



Online-Account schützen

Sichere Passwörter und Zwei-Faktor-Authentisierung

Inhalt

- ① Schutz ist sinnvoll!
- ② Die Sache mit den Passwörtern
- ③ sichere Passwörter
- ④ kürzeres und komplexes Passwort
- ⑤ langes und weniger komplexes Passwort
- ⑥ Brute Force
- ⑦ Empfehlung für Passwörter
- ⑧ Anmelden ohne Passwort mit Passkey
- ⑨ Weitere Infos

Schutz der digitalen Identität

- **das Haus verlassen -» Haustür
abschließen**

hallo Datendieb
ser 12345
sicher passw
.345 Passwort
passwOrt unsicher
Angriff Hacker

Schutz der digitalen Identität

- **das Haus verlassen -» Haustür abschließen**
- **ins Auto steigen -» Sicherheitsgurt anlegen**

hallo Datendieb
ser 12345
sicher passw
345 Passwort
passwOrt unsicher
Angriff Hacker 1234

Schutz der digitalen Identität

- **das Haus verlassen -» Haustür abschließen**
- **ins Auto steigen -» Sicherheitsgurt anlegen**
- **aus Auto aussteigen -» Auto abschließen**

hallo Datendieb
ser 12345
sicher passw
345 Passwort
passwOrt unsicher
Angriff Hacker 1234

Schutz der digitalen Identität

- das Haus verlassen -» Haustür abschließen
- ins Auto steigen -» Sicherheitsgurt anlegen
- aus Auto aussteigen -» Auto abschließen
- online gehen -» ??

hallo Datendieb
ser 12345
sicher passw
345 Passwort
passwOrt unsicher
Angriff Hacker 1234

Schutz der digitalen Identität

- das Haus verlassen -» Haustür abschließen
- ins Auto steigen -» Sicherheitsgurt anlegen
- aus Auto aussteigen -» Auto abschließen
- online gehen -» ??
- **Sicheres Passwort benutzen!**

hallo Datendieb
12345
sicher passw
passwOrt unsicher
Angriff Hacker

Die Sache mit den Passwörtern

hallo Datendieb
ser 12345
sicher passw
passwOrt unsicher
Angriff Hacker

Wer kennt es nicht?

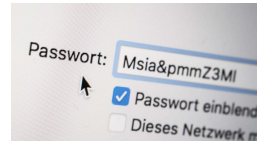
- Du willst einen Dienst im Internet nur kurz nutzen
- schon wird eine Anmeldung erbeten
- Du klickst dich zügig durch den Anmeldevorgang
- akzeptierst die AGB
- dann kommt die Frage nach dem Passwort – mal mit, mal ohne konkrete Vorgaben.

Hier sollte immer Sicherheit vor Schnelligkeit gehen!

Tips für sichere Passwörter

Du hast zwei Strategien zur Erstellung eines sicheren Passworts:

- kürzeres und komplexes Passwort (mindestens 10 Zeichen aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen)
- langes und weniger komplexes Passwort (mindestens 25 Zeichen, nur zwei Zeichenarten)



kürzeres und komplexes Passwort

Man denkt sich einen Satz aus und benutzt von jedem Wort nur den ersten Buchstaben (oder nur den zweiten oder den letzten). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen.



Hier ein Beispiel: **Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang.**

Nur die ersten Buchstaben: **'MsiaupmmZdMI'.**

'i' und 'l' sehen aus wie '1', '&' ersetzt das 'und': **'Ms1apmmZ3M1'.**

Es ist ratsam, dass Du dir als Benutzerin oder Benutzer des Passwortes den Satz selbst ausgedacht hast. Wird als Merksatz zum Beispiel ein bekanntes Literaturzitat oder eine Liedzeile als Passwort gewählt, so ist es wahrscheinlicher, dass Angreifer dies auch herausfinden können.

langes und weniger komplexes Passwort

elster-erlauben-geben-jemand-pendel
 KaffeeLieblingsTasseFruehling
 Frau_Gazelle_Korken_Tundra_Verrueckt
 1BlauerHundLaeuftDurchKasse1
 Sonne!Kaffee+Fruehstueck=Glueck
 MeinKollegeTrinktSeinTee=Um8

