Sichere Passwörter im Team einfach organisieren

Montag, 22.06.2026
17:00 bis 18:30 Uhr
Online via Zoom

Tatjana Ljucović
DIGITAL.SICHER.NRW


Landesservicestelle
für bürgerschaftliches Engagement
Nordrhein-Westfalen
Wir stärken das Ehrenamt
in Nordrhein-Westfalen!
Landesservicestelle
für bürgerschaftliches Engagement
Ein Angebot für Engagierte, Initiativen
Vereine und Co.

Landesservicestelle für bürgerschaftliches Engagement Nordrhein-Westfalen

- Zentrale Anlaufstelle des Landes für Engagierte und zivilgesellschaftliche Organisationen
- Angebote:
  - Engagement-Portal engagiert-in-nrw.de
  - Boxenstopp fürs Ehrenamt: Wissen, Tipps und Austausch für Engagierte
  - Servicehotline und E-Mail-Beratung
  - Engagement-Newsletter
  - Facebook: @engagiertinnrw
  - Instagram: @engagiert_in_nrw

Landes-servicestelle

Engagement-Newsletter

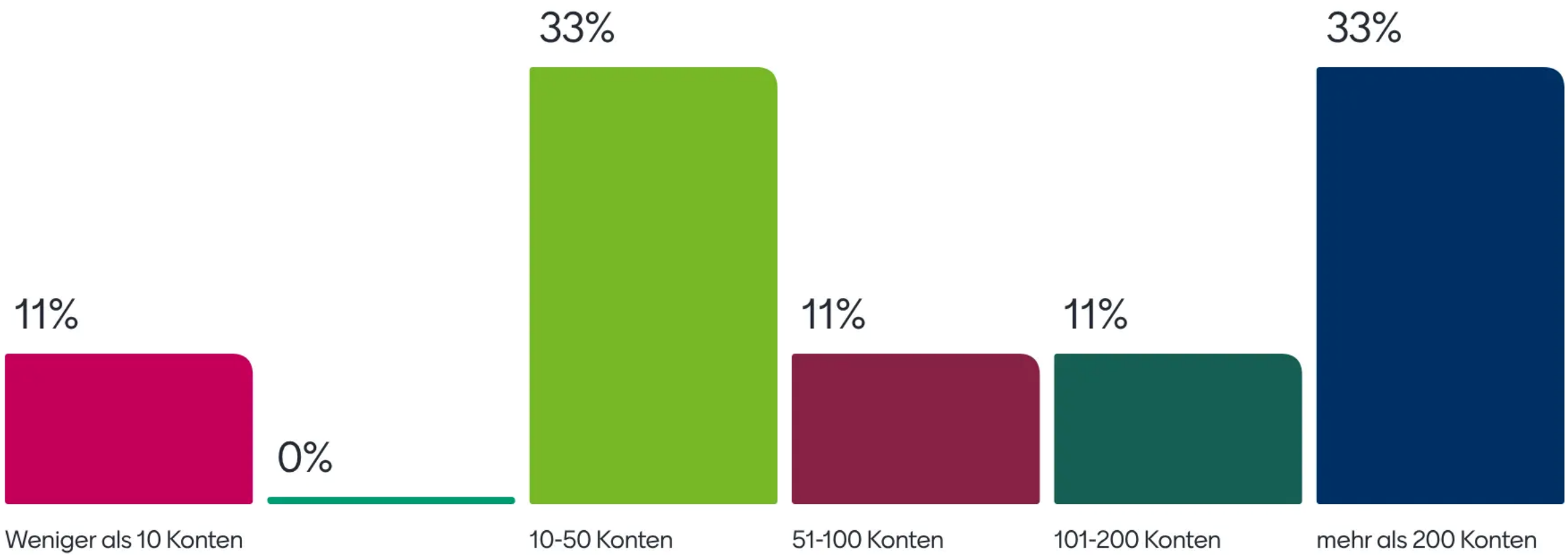
Engagement voranbringen

Online-Workshops zur Stärkung von Engagierten, Initiativen, Vereinen und Co.

