



Jahreshauptversammlung des Bürgerverein
Krefeld-Gartenstadt 1958 e.V.

Tipps zum sicheren Umgang mit digitalen Medien

Was sind digitale Medien?

- Webseiten/Blogs
- Soziale Netzwerke (Instagram, Facebook, TikTok usw.)
- E-Mails & Messenger-Dienste (z. B. WhatsApp, Signal, Telegram)
- Streaming-Plattformen (z. B. YouTube, Netflix, Spotify)
- E-Books & digitale Zeitungen
- Videospiele
- Apps
- Online-Banking oder Online-Shops

Account absichern

1. Starke Passwörter verwenden

- kleine Buchstaben (z.B. t)
 - große Buchstaben (z.B. T)
 - Zahlen (z.B. 3)
 - Sonderzeichen (z.B. %)
 - mind. 12 Zeichen lang
 - Kein persönlicher Bezug (z.B. kein Name, Geburtsdatum, Haustier & Familie)
 - keine einfachen Passwörter (z.B. 123456, qwertz, password)
-
- Ideales Passwort: **G!7d@fT\$9xLm2#**
 - Passwort-Manager nutzen (z. B. Bitwarden)
 - Alternatives Passwort:
 - (Wir2Können0Auch2Einen5GanzenSatzNehmen)

Top Ten deutscher Passwörter 2023:

1. 123456789

6. password

2. 12345678

7. password1

3. hallo

8. target123

4. 1234567890

9. iloveyou

5. 1234567

10. gwer123

Zeit zum knacken eines Passwortes

Nutzung von Groß- Kleinbuchstaben, Ziffern & 10 Sonderzeichen (72 verschiedene Zeichen)

Möchten Sie sich lange Passwörter nicht merken, dann kann Ihnen der Einsatz von Sonderzeichen, wie _ - + : * ; / & ! % helfen.

Rechengeschwindigkeit des Rechners (2147483600 Schlüssel pro Sekunde (Keys/sec))

Passwortlänge in Zeichen	Mögliche Kombinationen	Anzahl der maximal benötigten Zeit				
		in Sekunden	sind x Minuten	sind x Stunden	sind x Tage	sind x Jahre
1	72	3.352761343555779e-8				
2	5184	0.0000024139881673601606				
3	373248	0.00017380714804993155				
4	26873856	0.012514114659595073				
5	1934917632	0.9010162554908452				
6	139314069504	65	1.08			
7	10030613004288	4671	77.85	1.30		
8	722204136308736	336303	5605.04	93.42	3.89	
9	51998697814228990	24213781	403563.02	6726.05	280.25	
10	3743906242624487400	1743392239	29056537.32	484275.62	20178.15	55.28
11	269561249468963100000	125524241242	2092070687.36	34867844.79	1452826.87	3980.35
12	1.9408409961765343e+22	9037745369401	150629089490.02	2510484824.83	104603534.37	286585.03
13	1.3974055172471047e+24	650717666596897	10845294443281.62	180754907388.03	7531454474.50	20634121.85
14	1.0061319724179154e+26	46851671994976600	780861199916276.60	13014353331937.95	542264722164.08	1485656773.05
15	7.244150201408991e+27	3373320383638315500	56222006393971930.00	937033439899532.10	39043059995813.85	106967287659.76

Die Werte stellen eine optimale Sicherheit dar. Dass heißt, es wird davon ausgegangen, dass die richtige Kombination erst mit der letzten Kombinationsmöglichkeit gefunden wird.

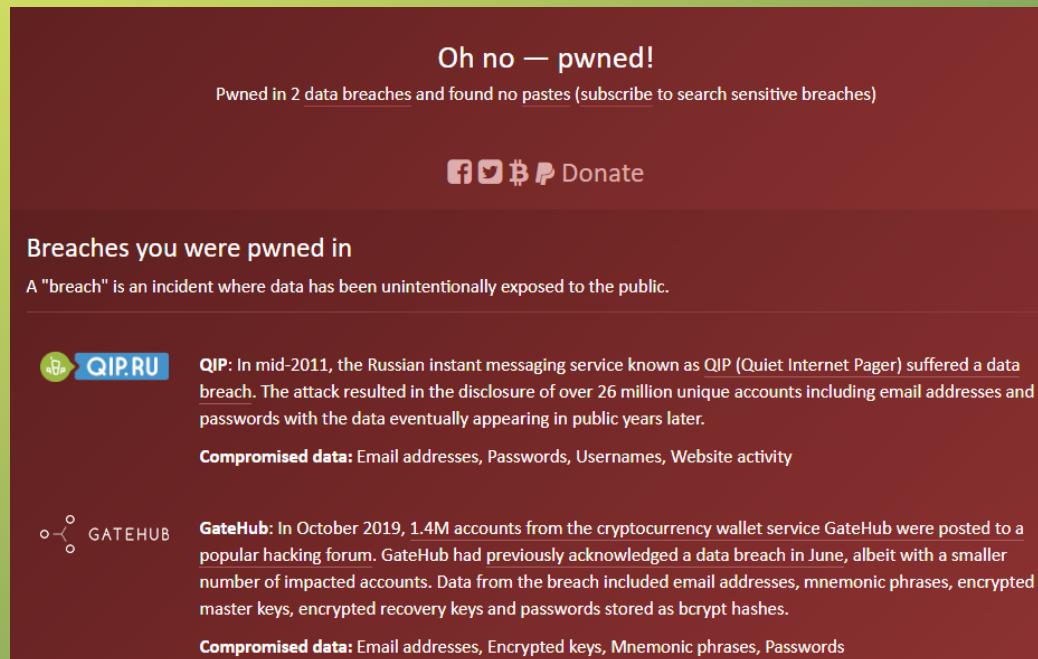
Account absichern (Teil 2)