12 x RYA 5090 boryat (10)					
Passwortlänge (# Zeichen)	nur Zahlen	nur Kleinbuchstaben	Zahlen & Großbuchstaben	Zahlen und Klein- buchstaben	Zahlen, Klein- buchstaben, Groß- buchstaben und Symbole
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	17 Minuten	2 Stunden	4 Stunden
6	Sofort	46 Minuten	2 Tage	6 Tage	2 Wochen
7	Sofort	20 Stunden	4 Monate	1 Jahr	2 Jahre
8	Sofort	3 Wochen	10 Jahre	62 Jahre	164 Jahre
9	2 Stunden	2 Jahre	791 Jahre	36 Jahre	79 Jahre
10	1 Tag	40 Jahre	476 Jahre	2284 Jahre	6536 Jahre
11	1 Woche	16 Jahre	3460 Jahre	18 Mio Jahre	52 Mio Jahre
12	3 Monate	276 Jahre	101 Mio Jahre	507 Mio Jahre	2 Mio Jahre
13	6 Jahre	2504 Jahre	5 Mio Jahre	56 Mio Jahre	275 Mio Jahre
14	10 Jahre	50 Mio Jahre	350 Mio Jahre	9 Mio Jahre	18 Mio Jahre
15	261 Jahre	697 Mio Jahre	16 Mio Jahre	218 Mio Jahre	1 Bio Jahre
16	36 Jahre	12 Mio Jahre	812 Bio Jahre	13 Bio Jahre	94 Bio Jahre
17	216 Jahre	312 Mio Jahre	42 Bio Jahre	840 Bio Jahre	6 Tris Jahre
18	2666 Jahre	8 Bio Jahre	2 Tris Jahre	52 Tris Jahre	463 Tris Jahre

Das sind sechs Beispiele für lange Passwörter, sog. **Passphrasen**. Sie sollen mindestens 25 Zeichen lang sein und aus zwei Zeichengruppen stammen.

Passwort knacken mit brutaler Gewalt

2020

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

Passwort knacken mit brutaler Gewalt

2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Passwort knacken mit brutaler Gewalt

2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Empfehlung für Passwörter

- **Länge ist entscheidend:** Nimm mindestens 12 Zeichen, idealerweise 16 oder mehr.
- **Vielfalt ist wichtig:** Verwende eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- **Vermeide persönliche Informationen:** Verwenden Sie keine Namen, Geburtstage, Adressen oder andere leicht zu erratende Informationen.
- **Nutze einen Passwort-Manager:** Verwende einen seriösen Passwort-Manager, um starke, zufällige Passwörter zu generieren und sicher zu speichern.
- **Aktiviere die Zwei-Faktor-Authentifizierung (2FA):** 2FA bietet eine zusätzliche Sicherheitsebene, selbst wenn Dein Passwort kompromittiert wird.
- **Aktualisiere Deine Passwörter regelmäßig:** Ändere die Passwörter regelmäßig, insbesondere für wichtige Konten wie E-Mail, Bankgeschäfte und soziale Medien.
- **Passphrasen:** Anstatt ein komplexes, zufälliges Passwort zu verwenden, kann eine lange und zufällige Passphrase verwendet werden. Eine Passphrase ist einfach ein Satz, der leicht zu merken ist, aber für einen Computer schwer zu knacken ist.

Passkey - Nutzen

Passkeys sind der gewöhnlichen Anmeldung mit Benutzernamen und Passwort in vielerlei Hinsicht überlegen:

- **Passkeys können nicht zu simpel oder zu kurz sein** – Passwörter dagegen schon.
- **Passkeys können im Gegensatz zu Passwörtern nicht vergessen werden.**
- **Passkeys werden schnell und automatisiert erstellt.**
- **Es ist unwahrscheinlicher, dass Passkeys durch Phishing oder Datendiebstahl verloren gehen.**
- **Jeder Passkey schützt immer genau einen Account** – so können nie mehrere Accounts gefährdet sein, sollte ein Passkey missbraucht werden.
- **Diensteanbieter muss den Login ermöglichen** - Anmeldung per Passkey im entsprechenden Account einrichten
- **Dein eigene Gerät hinterlegt einen geheimen und einen öffentlichen Schlüssel im eigenen Speicher**; der Onlinedienst bekommt den öffentlichen Schlüssel
- **Diese Schlüssel sind die Grundlage für ein komplexes, kryptografisches Verfahren, das ab der Registrierung bei jeder Anmeldung von Dir unbemerkt abläuft.**

Weitere Infos

BSI-Basischutz Sichere Passwörter: <https://tinyurl.com/28lcts9p>

BSI-Passwörter Schritt für Schritt merken: <https://tinyurl.com/yy848ygo>

Uni-Kassel: Passkeys: <https://tinyurl.com/2ay8sobp>

Passwortgenerator (deutsch): <https://generate-random.org/passphrases/de>

Am ersten Montag im Monat im Gebäude der Verbandsgemeinde Pellenz in
Plaidt: **Digi-Hilfe-Treff**

Alle Angaben im Vortrag vom BSI