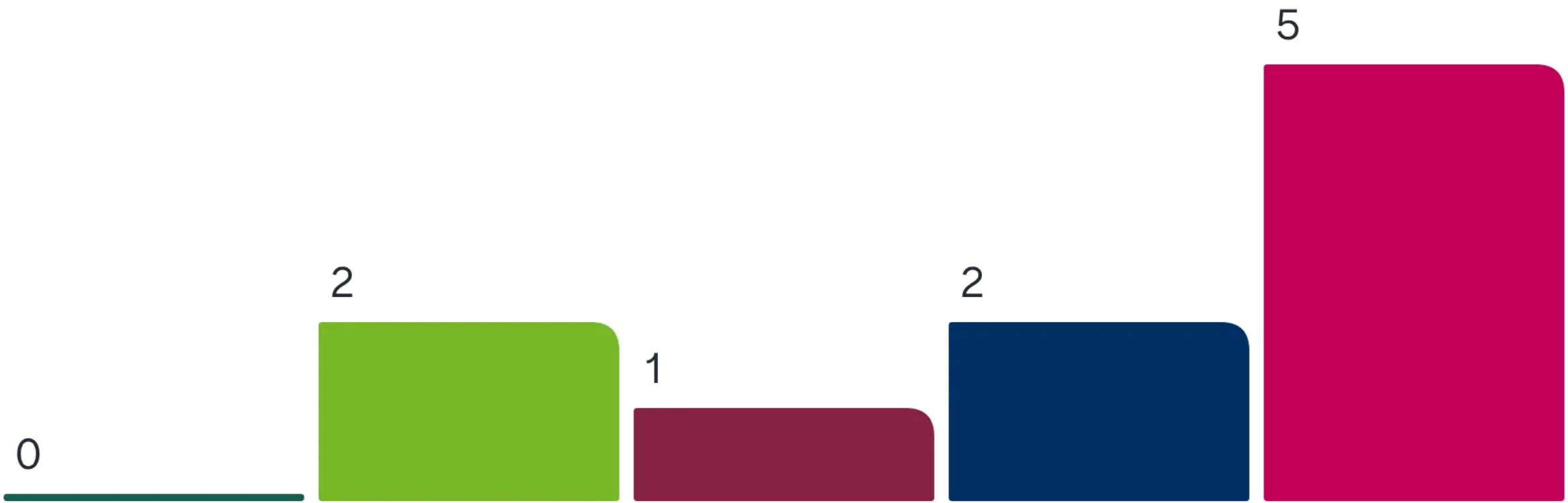
Zwei Fragen zum Start

- „Wie viele Konten hast du?“
- „Wie viele Passwörter hast du?“

Wie viele Konten hast du?



Wie viele Passwörter hast du?



Agenda

- Begrüßung
- **Teil I**
  - Sichere und unsichere Passwörter und Risiken
  - Moderierte Fragerunde
- **Teil II**
  - Werkzeuge für das Passwortmanagement
  - Moderierte Fragerunde
- **Teil III**
  - Passwörter im Team benutzen und verwalten
- Feedback und Abschied

Referentin

Tatjana Ljucović

Beraterin für digitale Sicherheit

DIGITAL.SICHER.NRW

DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

SICHERE PASSWÖRTER IM TEAM EINFACH ORGANISIEREN

Bochum, 22. Juni 2026

Beauftragt vom

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

KURZE VORSTELLUNG

- Master of Science in Internet-Sicherheit
- Mitarbeit in der Forschung zu sicheren Kommunikationslösungen für Unternehmen
- Tätigkeit im Bereich sichere Authentifizierung am Institut für Internet-Sicherheit
- Beraterin für digitale Sicherheit bei DIGITAL.SICHER.NRW

Tatjana Ljucovic

RISIKEN

RISIKO

Die häufigsten Fehler:

- schwache Passwörter
- dasselbe starke Passwort für viele Konten
- aufgeschrieben auf Zetteln oder in unverschlüsselten Excel-Listen
- im Team mündlich oder per Chat weitergegeben

