufig: TOTP-Verfahren (Apps: FreeOTP, Google Authenticator, …)
  - 2FA: Zustellung per Mail / SMS vermeiden (kann ggfs. abgehört werden)
  - Herausforderung: Phishing bleibt möglich – aber sicherer als nur ein Passwort zu haben
  - Backup-Codes sichern!
- Passkeys verwenden
  - Nutzen Sicherheitstechniken des Geräts (z.B. Fingerabdruck, FaceID…)
  - Verhindern

Empfehlungen

- Passwortmanager verwenden
  - Passwörter sicher & zufällig generieren und abspeichern
  - Praktische eingebaute Lösungen im Browser (Firefox, Chrome, Safari)
  - Separate Programme, z.B. KeepassXC, Bitwarden, …
  - Gut überlegen: Will ich die Daten in der Cloud haben?
  - Sichere “Ablage“ des Hauptpassworts
  - Backup der Daten haben (z.B. wenn ich das Telefon verliere)

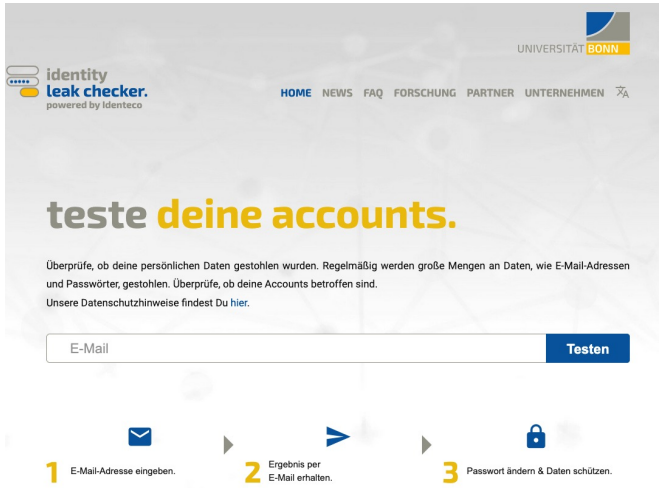
- 2-Faktor-Authentisierung (2FA) aktivieren
  - 2FA: Neben Wissen wird etwas von einem Gerät im Besitz abgefragt (→ nur das Passwort reicht nicht für Angriff)
  - Häufig: TOTP-Verfahren (Apps: FreeOTP, Google Authenticator, …)
  - 2FA: Zustellung per Mail / SMS vermeiden (kann ggfs. abgehört werden)
  - Herausforderung: Phishing bleibt möglich – aber sicherer als nur ein Passwort zu haben
  - Backup-Codes sichern!

Empfehlungen (Forts.)

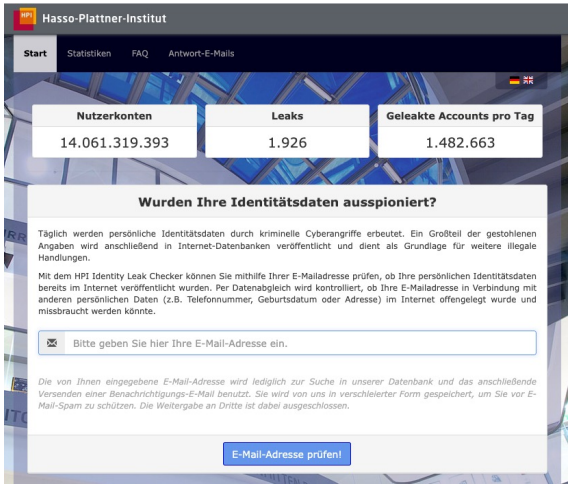
- Passkeys verwenden
  - Nutzen Sicherheitstechniken des Geräts (z.B. Fingerabdruck, FaceID…)
  - Verhindern Phishing und funktionieren nur auf der „echten“ Webseite
  - Details beschreibt z.B. das BSI unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html

Identitätsdiebstahl

- Es gibt verschiedene Dienste, um herauszufinden, ob persönliche Daten / Passwörter offengelegt worden sind.
- Im Fall der Fälle: Betroffene Zugangsdaten sofort ändern, ggfs. weitere Maßnahmen ergreifen!
- Gute Übersicht: Cybersicherheitslotse des Bundesamts für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html



https://leakchecker.uni-bonn.de/de/index



https://sec.hpi.de/ilc/

Take-Home Message

- Minimum: Kreative, gute und möglichst zufällige Passwörter wählen
- Besser: Passwort-Manager ausprobieren / verwenden
- 2-Faktor-Authentifizierung verwenden (vor allem bei höheren Sicherheitsanforderungen)
- Ggfs. Passkeys ausprobieren

Ansprechpartner:

informationssicherheit@tu-freiberg.de

https://tu-freiberg.de/informationssicherheit

Servicedesk: 03731 / 39 - 1818

Rückfragen zum Vortrag:

Prof. Dr. Bastian Pfleging

bastian.pfleging@informatik.tu-freiberg.de

License