Skillsharing-Workshop

Wie verwalte ich
sicher, *nachhaltig* und *bequem*
meine Passwörter?

03.03.2021

Agenda

1. Passwörter
2. Was ist ein Passwortsafe?
3. Warum macht er mein Online-Leben sicherer, nachhaltiger und bequemer?
4. Los geht‘s 😀
5. Weitere Tipps

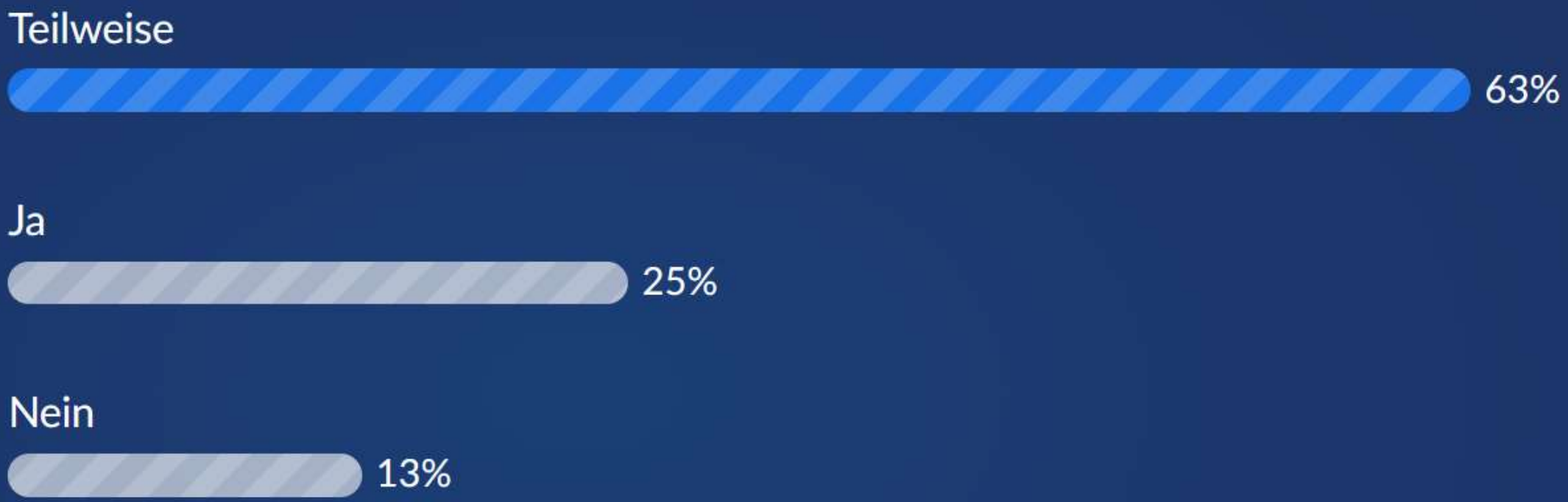
Was kommt dir in den Kopf, wenn du an „Passwörter“ denkst?

Aus wie vielen Zeichen bestehen i.d.R. deine Passwörter?

008

Nutzt du das exakt gleiche Passwort bei mehreren Online-Diensten?

008



Nutzt du einen Passwort-Safe? Wenn ja, welchen?

006

bidwarden

Nein

Nein :(

nein

Nein

Bitwarden

Wurde mein Passwort schon mal gestohlen?

008

Passwörter

Online Security Survey

Password reuse is still a common practice

52% reuse the same password for multiple (but not all) accounts

35% Use a different password for all accounts

13% Reuse the same password for all their accounts

ONLY 24% Use a password manager, despite many people saying they need a better way to track passwords

Quelle: https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Passwörter

Wurde mein Passwort schon mal gestolen?