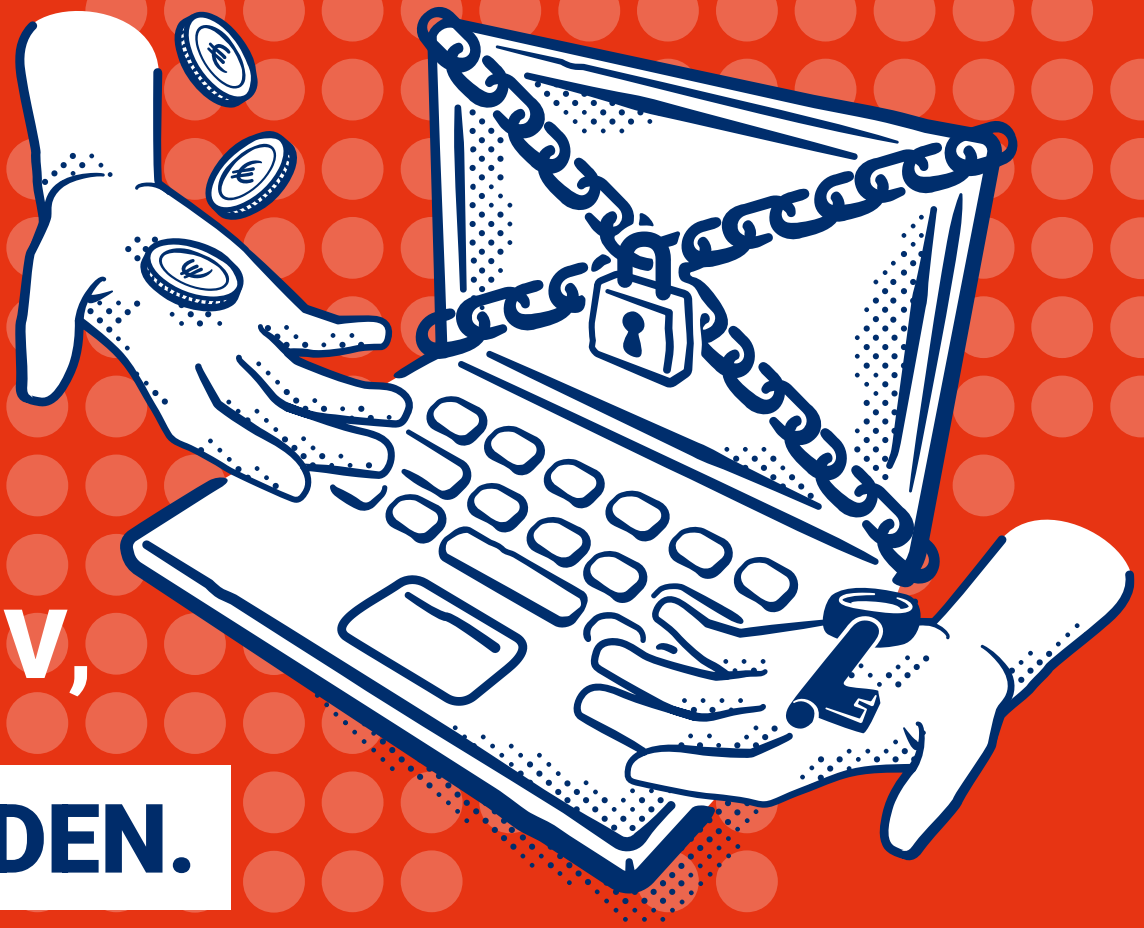
FOLGEN

- **Datenleck**: wenn Passwörter ins Netz gelangen
- Angreifende hacken einen Online-Dienst.
  → Millionen Logins werden gestohlen.
- Diese Listen werden im Internet verkauft oder veröffentlicht.
- Mit eurer alten E-Mail-Passwort-Kombination probieren Kriminelle automatisch andere Dienste durch.
  → Das nennt sich „Credential Stuffing".