2. Zwei-Faktor-Authentifizierung (2FA)

- Code über SMS
- TOTP (Zeitbasiertes Einmalpasswort) über eine App (z.B. Google Authenticator)

3. Für jede Anwendung ein anderes Passwort

4. Prüfe, ob E-Mail Adresse bereits geleakt wurde: <https://haveibeenpwned.com>



Oh no — pwned!

Pwned in 2 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

[f](#) [t](#) [v](#) [b](#) [p](#) [p](#) Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

	QIP: In mid-2011, the Russian instant messaging service known as QIP (Quiet Internet Pager) suffered a data breach. The attack resulted in the disclosure of over 26 million unique accounts including email addresses and passwords with the data eventually appearing in public years later. Compromised data: Email addresses, Passwords, Usernames, Website activity
	GateHub: In October 2019, 1.4M accounts from the cryptocurrency wallet service GateHub were posted to a popular hacking forum. GateHub had previously acknowledged a data breach in June, albeit with a smaller number of impacted accounts. Data from the breach included email addresses, mnemonic phrases, encrypted master keys, encrypted recovery keys and passwords stored as bcrypt hashes. Compromised data: Email addresses, Encrypted keys, Mnemonic phrases, Passwords

Gefahren erkennen

- **Phishing: Stehlen von persönlichen Informationen**

- Versuch der Manipulation auf emotionaler Ebene. Etwa durch Drohungen, Neugier oder scheinbar persönliche Kontakte

Trifft ein...

per E-Mail

als SMS

als What'sApp-Nachricht

per Anruf

als Brief!!!!

- **Fake News erkennen**

- Quellen prüfen (<https://www.bundesregierung.de/breg-de/aktuelles/desinformation-erkennen-1750146>)
- Faktenchecks (<https://correctiv.org/faktencheck/>)

Persönliche Daten schützen

- **Was teile ich online?**
 - Fotos (Gefahr durch Missbrauch von Bildern)
 - Aufenthaltsorte (Diebe wissen, wann leichte Beute gemacht werden kann)
 - Kontakte (Persönlichen Bezug in z.B. Phishingmails herstellen)
 - Nachrichten (Persönlichen Bezug in z.B. Phishingmails herstellen)
- **Einstellungen zur Privatsphäre prüfen**
- **Einstellungen zum Datenschutz prüfen**
- **Auf Fremdsystemen immer nach Verlassen „Abmelden“**
- **Das Internet vergisst nicht!**

Zusammenfassung

- **Starke Passwörter mit mind. 12 Zeichen + 2FA nutzen**
- **Mehrere Passwörter für verschiedene Dienste nutzen**
- **Unerwartete Nachrichten, welche meine Neugier wecken oder mich unter Druck setzen, besonders hinterfragen**
- **Weniger ist mehr: Daten im Internet sparsam teilen**
- **Meldet euch nach Benutzung der Online-Dienste ab**

Ich wurde gehackt, was jetzt?

1. Passwort sofort ändern!

- Starkes Passwort + 2FA einrichten

2. Passwort auch für andere Konten ändern, wenn es ebenfalls woanders verwendet wird!

3. Alle bestehenden Anmeldungen am Onlinedienst trennen

4. Prüfe PC/Smartphone mit Antivirus-/Antimalware-Programm

5. Informiere Familie & Freunde über mögliche Phishing-Versuche

6. Achte die nächsten Wochen auf verdächtige Transaktionen

7. Ggf. die Polizei informieren

- z.B. in Fällen von Identitätsdiebstahl, Betrug oder unbefugte finanzielle Transaktionen

**Vielen Dank für die
Aufmerksamkeit!**