Wie sicher ist mein Passwort? Typische Fehler & worauf Sie achten sollten

Erfahren Sie hier, wie sicher Ihr Passwort ist und was Sie alles tun können, um die Sicherheit zu verbessern.

Ganz gleich ob bei der täglichen Arbeit oder dem Spaziergang durch das Internet: Für den Datenschutz und die Sicherheit Ihrer Privatsphäre kommen Sie um die Vergabe von Passwörtern in der digitalen Welt nicht herum. **Häufig basieren diese allerdings auf persönlichen Daten** wie Geburtstagen oder dem Namen des Haustieres. Das macht es Hackern besonders einfach, sich Zugang zu verschaffen. **In diesem Beitrag verraten wir Ihnen, wie Sie ein starkes Passwort erstellen** und wo Sie online überprüfen können, wie sicher dieses ist.

- ✔ Für das Knacken eines fünfstelligen Passwortes brauchen geübte Hacker weniger als 20 Minuten.
- ✔ Cyberkriminelle erschleichen sich Ihr Vertrauen um an persönliche Informationen zu gelangen.
- ✔ Sensible Accounts wie Online-Banking-Zugänge oder Administratoren-Logins erfordern ein besonders sicheres Passwort.

Inhalt [Ausblenden]

1. So gehen Cyberkriminelle vor, um Passwörter zu stehlen

So stellen sich die meisten Menschen einen Hacker vor.

Beim Begriff „Hacker“ haben die meisten zuallererst das Bild eines Computer-Nerds im Kopf, der mithilfe von Viren oder Trojanern die

Passwörter Ihres Rechners knackt. Auch die gängige Methode, sich diese mittels täuschend echt aussehender Phishing-Mails zu erschleichen, ist keine Unbekannte. **Doch es müssen nicht zwangsläufig immer Sicherheitslücken oder Schadcode sein**:

Immer mehr Cyberkriminelle nutzen inzwischen auch das sogenannte **Social Engineering**, **um Informationen über Sie zu sammeln** und dadurch Rückschlüsse auf Ihre Kennwörter zu ziehen. Dabei verleiten die Täter Ihr Opfer **zur Preisgabe sensibler Informationen**, indem Sie sich Ihr Vertrauen erschleichen und an menschliche Eigenschaften wie Angst oder Hilfsbereitschaft appellieren.

2. Tipps, wie Sie ein sicheres Passwort erstellen

Ein gutes Passwort sollte aus möglichst vielen Zeichen bestehen. Acht Zeichen gelten als Minimum, nach oben hin ist die Grenze offen. Grundsätzlich gilt: **Je länger das Kennwort ist, desto sicherer ist es auch**. Bei WLAN-Kennwörter dürfen es daher auch gerne einmal 20 Zeichen oder mehr sein. Bedenken Sie dabei aber, dass Sie es auch das ein oder andere Mal wieder eingeben müssen.

In dieser Liste finden Sie hilfreiche **Tipps und Tricks für die Erstellung eines sicheren Passwortes**:

- Ihr Kennwort sollte **mindestens acht Zeichen haben** und möglichst aus mehr als einem Wort bestehen.
- Ein **absolutes No-Go bei Passwörtern** sind „echte“ Wörter und Begriffe (die so auch im Duden zu finden wären) sowie das Geburtsdatum und Namen. Auch **sämtliche Abwandlungen des Wortes „Passwort“** (zum Beispiel „P$$w0rt“ oder „P@sswor!“) sollten Sie tunlichst vermeiden.
- Verwenden Sie **Groß- und Kleinbuchstaben, Zahlen und möglichst viele Sonderzeichen** wie #, ?, * oder % und mischen Sie diese gut durch.
- Vermeiden Sie Umlaute (ä, ö, ü), da diese **vor allem bei fremdsprachigen Angeboten** zu Problemen führen können.
- Verwenden Sie **keine Tastaturmuster („qwertz“), Palindrome („Reliefpfeiler“) oder Wiederholungen**.

> **Manchmal kommt es eben doch auf die Länge an:** Für das Knacken eines 8-stelliges Passwort, bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, brauchen moderne Computer mehrere Monate. Mit jedem zusätzlichen Zeichen steigt die Sicherheit.
> **Zum Vergleich**: Für 15 Stellen werden rund 30 Jahre benötigt.