KEIN UNTERNEHMEN IST

ZU JUNG,
ZU KLEIN,
ZU UNBEDEUTEND,
ZU UNATTRAKTIV,

UM ANGEGRIFFEN ZU WERDEN.



SELBST-CHECK

? Sind eure Daten schon im Netz?

! kostenlose Leak Checker:

- Leak Checker der Uni Bonn: **leakchecker.uni-bonn.de**
- Identity Leak Checker (HPI)**: sec.hpi.de/ilc**

! einfach E-Mail-Adresse eingeben → ihr seht, in welchen Leaks ihr auftaucht

UNSICHERE PASSWÖRTER

DIE TOP NINE PASSWÖRTER IN DEUTSCHLAND VON 2025

Quelle: https://hpi.de/artikel/hpi-veroeffentlcht-meist-geleakte-passwoerter-2025/

WIE LANG DAUERT ES EIN PASSWORT ZU KNACKEN?

Zeichenanzahl	nur numerisch	nur Kleinbuchstaben	Groß- und Kleinbuchstaben	Ziffern, Groß- und Kleinbuchstaben	Ziffern, Groß- und Kleinbuchstaben, Symbole
8	Sofort	30 Minuten	5 Tage	3 Wochen	2 Monate
12	2 Stunden	26 Jahre	107.000 Jahre	889.000 Jahre	3 Mio. Jahre
13	1 Tag	684 Jahre	5 Mio. Jahre	55 Mio. Jahre	267 Mio. Jahre
14	1 Woche	17.000 Jahre	291 Mio. Jahre	3 Mrd. Jahre	18 Mrd. Jahre
15	3 Monate	462.000 Jahre	15 Mrd. Jahre	212 Mrd. Jahre	1 Bio. Jahre
16	3 Jahre	12 Mio. Jahre	277 Mrd. Jahre	13 Bio. Jahre	91 Bio. Jahre
17	28 Jahre	312 Mio. Jahre	40 Bio. Jahre	815 Bio. Jahre	6 Brd. Jahre
18	276 Jahre	8 Mrd. Jahre	2 Brd. Jahre	50 Brd. Jahre	449 Brd. Jahre

Methode: Bruce-Force „durch Ausprobieren“, mit der Rechenleistung eines Rechners aus 2025

SELBST-CHECK

Diese Passwörter sind unsicher, auch wenn sie sich kompliziert anfühlen:

- Namen: Partner, Kinder, Haustier, Lieblingsstar
- Geburtsdaten oder Postleitzahlen
- Tastaturmuster: „qwertz“, „asdfgh“, „123abc“
- einfaches Wort mit „!“ oder „1“ am Ende wie „Sommer2024!“
- dasselbe Passwort für mehrere Dienste

SICHERE PASSWÖRTER

WIE SIEHT EIN SICHERES PASSWORT AUS?

- starken Merksatz bauen
  - Beispiel: vier zufällige Wörter + ein Trennzeichen
- 32 Zeichen lang
- schafft Bilder im Kopf
- für Hacker extrem schwer zu knacken
- **Wichtig:** Wörter wirklich zufällig wählen, kein Zitat oder Sprichwort

WIE SIEHT EIN SICHERES PASSWORT AUS?

Brötchen kaufe ich beim 7. Autobäcker meines Vertrauens.

oder

Bnkib7ArmVs.

WIE SIEHT EIN SICHERES PASSWORT AUS?

- zufällige Zeichen
- mindestens 13 Zeichen lang
- Kleinbuchstaben und Großbuchstaben
- Zahlen
- Sonderzeichen

PASSWÖRTER: DO‘S & DONT‘S

Dont‘s:

- Passwörter in Word-/Excel-Dokumente oder auf Post-Its
- Wiederverwendung oder Weitergabe
- regelmäßiges Ändern

Do‘s:

- Komplex ist gut, aber...
- je länger desto besser!
- Zwei-Faktor-Authentifizierung (2FA) nutzen

PASSWÖRTER IM BROWSER SPEICHERN

Superpraktisch, aber auch sicher?

