Passwortsicherheit

Hier erfährst du:

- Warum Passworte eine Grundlage von Datensicherheit darstellen.
- Wie du sichere Passworte erfinden oder erstellen lassen kannst.
- Wie du dir Passworte merken kannst.
- Welche Programme dir bei der Passwortsicherheit helfen könne.
- Tipps zur Zwei-Faktor-Authentifizierung von Online-Konten

Passwörter dienen dazu, eure Daten zu schützen. Sie schützen eure Emails vor unbefugtem Zugriff, sie schützen eure Dateien auf dem Computer, sie schützen eure Festplatte davor, von den Repressionsbehörden entschlüsselt zu werden und sie schützen eure Accounts, die oft auch Hinweise auf weitere Accounts enthalten. Passwörter schützen euch, sie schützen eure Freund:innen und sie schützen unsere Zusammenhänge!

Dieser ganze Schutz wird zunichte gemacht, wenn ihr mit den Passwörtern nicht verantwortungsbewusst umgeht.

Ein empfehlenswerter Artikel zu **Passwortsicherheit vom Kuketz-Blog**

Grundlegende Sicherheitsmaßnahmen

Pro Login ein eigenes Passwort
Jedes Gerät, jede Festplatte, jeder Account, jedes Netzwerk wird mit je einem eigenen Passwort gesichert! Wenn ein Passwort gestohlen oder geknackt wird, ist nicht gleich alles im Eimer.
Wählt sichere Passwörter und ändert sie immer mal wieder
Profile auf sozialen Netzwerken sind dankbare Quellen, um an Passworthinweise zu gelangen (Name des Haustiers, Zitat der Lieblingsband oder Zitat der Lieblingsrevolutionär_in). Auf keinen Fall sollten Standardkombinationen wie «12345», «admin» oder der Name des Netzwerks gewählt werden. Passwort-Knack-Programme können zudem mit Hilfe von Wörterbüchern oder dem Internet alles mögliche ausprobieren: Also alles was irgendwo als Text steht - Zitate, etc. sind tabu!. Passworte sind deine erste und meist einzige Verteidigung gegen Zugriffsversuche! Wichtig ist, dass Passwörter ausreichend lang sind (**Passworte sollen aus mindestens 7 verschiedenen Wörtern bestehen**). Die Länge ist auch wichtiger, als Sonderzeichen oder Zahlen zu verwenden. Außerdem sollten die Passwörter immer mal wieder geändert werden.
Benutze einen Passwort-Tresor
Die vielen komplizierten Passwörter kann man sich oft nicht mehr merken. Passwörter sollten aber dennoch auf keinen Fall unverschlüsselt irgendwo aufgeschrieben werden. Eine sichere Lösung zur Aufbewahrung eurer Passwörter bietet ein Passwort-Tresor. Diese Programme funktionieren wie ein Tresor im eigenen Computer oder Smartphone, in dem die Passwörter für die verschiedenen Dienste sicher abgelegt werden können. Der Passwort-Tresor hilft zudem beim Generieren von zufälligen Passwörtern und sorgt damit mit wenigen Klicks für ausreichend komplexe Passwörter. Dann braucht ihr euch nur wenige lange und gute Passworte merken und den Rest könnt ihr im Passwort-Tresor erstellen und gespeichert haben. Weiter unten im Artikel findet ihr dazu eine Empfehlung von uns.
Verwendet keine biometrischen Daten als Passwort
Abhilfe im Passwortdschungel sollen auch biometrische Daten – unsere Stimme, Fingerabdruck oder Gesicht – schaffen. Sie versprechen Bequemlichkeit, sind aber gefährlich. Denn einmal gehackt,

lassen sich Gesichter und Fingerabdrücke nicht einfach austauschen. Außerdem wird ihre Sicherheit auch auf technischer Ebene immer wieder in Frage gestellt. Darum: Lass es und verwende Passwort-Tresore!!

Anleitungen zur Passwortsicherheit

Wir empfehlen ein Programm zu nutzen, das eure Passwörter für verschiedene Accounts verschlüsselt speichert und ein ultra-sicheres Passwort für den Zugriff auf den Passwort-Tresor. Denn keine:r kann sich alle Passworte für jeden Account merken.