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.
verifications.io	Feb. 2019	✓	763.002.527	–	–	–	–	–	–	–	–
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–	–	–
Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.											
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–	–	–
nexusmods.com	Dez. 2015	✓	5.918.307	Betroffen	–	–	–	–	–	–	–
kickstarter.com	Feb. 2014	✓	5.174.845	–	–	–	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–
last.fm	Jun. 2012	✓	39.329.766	Betroffen	–	–	–	–	–	–	–

Quelle: HPI Identify Leak Checker

Passwörter

Was sind (tatsächlich) wichtige Faktoren für sichere Passwörter? Was sind Mythen?

Regelmäßiger Wechsel?

(Sehr) Langes Passwort?

Viele Sonderzeichen?

Notieren mit Stift und Papier?

Kein persönlicher Bezug?

Alle müssen einmalig sein?

Verwendung eines Passwortsafes?

2-Faktor-Authentifizierung?

Biometrisches Passwort?

Passwörter

Empfehlungen vom Hasso-Plattner-Institut

- Lange Passwörter (> 15 Zeichen)
- Alle Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
- Verwendung von Passwortmanagern
- Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
- Zwei-Faktor-Authentifizierung aktivieren, wenn möglich

Quelle: https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html

Passwortsafe

Sicher, nachhaltig, bequem?

- ✓ Überall verschiedene, sehr sichere Passwörter

- ✓ „Passwort vergessen“ gibt es nicht mehr (es müssen nur 2-3 Passwörter gemerkt werden)
- ✓ Überblick über alle Accounts

- ✓ Automatisches Einfügen von Zugangsdaten
- ✓ Verfügbar auf allen Geräten

Passwortsafe

Nur für Passwörter?

- Passwörter
- WLAN-Schlüssel
- Nummern (z.B. Sozialversicherungsnummer, Mitgliedsnummern, etc.)
- Lizenzschlüssel
- Private Informationen
- …

Passwortsafe

Große Auswahl

Open Source & Locally stored

KeePass Password Safe

KEEPASSXC

Open Source & Self-Hosting

bitwarden

Closed Source & Cloud-Services

LastPass

1Password

NordPass

dashlane

Passwortsafe

KeePass

- ✓ Offener Standard + große Community + viele Open Source Implementierungen
- ✓ Lokale Speicherung → kein automatisches Hochladen zu irgendwelchen Servern
- ✓ KISS-Prinzip → einzelne Datei (Synchronisation wird anderen Tools überlassen)
- ✓ Es existieren Programme für Linux, MacOS und Windows, Apps für Android & iOS sowie Browser-Erweiterungen
- ✓ Viele Funktionalitäten & Anpassungsmöglichkeiten

KeePass

Kleine Auswahl an KeePass-kompatiblen Programmen / Apps

	Name	Kosten	Open Source	Browser-Integration	Anmerkungen
Windows	KeePassXC	-	ja	*KeePassXC-Browser**	
Linux	KeePassXC	-	ja	*KeePassXC-Browser**	
macOS	KeePassXC	-	ja	*KeePassXC-Browser**	
Android	KeePassDX / Keepass2Android	-	ja	-	
iOS	KeePassium (Free)	Free: 0 € Pro: 14,99 € p.a.	ja	-	• Mit TouchID • nur eine Datenbank
	Strongbox (Free)	Free: 0 € Pro: 13,49 $ p.a.	ja	-	• Ohne TouchID • mehr als eine Datenbank

*Erweiterung verfügbar für Google Chrome, Vivaldi, Brave, Mozilla Firefox, Microsoft Edge, Chromium