Problem:

- Schwachstellen
- veraltete Software
- Drittpersonen
- leicht zu löschen
- schwach bis gar nicht verschlüsselt

Lieber:

- automatisches Speichern und Ausfüllen in den Browser-Einstellungen unterbinden
- sichere Alternative wie einen Passwortmanager nutzen

3. WERKZEUGE

DREI WERKZEUGE

drei Bausteine sicherer Anmeldung

- **Passwortmanager:** das Werkzeug für die Passwörter, die ihr noch braucht
- **Zwei-Faktor-Authentifizierung (2FA):** die zusätzliche Tür
- **Passkeys:** das, was Passwörter langsam ablöst

PASSWORTMANAGER

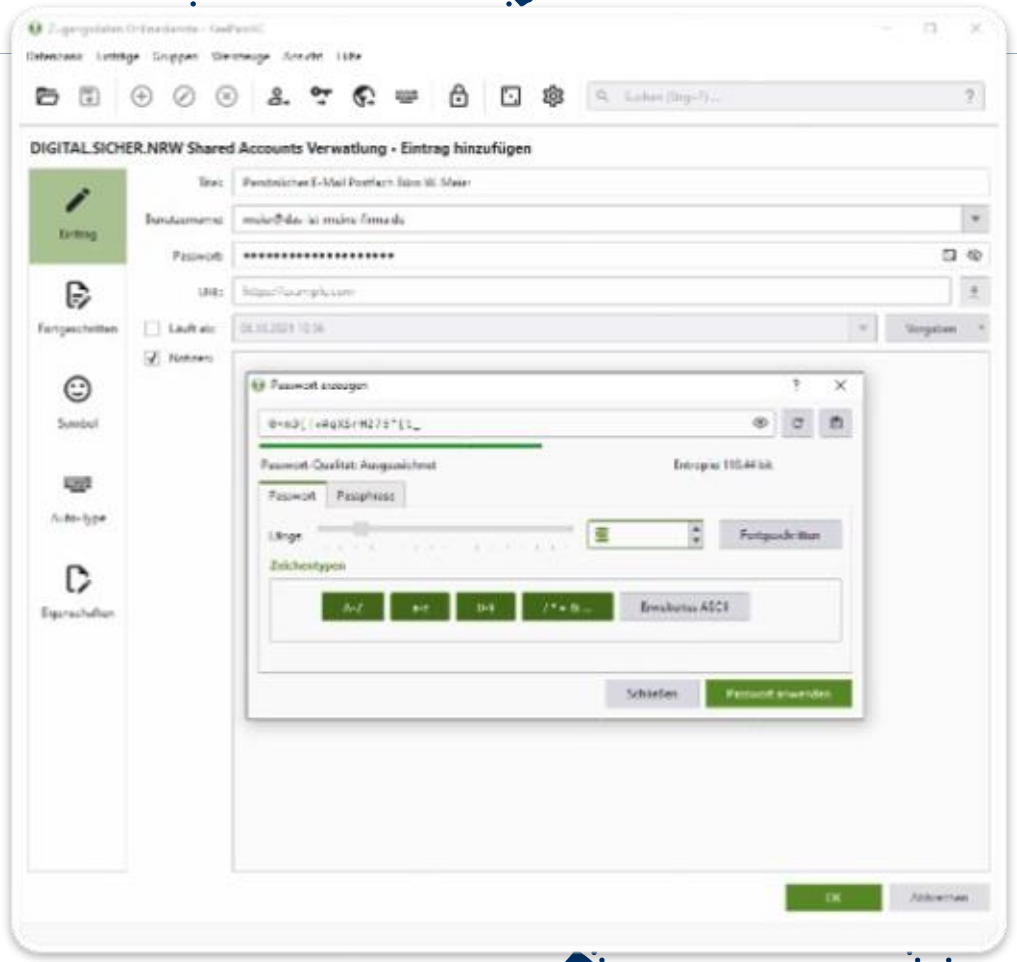
Superpraktisch und sicher!

Der Passwortmanager...

