

PASSWÖRTER MERKEN ADÉ: RICHTEN SIE SICH MIT UNS IHREN EIGENEN PASSWORTMANAGER EIN

Eine effiziente IT-Sicherung beginnt mit sicheren Passwörtern. Als Schlüssel schützen Sie nämlich nicht nur den eigenen Computer, sondern oft auch das Unternehmensnetzwerk und viele Dienste im Internet. **Wie Sie immer sichere Passwörter auswählen und sich diese nicht einmal selbst merken müssen, erfahren Sie hier!**



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

Beauftragt vom

Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen





ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN



WARUM SIND SICHERE PASSWÖRTER SO WICHTIG?

Passwörter sind wie ein Türschlüssel zu allen unseren Informationen. Sind Passwörter zu leicht gewählt und schnell zu erraten, können sich Kriminelle mit wenig Aufwand Zugriff auf die zu schützenden Daten verschaffen. Damit stehen ihnen für einen Identitätsdiebstahl oder einen Angriff auf Ihr Unternehmen Tür und Tor offen.

WARUM SIND NICHT ALLE PASSWÖRTER SICHERE PASSWÖRTER?

Für die Sicherheit eines Passworts sind die Länge und die Komplexität entscheidend. Passwörter sollten immer mindestens 13 Zeichen lang sein und aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Je länger das Passwort, desto schwieriger haben es Kriminelle, sich in Ihre Accounts einzuhacken.

WIE SICHERT IHR ANBIETER IHRE PASSWÖRTER?

Entscheidend ist, dass Online- oder Softwareanbieter Passwörter nicht im Klartext abspeichern, sondern *hashen*. Beim *hashen* werden Passwörter so transformiert, dass selbst der Anbieter Ihr Passwort nicht kennt. Nutzt Ihr Anbieter dieses Verfahren für Passwörter nicht, sind Passwörter in Gefahr. Durch Nachfragen können Sie Bewusstsein schaffen.



ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN

WARUM IST "EIN SICHERES PASSWORT FÜR MEHRERE DIENSTE" NICHT SICHER?

Schwachstelle Onlinedienst:

Wird ein Dienst gehackt und die Passwörter dort nicht *gehasht* – also unkenntlich gemacht und gesichert – sind alle Onlinedienste, bei denen dieses Passwort verwendet wird, in Gefahr.

Schwachstelle Mensch:

Wenn ein Endgerät gehackt wird, können Angreifer z.B. Tastatureingaben und damit auch Passwörter mitlesen.

Schwachstelle Passwort:

Angreifer können durch Hau-Drauf-Taktiken (*Brute-Force*, das Ausprobieren aller möglichen Zeichen-Kombinationen) Passwörter ermitteln. Je nach Länge und Komplexität des Passworts ist das mit vertretbarem Aufwand möglich.

WELCHE GEGENMASSNAHMEN GIBT ES ?

Passwortmanager (PWM) sind Programme, die Ihre Passwörter verschlüsselt und damit sicher aufbewahren. Man kann sich den PWM wie einen Tresor vorstellen, in dem alle Ihre Passwörter sicher abgelegt werden. PWM auch gleich sichere Passwörter, wenn Sie für einen neuen Dienst ein neues Passwort benötigen. Geschützt werden die im PWM gespeicherten Passwörter durch ein „Hauptpasswort“. Mit diesem öffnen Sie den Tresor, wenn Sie ein Passwort benötigen. Sie müssen sich somit lediglich das Hauptpasswort merken.

Passwortmanager sind für Passwörter deutlich sicherer als Zettel, Textdateien oder Browser. Es gibt verschiedene Programme wie beispielsweise KeepassXC, Keepass2, 1Password, Bitwarden, LastPass oder Enpass.

SICHERE PASSWÖRTER – EIN MUSS FÜR JEDEN!

Sichere Passwörter sind essenziell, wenn es um den Schutz von Daten geht. Sie gehören zur Grundvorsorge, um sich selbst und das eigene Unternehmen vor Hackerangriffen und einem Datendiebstahl zu schützen.

Wie Sie sich Ihren eigenen Passwortmanager einrichten, zeigen wir Ihnen Schritt für Schritt in unserer Videoanleitung, die Sie über den QR-Code erreichen!

Password:



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

Beauftragt vom

Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen



Erklärvideo – Passwortmanager