Mit 3 Passworten bestens abgesichert

- Ich merke mir ein sicheres Passwort für die **Festplattenverschlüsselung** meines Computers.
- Ich merke mir ein zweites sicheres Passwort oder eine lange PIN für die Verschlüsselung meines **Smartphones**.
- Ich merke mir ein drittes sicheres Passwort für den **Passwort-Tresor**. Damit habe ich Zugriff auf alle weiteren Passwörter.

Im folgenden Abschnitt stellen wir verschiedenen Systeme vor, die beim Erstellen und Merken von sicheren Passworten helfen können.

Passworte sicher abspeichern - Passworte-Tresor

Ein Passwort-Tresor speichert deine Passworte und legt sie verschlüsselt ab. Zudem kann ein solcher auch zufällige Passworte und Passphrasen generieren - das ist sicherer als wenn du dir ständig neue Passworte ausdenkst. Geschützt wird der Passwort-Tresor mit einer sicheren Passphrase die du dir merken musst. Wie bei fast allem was du verlierst oder vergisst: Wenn du dein Passwort nicht mehr weisst, sind deine Passworte im Passwort-Tresor nicht mehr zugänglich. Ebenso gilt: Wenn du keine Sicherungskopie (Backup) von deinem Passwort-Tresor hast oder dein Computer kaputt geht oder abhanden kommt, hast du keinen Zugriff mehr auf die Passworte.

Wir empfehlen den KeePass XC Passwort-Tresor. Er funktioniert auf Linux, Windows, MAC und deinem Handy.

Anleitung zum Programm:
Passwortmanagement erklärt by Kuketz-Blog

Kurzanleitung:
⇒ Installiere KeePass XC
⇒ Erstelle im Programm eine „Neue Datenbank“ und wähle aus, wo du diese abspeichern möchtest. Es wird eine einzelne Datei am gewünschten Ort abgelegt: das ist deine verschlüsselte Passwort-Datenbank.
⇒ Setze eine sichere Passphrase, die du auswendig lernst!! Bedenke: Wenn du es wo aufschreibst, kann jemand damit Zugriff auf alle deine gespeicherten Zugänge bekommen.
⇒ Nun kannst du mit „Neuen Eintrag hinzufügen“ Einträge anlegen: Die Webseite für das Passwort, die Nutzer:Innen-Daten und das Passwort angeben oder noch besser generieren lassen (mit dem Würfel-Symbol).
⇒ Sichere deine Datenbank regelmäßig. Dazu öffnest du den Passwort-Tresor und gehst auf Datenbank→Datenbank speichern unter

Passwort-Tresor am Handy und PC
Du kannst deine Passwort-Tresor-Datei auch auf einen unverschlüsselten USB-Stick oder in einen Cloud-Ordner speichern. Das Gute ist, deine Passworte liegen sicher im Tresor - Zugang ist nur möglich über dein Passwort-Tresor-Passwort, das ja nur du kennst. Wichtig ist, dass du deine Passwort-Tresor-Datei nur auf Computern öffnest, denen du vertraust.

Passworte leicht merken

Einzelne Worte sind leichter zu merken als willkürliche Anordnung von Zeichen und Buchstaben. Dein Gehirn tut sich besonders leicht, wenn das Passwort eine Geschichte ergibt. Mit der sogenannten Diceware-Methode werden mehrere zufällige Wörter ausgewählt, die dann die das Passwort (bzw. die „Passphrase“) bilden. Das passiert mit einem klassischen Würfel mit den Zahlen 1-6 und einer Wortliste. Du nimmst dir also eine zur Verfügung gestellte Wortliste und erwürfelst dir quasi dein Passwort. Noch leichter geht es mit deinem Passwort-Tresor: Dort kannst dir solche Passworte auch einfach erstellen lassen, dann sind sie besonders willkürlich und damit sicher.

Der Passwort-Tresor spuckt dir folgende Worte aus:

```
perfume late diagnosis fragrance issue froth manifesto
```

Zum leichten Merken überlege ich mir mit diesen Schlüsselworten eine Geschichte:
„*I put on my favorite **perfume**. Very **late** I made my **diagnosis** of the **fragrance**: It has an **issue** with **froth** which was not mentioned in the communist **manifesto***.“

Die Geschichte muss überhaupt keinen Sinn ergeben. Das Gute ist: Das ist deinem Gehirn egal, sie hilft trotzdem ungemein beim merken.

Du kannst als Füllzeichen auch Varianten erstellen:
perfume!late!diagnosis!fragrance!issue!froth!manifesto!
oder
PerfumeLateDiagnosisFragranceIssueFrothManifesto, usw.