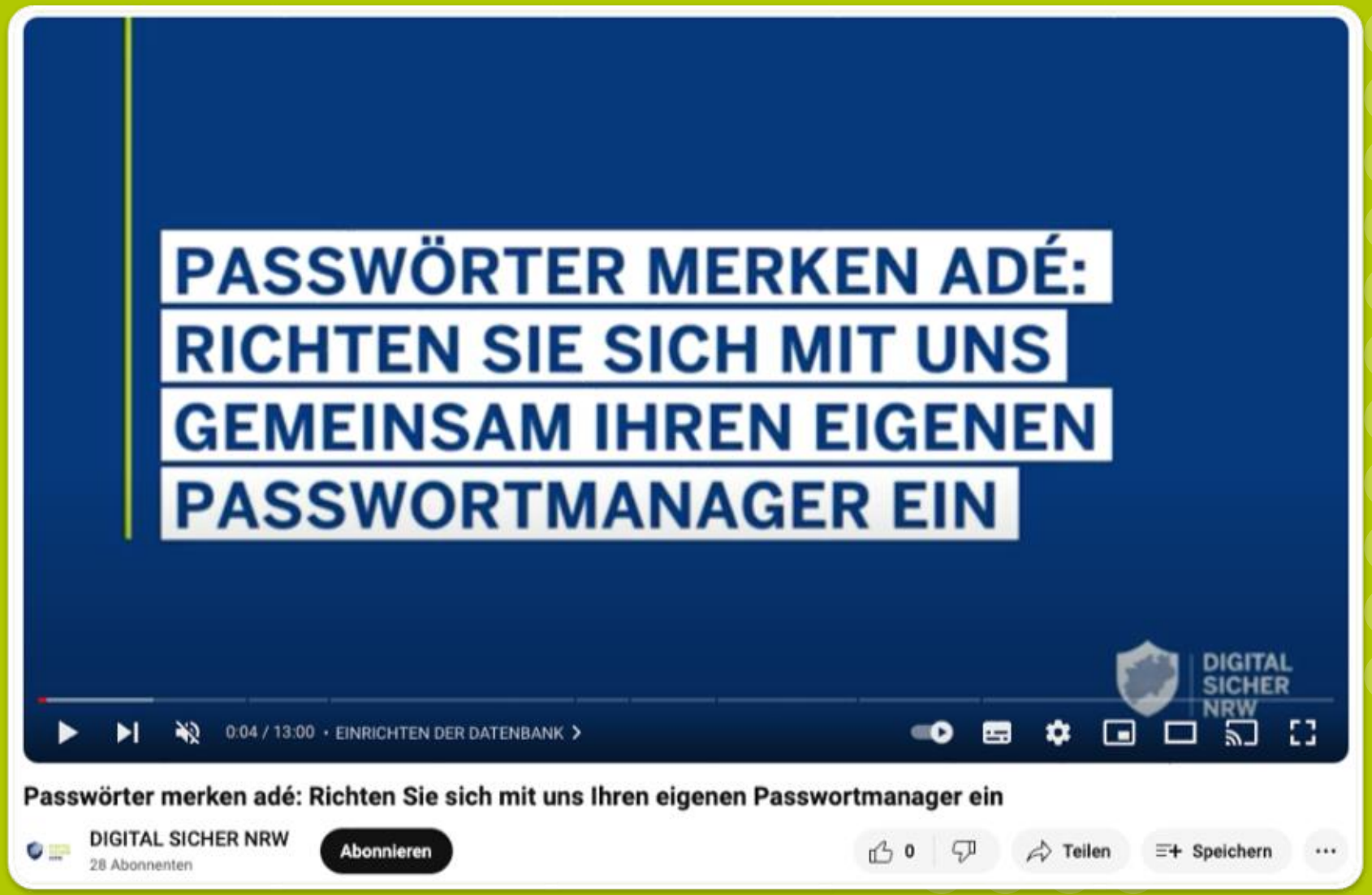
- kann Passwörter generieren,
- sie sich merken
- und verschlüsselt speichern.