Erstellen eines sicheren Passworts

Merkhilfen

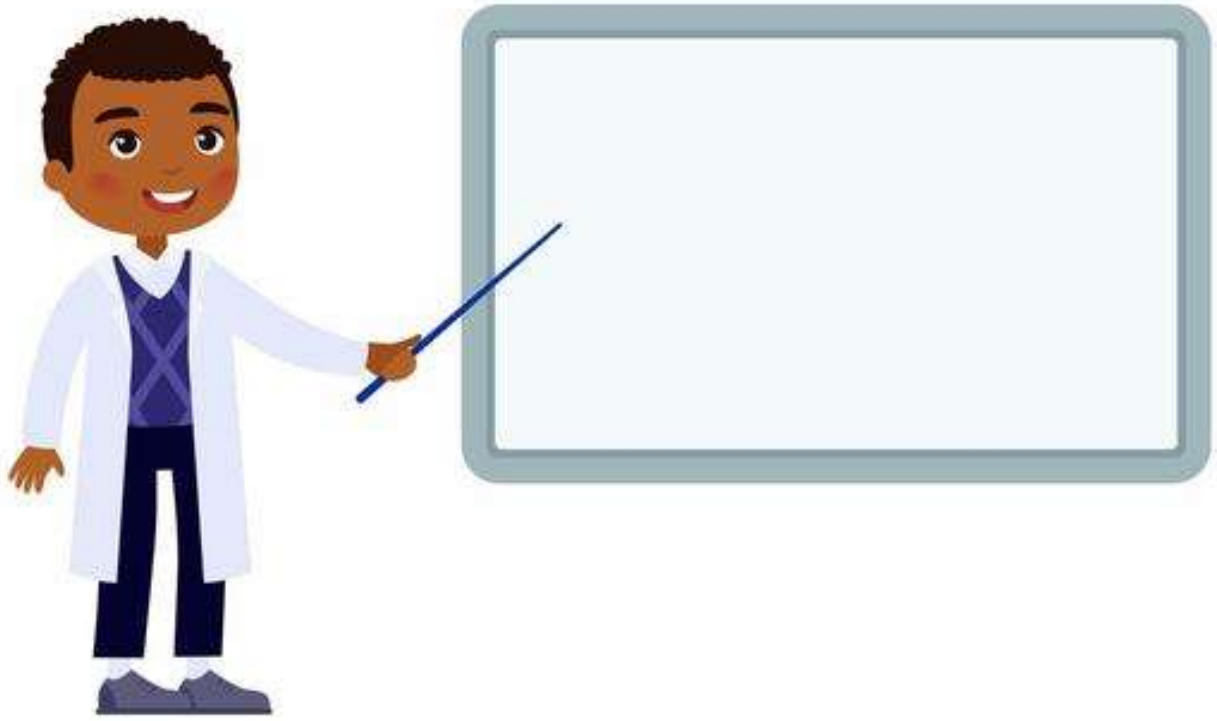
- **Leicht zu merkende Basis**: Sprichwort, persönlicher Satz, …

  Beispiel: „Hallo IT, ich habe mein Passwort vergessen ☹“
  → HIT,ihmPv:(

- **System**: Passwort wird aus Blöcken zusammengesetzt

  Beispiel: „x1C“ **+** Trenner **+** Abkürzung für Dienst **+** Trenner **+** Name
  → x1C&nWb&ppoK

Demo



Los geht‘s!

Einrichtung eines Passwortsafes

To-dos:

1. Passwortsafe installieren
2. Datenbank erstellen
3. Datenbank synchronisieren
4. Passwortgenerator verwenden
5. Browser-Integration einrichten
6. App auf Smartphone / Tablet einrichten

Fragen:

- Wer macht mit?
- Welches OS setzt ihr ein?
- Synchronisation mit mobilen Endgerät?

Getting Started Guide

KeePassXC: Getting Started Guide:

https://keepassxc.org/docs/KeePassXC_GettingStarted.html

03.03.2021

Weitere Hinweise

- Backup
  - Datenbank-Datei an verschiedenen physikalisch getrennten Orten speichern
  - Ausdruck auf Papier (nur dann, wenn du einen sehr sicheren Ort hast) → Paper Backup
- 2FA-Authentifizierung

Fragen / Probleme

David Kopp

Telegram: @davidkopp

Matrix: @dkopp:stuvus.de

E-Mail-Adresse: david.kopp@campusforfuture.de

Du hast es geschafft!