Trotzdem führen erschreckenderweise immer noch **einfache Zahlenkombinationen und Wörter** die weltweiten Passwort-Hitlisten an:

`12345`	`qwertz`	`passwort`	`01.01.1980`
`111login111`	`22222`	`hallo`	`bello123`

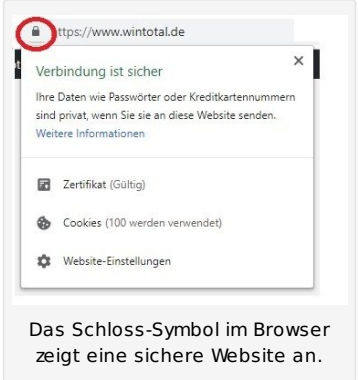
sind beispielsweise beliebte Kennwörter, für deren Entschlüsselung es **keine großen Hacking-Künste** braucht.

3. Tipps und Tricks für die sichere Verwendung von Passwörtern

Einen hundertprozentigen Schutz vor Datenklau gibt es natürlich auch bei besonders sicheren Passwörtern nie. Mit den folgenden **Tipps & Tricks** können Sie **es potenziellen Dieben aber dennoch um einiges schwerer machen**:

- Verwenden Sie grundsätzlich **für alle Ihre Dienste und Accounts unterschiedliche Passwörter**. So stellen Sie sicher, dass der Hacker im Falle eines Erfolges nicht gleich auf alle Ihre Daten zugreifen kann.
- **Legen Sie Passwörter niemals frei zugänglich ab** (bekanntestes Negativ-Beispiel: der Merkzettel unter der Tastatur) und nutzen Sie bei mehreren oder besonders komplexen Kennwörtern alternativ lieber einen Passwort-Safe.

> **Tipp:** Wenn Sie sich Kennwörter generell schlecht merken können, bauen Sie sich eine Eselsbrücke zur Unterstützung: Aus dem Satz „**I**ch **e**sse **s**onntags **g**erne **z**wei **S**tück **Z**itronenkuchen**!**“ wird so beispielsweise **Iesg2SZ!**.



Das Schloss-Symbol im Browser zeigt eine sichere Website an.

- Nutzen Sie im Internet nur **Webseiten, die eine SSL-Verschlüsselung verwenden**. Das Schloss-Symbol zeigt in Ihrem Browser die sichere Verbindung an. Die meisten Browser weisen Sie aber auch noch einmal extra daraufhin, wenn Sie **eine unsichere Seite betreten**.

- Viele große Internet-Dienste wie Google, Amazon oder Facebook schützen Ihre Accounts bereits mit der sogenannten **Zwei-Faktor-Authentisierung (2FA)**: Dabei loggen Sie sich wie gewohnt mit Ihrem Benutzernamen und Kennwort ein und bekommen Ihm Anschluss **eine (meist) sechsstellige PIN an Ihr Smartphone** oder Handy gesendet. Erst nach deren Eingabe wird der endgültige Zugriff gewährt.
- Deaktivieren Sie das **Speichern von Kennwörtern im Browser**. Die Daten sind zwar verschlüsselt abgelegt und, beispielsweise in Opera oder Firefox, **mit einem zusätzlichen Master-Passwort gesichert**, für die meisten Keyword-Breaker stellt das aber dennoch kein allzu großes Hindernis dar.

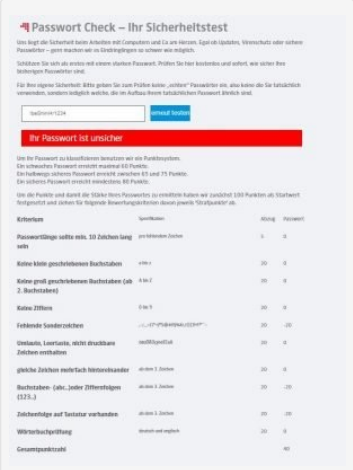
3.1. Grundsätzlich gilt: Trauen Sie niemandem!

- **Seien sie generell misstrauisch**, wenn Sie im Internet von Personen kontaktiert werden, die Sie nicht persönlich kennen und geben Sie so wenig persönliche Informationen wie möglich preis.
- Schauen Sie auch **bei vermeintlich seriösen Emails** lieber noch einmal genauer hin und antworten **mit einer neuen Nachricht** anstatt den „Antwort-Button“ zu benutzen. Wenn Sie in einer Email **zur Eingabe von Login-Daten aufgefordert** werden, sollten ohnehin sämtliche Alarmglocken bei Ihnen schrillen.

4. Online-Check: Wie sicher ist ihr Passwort?

Im Netz gibt es eine **Vielzahl von Portalen, bei denen Sie Ihre Passwörter auf die Sicherheit hin überprüfen** lassen können. Allerdings gilt auch hier: Vorsicht ist besser als Nachsicht, denn **wie überall sonst gibt es auch hier schwarze Schafe**, die genau das Gegenteil bewirken möchten: Nämlich Ihre Login-Daten stehlen! Um auf Nummer sicher zu gehen, sollten Sie daher **möglichst auch nur ein Passwort checken, welches Sie nicht mehr aktiv verwenden**.

Wir haben zwei **seriöse Anbieter unter die Lupe genommen** und die wichtigsten Merkmale für Sie zusammengefasst.



Password Check zeigt im Detail, wo die Schwächen Ihres Kennwortes liegen.

4.1. PC112 Passwort Check – Ihr Passwort im Detail

Das Internetportal PC112 (ehemals PC-Feuerwehr) bietet auf seiner Homepage einen kostenlosen Check an. Dazu müssen Sie lediglich **die Seite des Anbieters aufrufen** und Ihr gewähltes Passwort eingeben.

Im Anschluss erhalten Sie **sofort eine Auswertung zu Ihrem Passwort-Sicherheitstest**: rot bedeutet „unsicher“, bei gelb gibt es noch Verbesserungspotential und grün steht für „sehr sicher“.

Darunter wird detailliert aufgeschlüsselt, woran es „hapert“: Gestartet wird mit 100 Punkten, für jedes nicht vorhandene Kriterium (beispielsweise Sonderzeichen oder Ziffern) gibt es Punktabzug. **Je höher die Gesamtpunktzahl am Ende ausfällt**, **desto sicherer ist auch das Passwort**. Sie sollten in jedem Fall aber mindestens 80 Punkte erreichen.

4.2. Pwned Passwords – Sind Sie etwa schon drin?

Mit dem Web-Tool Pwned Passwords des australischen Sicherheitsforschers Troy Hunt können Sie ü**berprüfen, ob Ihr gewähltes Passwort in der Vergangenheit schon einmal gehackt oder gestohlen wurde**. Bei einem Treffer sollten Sie es schleunigst ändern, damit Sie nicht zum **Opfer eines Brute-Force-Angriffes** werden können.

Mit Pwned Passwords können Sie herausfinden, ob Ihr Kennwort in der Vergangenheit schon einmal gehackt wurde.

Für den Abgleich stehen mehr als eine halbe Milliarde Datensätze aus diversen Datenlecks zur Verfügung, in denen Sie nach geknackten Kennwörtern und Mailadressen suchen können. Auch SHA1-Hashes von Passwörtern können über den Dienst abgefragt werden.

Achtung: Sollte Ihr Passwort in Pwned Passwords nicht gefunden wird, bedeutet das nicht automatisch, dass es auch sicher ist.

32 Bewertungen

Ø 4,47

Ähnliche Artikel:

- USB-Stick-Schlüssel: Die bequeme Art, Ihren PC zu schützen
- Sicherheit im Heimnetzwerk – so schützen Sie Ihren…
- Sicher bezahlen im Internet: Die besten…
- Keine Lücken in der Sicherheit – Penetration-Test
- Hacking Tools: Mit dieser legalen Software kommen…
- McAfee Test 2018: Was kann die Total Protection Suite?

Weitere Rubriken:	Internet & Kommunikation, Schädlinge, Sonstiges
Plattformen:	Windows 10, Windows 7, Windows 8.x
Eingetragen am:	26.02.2019
Aktionen:	Aktionen

Please upgrade to a supported browser to get a reCAPTCHA challenge.

Why is this happening to me?