Wichtig:

- sicheres Masterpasswort wählen
- Passwortdatenbank in Datensicherung aufnehmen



SCHRITT-FÜR-SCHRITT ANLEITUNG (KeePassXC)



-> https://youtu.be/boS-BpJEfM0?si=tOZFsMLfKC3a929K

YouTube

KeePassXC-Download:
https://keepassxc.org/

KRITERIEN: PASSWORTDATENBANK

Was einen guten Passwortmanager ausmacht

- **starke Verschlüsselung** (Stichwort: AES-256)
- **Zero-Knowledge-Prinzip:** selbst Anbietende können eure Daten nicht lesen
- **Zwei-Faktor-Authentifizierung** für den Passwortmanager selbst
- **funktioniert auf allen Geräten**, die ihr nutzt
- **Im Team:** Möglichkeit, Passwörter sicher zu teilen und Rechte zentral zu verwalten

ZWEI FAKTOR AUTHENTIFIZIERUNG

- **2FA:** die zweite Tür hinter dem Passwort
- So funktioniert es:
  - Ihr gebt euer Passwort ein (Wissen).
  - Ihr bestätigt zusätzlich mit etwas, das nur ihr habt: Code aus einer App, Hardware-Stick oder Fingerabdruck (Besitz oder Biometrie).
  - Selbst wenn euer Passwort gestohlen wird, kommt niemand rein.
  - **2FA überall aktivieren, wo der Dienst es anbietet.**

ZWEI FAKTOR AUTHENTIFIZIERUNG

- **Authenticator-Apps**
- **Hardware-Sicherheitsschlüssel (FIDO2/USB-Stick)**
- Push-Bestätigung in der App des Anbietenden
- **SMS-Code aufs Handy**

- **Tipp**: Hinterlegt wenn möglich zwei zweite Faktoren als Backup, falls ein Gerät verloren geht.

PASSKEYS

- Passkeys: die nächste Generation
- Login-Methode komplett ohne Passwort
- Ihr bestätigt einfach mit Fingerabdruck, Gesichtsscan oder Geräte-PIN.
- kein Passwort, das jemand stehlen kann
- immun gegen Phishing
- Zu kurz oder zu einfach gibt es nicht mehr.
- pro Konto ein eigener Passkey
- schon nutzbar bei: Google, Microsoft, Apple, Amazon, PayPal und vielen weiteren Diensten

IM TEAM

PASSWÖRTER IM TEAM

- Im Team wird es kompliziert.
- Typische Situationen:
  - Mehrere Personen brauchen Zugang zum Vereins-E-Mail-Konto.
  - Der Social-Media-Account wird von wechselnden Personen betreut.
  - Ein Mitglied verlässt das Team – wer ändert was?
  - Eine wichtige Person ist im Urlaub – wer hat den Zugang?

VIER REGELN IM TEAM

Vier Grundregeln für sichere Team-Zugänge

1. **geteilter Passwortmanager,** nicht WhatsApp oder Excel
2. **klare Rollen:** Wer darf was sehen und ändern?
3. **Onboarding & Offboarding:** feste Schritte beim Kommen und Gehen
4. **Notfallplan:** Wer kommt rein, wenn die Hauptperson ausfällt?

SO TEILST DU EINE PASSWORTDATENBANK

1. Datenbank-Datei z.B. über die Cloud oder einen Datenträger zur Verfügung stellen
2. Speichere das Passwort zum Entschlüsseln der gemeinsam genutzten Datenbank in deiner persönlichen Passwortdatenbank.
3. Vergewissere dich, dass das Passwort auf einem sicheren Weg übermittelt wird (z.B. über den Messenger „Signal“) .

VIER REGELN IM TEAM

Damit es nicht nach zwei Wochen einschläft:

- klein anfangen: eine Person macht den Anfang, baut den Manager auf
- Stück für Stück übertragen: die wichtigsten 5-10 Konten zuerst
- feste Person als Ansprechperson für Passwörter im Team benennen
- einmal im Jahr: alle Zugänge durchgehen, Karteileichen löschen
- bei Datenleck-Meldung: gezielt das betroffene Passwort ändern, kein Aktionismus

ZUSAMMENDFASSUNG

Was ihr mitnehmen solltet:

- starkes Passwort: komplex und lang
- Jedes Konto braucht ein eigenes, starkes Passwort.
- Passwortmanager nutzen – im Team gemeinsam mit Rollen
- 2FA aktivieren, wo immer es geht
- Passkeys nutzen, wo angeboten
- klein anfangen, dauerhaft pflegen, eine Person verantwortlich

PORTFOLIO: UNSERE ANGEBOTE

DIGITAL SICHER NRW

- Erstberatung
- IT-Sicherheitskompass
- Wissen
- Veranstaltungen
- Webinare
- Kooperationen

kostenfrei & produktneutral

www.digital-sicher.nrw

IT-SICHERHEITSKOMPASS

Schauen Sie unbedingt auf unserer Webseite vorbei oder sprechen Sie uns an!

www.digital-sicher.nrw

Grundregeln der IT-Sicherheit

Fast alle mittelständischen Unternehmen in Nordrhein-Westfalen haben sich in den letzten Jahren zunehmend digitalisiert. Das hat einerseits viele Arbeiten enorm erleichtert. Andererseits wurden so neue Angriffsflächen innerhalb von Unternehmen geschaffen. Diese zu schließen und sich vor einem Großteil digitaler Kriminalität zu schützen, ist für kleine und mittlere Unternehmen ein zentrales Zukunftsthema.

- Passwörter
- Passwortmanager
- Smartphones und Tablets
- Internet und Browser
- Spam und Anti-Virus
- Backups (Sicherheitskopien)
- Löschen und Zerstören
- Home-Office und mobiles Arbeiten
- Online-Shops
- Verschlüsselung

Newsletter,

stelle mir bitte regelmäßig Informationen und Veranstaltungen rund um das Thema digitale Sicherheit zusammen. Danke!

Melden Sie sich an,
um nichts mehr zu verpassen.

DIGITAL SICHER NRW

- **Ratgeber mit hilfreichen Tipps**
- **aktuelle Veranstaltungen**
- **Neues vom Kompetenzzentrum**

1 x monatlich

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

Die Grundlagen der digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer digitalen Daten.

Besuchen Sie unsere Website: www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

+49 234 - 5200 7334

info@digital-sicher.nrw

Social Media

DIGITAL SICHER NRW

CYBER SECURITY CLUSTER BONN

eurobits

Beauftragt durch

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

Eine Frage zum Schluss

- „Was nimmst du aus dem heutigen Online-Workshop mit?“

Was nimmst du aus dem heutigen Online-Workshop mit?

passwortmanager nutzen

anderen passwortmanager

passkeys

ab ins die umsetzung

kein one-fits-all

Nächste Veranstaltungen

Demokratie vor Ort gestalten und fördern
Dienstag, 23.06.2026, 17:00–18:15 Uhr

Ehrenamt als Nebentätigkeit
Mittwoch, 24.06.2026, 12:15–12:50 Uhr

Gemeinsam gegen Rassismus im Ehrenamt (Teil 2)
Donnerstag, 25.06.2026, 17:00–19:00 Uhr

Vereine digital organisieren: Wissen und Kommunikation
Montag, 29.06.2026, 17:00–18:30 Uhr

Digitale Mitgliederversammlung mit Online-Wahl
Mittwoch, 01.07.2026, 17:00–18:30 Uhr

Förderung von Projekten zur Gewaltprävention (CERV-Aktionsbereich Daphne)
Dienstag, 14.07.2026, 17:00–18:15 Uhr

Weiterführende Informationen

- Leak Checker der Uni Bonn: *https://leakchecker.uni-bonn.de/de/index*
- Identity Leak Checker (HPI): *https://sec.hpi.de/ilc/*

Soziale Medien

Wir sind auch in den sozialen Medien zu finden:

Facebook:
@engagiertinnrw

Instagram:
@engagiert_in_nrw