Variationen, Sprachen und Tipps:

- Diceware Erklärung auf Wikipedia
- Diceware Wortlisten gibt es in verschiedenen Sprachen, du kannst dich also austoben!
- Englischsprachige Anleitung zum Erstellen der Passphrase.
- Passphrasen-Generatoren erstellen und speichern Diceware-Passwörter für dich.

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung bedeutet, dass du für den Zugriff zu einer Webseite oder einen Account zwei verschiedene Schlüssel benötigst, die aus unterschiedlicher Quelle kommen. Du verwendest im Alltag vermutlich schon länger diese Sicherheitstechnologie: Für die Behebung von Bargeld am Geldautomaten benötigst du 1. (d)eine Bankkarte und 2. den dazugehörigen geheimen PIN – nur wenn du gleichzeitig im Besitz von beiden Schlüsseln bist, kommst du an das Geld auf (d)einem Konto.

Was ist jetzt mit der Sicherheit durch das „gute alte Passwort“? Die meisten Online-Accounts sind ja durch ein User*innen-Name und ein Passwort geschützt. Wobei der User*innen-Name oft kein

Geheimnis darstellt: Oft ist es die Emailadresse und diese meist öffentlich bekannt. Dann bleibt das hoffentlich sehr starke und sehr gut geschützte Passwort. Aber auch hier gibt es genug erfolgreiche Attacken. Es schadet also nicht neben dem nur dir bekannten geheimen Passwort noch eine zweite geheime Sicherheitsebene einzuziehen.

Richtig verwendet kann 2-Faktor-Authentifizierung die Zugriffssicherheit massiv erhöhen. Wichtig ist, dass du nur weil du einen 2ten Faktor hast, nicht deinen 1sten Faktor schwach wählst - es gilt also weiterhin ein starkes und sicheres Passwort zu verwenden!

Zwei-Faktor-Authentifzierung geht natürlich nur dort wo es auch technisch vorgesehen ist. Aber vom Google-Konto über deine Banking-App bis zur Zustellung deines Covid-PCR-Testergebnisses wird es immer mehr angewandt. Gerade auch Emailkonten oder Cloud-Services können oft freiwillig über die Zwei-Faktor-Authentifizierung gesichert werden. So bietet etwa auch das linke Tech-Kollektiv und emanzipatorischer Dienste-Anbieter Systemli die Möglichkeit von Zwei-Faktor-Authentifizierung an.

Software Schlüssel
Oft ist der „zweite Faktor“ - also der zweite Schlüsselteil - eine Authentifizierungsapp auf deinem Smartphone.

Authentifizerungsapps gibt es viele, wir stellen dir hier das free-and-open-Source App andOTP für Android-Telefone vor. Du bekommst es im Appstore deiner Wahl!

1. App installieren (am besten auf deinem ohnehin verschlüsselten Smartphone)
2. Passwort/PIN für die App einrichten
3. Den jeweiligen Anleitungen des Accountes (z.B. Systemli) für die Einrichtung der Zwei-Wege-Verschlüsselung folgen. Mit der App muss dann meist ein QR-Code gescannt sein.
4. **Backup in der App** machen. Das ist wichtig, damit du den Zugriff wiederherstellen kann, wenn dein Handy kaputt oder verloren geht. andOTP bietet eine verschlüsselte Datensicherung – damit kannst du sie sicher auf deinen PC/Festplatte/USB-Stick/Cloud kopieren und aufbewahren. Wähle ein sicheres Passwort und verwende am Besten (d)einen Passworte-Tesor!

Hardware Schlüssel

Neben deinem Passwort kannst du auch einen Hardware-Schlüssel wie den Yubi-Key einsetzen. Der zweite Weg ist quasi ein USB-Stick den du an den Computer oder das Handy anstecken musst um Zugang zu erhalten.

So ein Yubi-Key muss gekauft werden – kostet also Geld. Und du benötigst gleich zwei davon, damit du im Fall des Verlustes nicht ausgesperrt bist aus deinen Accounts.

Auf der Seite von Yubi-Key findest du ausführliche Informationen dazu.

Zum Weiterlesen

Passwortmanagement erklärt by Kuketz-Blog

Zwei-Faktor-Authentifzierung erklärt im Systemli-Wiki

Ausführlicher und gut verständliches „Erklärstück“ zur Zwei-Faktor-Authentifizierung in der

Tageszeitung Der Standard: