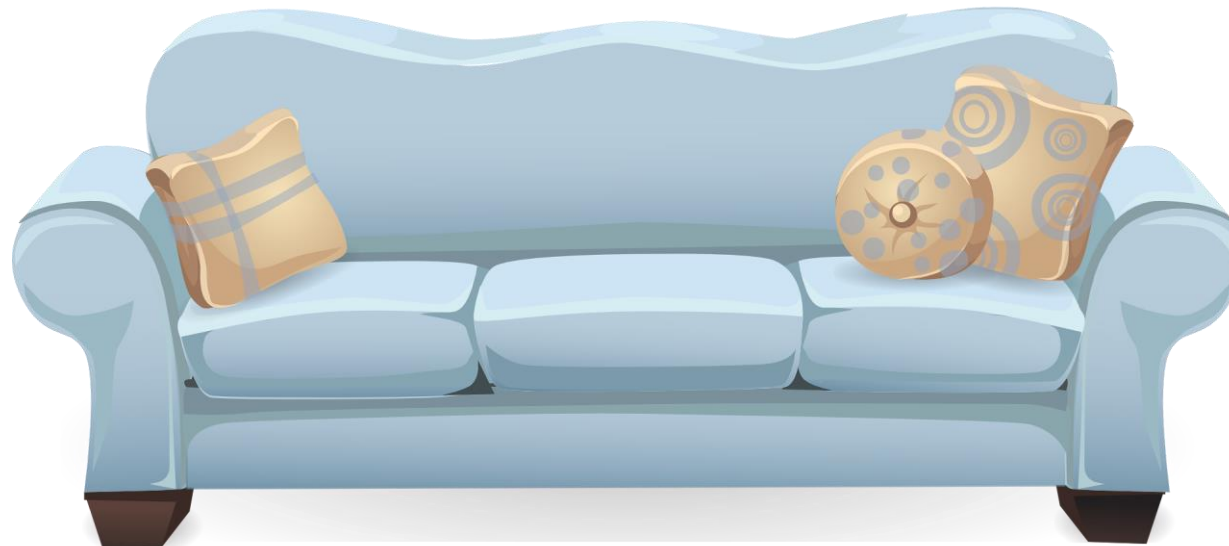
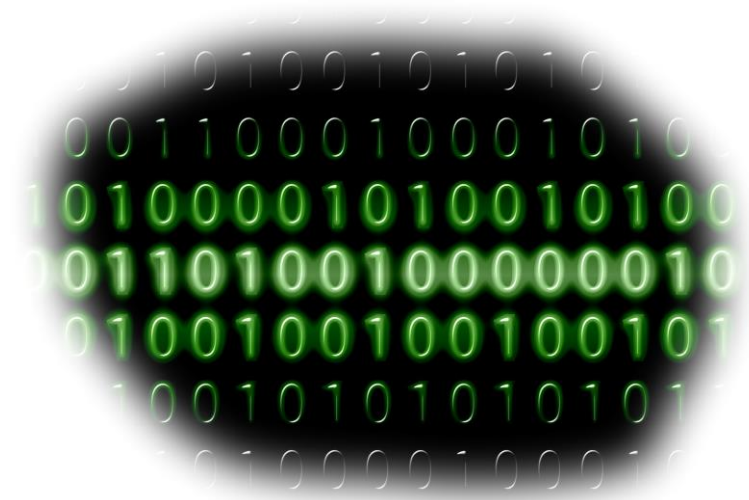


Digitales Sofa Johannesberg



Sichere Passwörter

Wofür brauche ich ein Passwort?

- Im Internet benötigt man ein Passwort zusammen mit einem Benutzernamen, um auf geschützte Bereiche einer Seite zuzugreifen:
 - Onlineshop
 - Onlinebanking
 - Verträge (z.B. Versicherungen)
 - Behörden (z.B. Finanzamt)
- Zugang zum E-Mail Postfach
- Anmeldung am Windows PC
 - Passwort ist optional
- Zugriff auf Smartphones
 - Ein Pin Code (Ziffernfolge) ersetzt hier das Passwort

Passwort vergeben

- Bei der Registrierung für einen Dienst (Onlineshop, E-Mail Postfach, usw.) muss ein Passwort vergeben werden
- In der Vergangenheit hat der Betreiber des Dienstes keine Vorgaben gemacht wie lange oder komplex das Passwort sein muss. Auch heute noch gibt es Anbieter, die einfache und kurze Passwörter zulassen
- Die beliebtesten Passwörter ⁽¹⁾:
 - 123456789, 12345678, 1234567890
 - password, password1
 - iloveyou
 - qwerty123

(1) Abhängig von der Methode wie die Statistik erstellt wird, gibt es andere Quellen, mit anderen Top Passwörtern

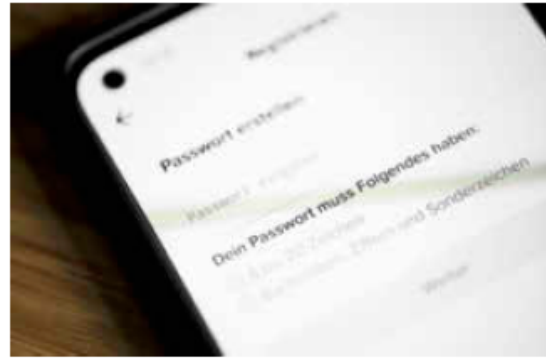
Main-Echo 20.12.2023

1, 2, 3 und die »123456789« ist geknackt

Digitale Welt: Herrlich einfach machen es sich immer noch viele Nutzer bei der Wahl ihrer Passwörter

Als digitale Gesellschaft sind wir eine kollektive Niete, es muss leider so gesagt werden. Bis Ende vergangenen Jahres war nach einer Erhebung des Hasso-Plattner-Instituts (HPI) – ein privat finanziertes IT-Institut – »123456« das meistverwendete Passwort der Bundesbürger, wenn es online um den Schutz persönlicher Daten und Formate ging. Inzwischen haben wir kapiert, dass diese einfallsslose Zahl doch allzu leicht zu erraten ist. Und so haben die meisten Nutzerinnen und Nutzer ein neues gemeinsames Passwort kreiert, hat HPI herausgefunden: »123456789«.

Immerhin: Man muss nun drei Ziffern mehr eingeben, um an die



Ein sicheres Passwort zu erstellen, ist entscheidend für den Schutz von Online-Konten. Foto: Fabian Sommer (dpa)


digitalen Konten anderer Menschen zu kommen. Allerdings ist das ein Aufwand, der sich lohnen dürfte.

Aktuell auf Platz 2 ist »12345678«, auf Rang 3 »hallo«. Ganz Gewiefte finden sich in guter

Gesellschaft auf den Plätzen 4 und 5 mit »1234567890« und »1234567«. Wer eine Abneigung gegen Zahlen hat, erweist sich allerdings auch nicht unbedingt als schlauer: »password« und »qwertz« – die ersten fünf Buchstaben von links der oberen Buchstabenreihe einer Tastatur – sind mit ein bisschen Grips durchaus zu knacken.

Der bisherige Spitzenreiter »123456« taucht nicht mehr in den Top Ten auf. Die HPI-Sicherheitsforscherinnen und -forscher erklären das damit, dass Nutzer selbst dann nicht kreativer bei der Passwortwahl werden, wenn Online-Dienste die Passwort-Anforderungen verschärfen, etwa bei der erforderlichen Länge.

Interessanterweise glauben aber viele Internetnutzer, dass sie ganz raffinierte Passwörter haben. Das hat eine Umfrage von Bitkom Research – ein Marktforscher für die digitale Welt – ergeben. 74 Prozent der Befragten gaben demnach an, auf ausreichend komplexe oder lange Passwörter zu achten. Aber: 38 Prozent notieren sich ihre Passwörter auf einem Zettel. *Stefan Reis*

 **Bundesamt für Sicherheit in der Informationstechnik (BSI):** Tipps zu Passwörtern: <http://dpaq.de/Gdob2>
BSI-Tipps zu Passwort-Managern: <http://dpaq.de/tE4bR>
BSI-Tipps zu einem Passwort-Merkblatt: <http://dpaq.de/sA08G>

Empfehlung für die Passwortvergabe

- Passwortlänge mindestens 8 Zeichen ⁽¹⁾
 - Mindestens ein Großbuchstabe
 - Mindestens ein Kleinbuchstabe
 - Mindestens ein Sonderzeichen
 - Mindestens eine Ziffer

Beispiel: Ar(15#xu

- Alternativ sehr lange Passwörter mit mehr als 25 Zeichen ⁽¹⁾

Beispiel: Meine_Oma_sitzt_im_Wohnzimmer

- Keine Kombinationen wie Vorname des Partners + Geburtsdatum

(1) Empfehlung Bundesamt für Sicherheit in der Informationstechnologie

Warum diese Komplexität?

- Angreifer im Internet (Hacker) nutzen verschiedene Möglichkeiten, um das Passwort für einen fremden Zugang herauszufinden:
 - Die Liste der häufigsten Passwörter
 - Liste von gestohlenen Zugangsdaten (z.B. aus dem Darknet)
 - Wörterbücher
 - Kombination aus gängigen Wörtern und Zahlen (Test1234, Test12345, ...)
 - Vollautomatisches Ausprobieren aller möglichen Zeichenkombinationen (Brute-Force-Methode = Methode der rohen Gewalt)
- Untersuchungen haben gezeigt, dass Computersysteme in der Lage sind, einfache Passwörter in wenigen Sekunden/Minuten zu hacken
- Für komplexe Passwörter brauchen selbst Supercomputer mehrere Jahre

Passwort Probleme

- Jetzt habe ich mir ein komplexes Passwort ausgedacht und auf allen Online Diensten mein einfaches Passwort mit dem komplexen ersetzt

STOP! Das sollten Sie keinesfalls tun!

- Für jeden Zugang sollte ein unterschiedliches Passwort benutzt werden
 - Sollte ein Dienst gehackt worden sein, sind zumindest die anderen Zugänge noch sicher
- Aber wie kann ich mir die vielen komplexen Passwörter merken?
 - Aufschreiben und an die Pinwand hängen ist keine gute Idee
 - Nutzen Sie einen Passwort Tresor

Tipps für ein gutes Passwort

- Sie merken sich einen langen Satz und nutzen daraus von jedem Wort den ersten Buchstaben und die Ziffern
 - Ich wurde 1959 geboren und arbeite bei Siemens
lw1959guabS
 - Fordert der Dienst den Einsatz von Sonderzeichen, dann ersetzt man typische Buchstaben durch das Sonderzeichen:
 - $a \rightarrow @$
 - $l \rightarrow !$
 - $s \rightarrow \$$
 - !w1959gu@b\$
 - Mit 11 Zeichen lang und komplex genug
 - Welche Sonderzeichen erlaubt sind, legt der Diensteanbieter fest
 - Bei vielen Online Zugängen wird es schwierig sich alle Sätze zu merken

Passwort Tresor – Passwort Manager

- Inzwischen gibt es eine ganze Reihe von guten und sicheren Apps/Programmen zum Speichern von Zugangsdaten
- Die Daten im Passwort Manager werden mit einem Hauptpasswort geschützt. Dieses sollte möglichst lang und komplex sein.
 - Risiko: wenn Sie das Hauptpasswort vergessen, können Sie nicht mehr auf die Daten zugreifen
- Auf was sollte ich bei der Auswahl eines Passwort Managers achten?
 - Kostenlos oder kostenpflichtig?
 - Betriebssystem: Windows, macOS, Android, iOS, Linux
 - Wo werden die Daten gespeichert (lokal oder in der Cloud)?
 - Daten synchronisieren (z.B. zwischen Windows und Smartphone)
 - Funktionsumfang (Passwort Generator, ...)
 - Benutzeroberfläche in Deutsch?

Vergleich Passwort Manager

Name	(1)	(2)	(3)	(4)	Win	mac	Android	iOS	Linux	€ (5)
Keeper	1	9	5	9	X	X	X	X		0 (ab 2,91\$/Monat)
Bitwarden	2	1	1	10	X	X	X	X	X	0 (10\$/Jahr)
1Password	3	8	3	7	X	X	X	X		0 (2,99\$/Monat)
Enpass	4		4	6	X	X	X	X	X	Ab 0,71€/Monat
Dashlane	5	7	2	4	X	X	X	X	X	0 (ab 4,99\$/Monat)
Sticky Password	6	5	8	8	X	X	X	X		0 (29,99\$/Jahr)
NordPass	7	2	6	2	X	X	X	X	X	0 (2,49\$/Monat)
LastPass (6)	10	6		1	X	X	X	X	X	0 (ab 3\$/Monat)
KeePass		3	9	13	X	X	X	X	X	0
RoboForm		4	7	11	X	X	X	X		0 (16,7\$/Jahr)
PasswordSafe				12	X		X	X		0

(1) chip.de, (2) kinsta.com, (3) PC Welt, (4) netzwelt.de

(5) Basis kostenlos, Zusatzfunktionen kostenpflichtig, (6) wurde gehackt

Passwort Manager Alternativen

- Hersteller von Internet Sicherheitspaketen versprechen einen Komplettschutz
 - Erweiterter Virenschutz
 - Schutz vor Tracking und Werbung
 - Passwort Manager
 - Auswahl Anbieter: Norton, McAfee, Avira, ...
 - Kostenpflichtig, meistens Jahresgebühr (ca. 30-50 Euro)
- Manche Banken bieten Manager für Passwörter und Dokumente
 - Beispiel: Sparkasse S-Trust (bis 25 Passwörter kostenlos, sonst 1,49 €/Monat)
- iOS Notizen mit Fingerabdruck oder FaceID verschlüsseln
 - Bedingt empfehlenswert
- iOS Passwörter

Passwort Überprüfung

- Wird meine E-Mail Adresse in einem Datenleck geführt?
 - Have I been pwned – Wurde ich verpiffen?
 - <https://haveibeenpwned.com/>
- Wie sicher ist mein Passwort?
 - Bitwarden
<https://bitwarden.com/de-DE/password-strength/>
 - NordPass
<https://nordpass.com/de/secure-password/>

Zwei-Faktor-Authentifizierung – 2FA

- Basis für die Anmeldung zu einem beliebigen Dienst stellt immer ein starkes Passwort dar
- Zusätzlich wird häufig 2FA angeboten, um die Sicherheit zu erhöhen
- Für die folgenden Beispiele erfolgt die Anmeldung zu einem Dienst mit einem Windows PC mit Benutzername und Passwort
 - Es wird eine E-Mail mit einem Einmal Passwort verschickt. Erst nach Eingabe des korrekten Einmal Passworts wird der Zugang gewährt
 - Eine SMS enthält einen Code, der eingegeben werden muss
 - Der Zugang muss über eine (vorher installierte) App freigegeben werden
 - Freigabe der Anmeldung über einen hinterlegten Sicherheitscode
 - Freigabe über die Online Funktion Personalausweis
 - Banken, Deutsche Rentenversicherung, ausgewählte Behörden, ...

2FA mit Personalausweis 1/2



- Voraussetzungen
 - Personalausweis mit Online-Ausweisfunktion
 - Alle aktuellen Personalausweise besitzen die Online-Funktion. Diese wurde 2010 eingeführt und Personalausweise sind nur 10 Jahre gültig
 - Selbstgewählte, 6-stellige PIN
 - Die 5-stellige Transport PIN muss einmalig geändert werden
 - Geeignetes Smartphone (NFC fähig) oder Kartenlesegerät
 - Software AusweisApp2 (entweder als App auf dem Smartphone oder als Software auf dem Computer)
 - Hinweis: App wurde von AusweisApp2 in AusweisApp umbenannt (November 2023)
- Möglichkeiten ID Check:
 - Smartphone
 - Computer und Smartphone
 - Computer und Kartenlesegerät

Beispiel Deutsche Rentenversicherung



- Geeignetes Smartphone mit installierter AusweisApp2
- Bereits registriert

login.deutsche-rentenversicherung.de

Deutsche Rentenversicherung

Ein herzliches Willkommen beim ID Check der Deutschen

So funktioniert's:

Wählen Sie Ihr Endgerät:

- Mobilgerät** +
- Computer und Mobilgerät +
- Computer und Kartenlesegerät +

Anmelden

Die App „Chrome“ möchte „AusweisApp“ öffnen

Abbrechen Öffnen

Ausweisen

Scan starten

Der NFC-Scan ist nicht aktiv. Bitte starten Sie den NFC-Scan.

NFC-Scan starten

Anbieter

Deutsche Rentenversicherung Bund Online Agentur

Tippen Sie hier für mehr Details

Weiter zur PIN-Eingabe

Karten-PIN

Bitte geben Sie Ihre sechs

Was ist die Karten-PIN?

Willkommen in Ihrem persönlichen Kundenportal

Persönliche Daten und Einstellungen

Versicherungsdaten und Rente

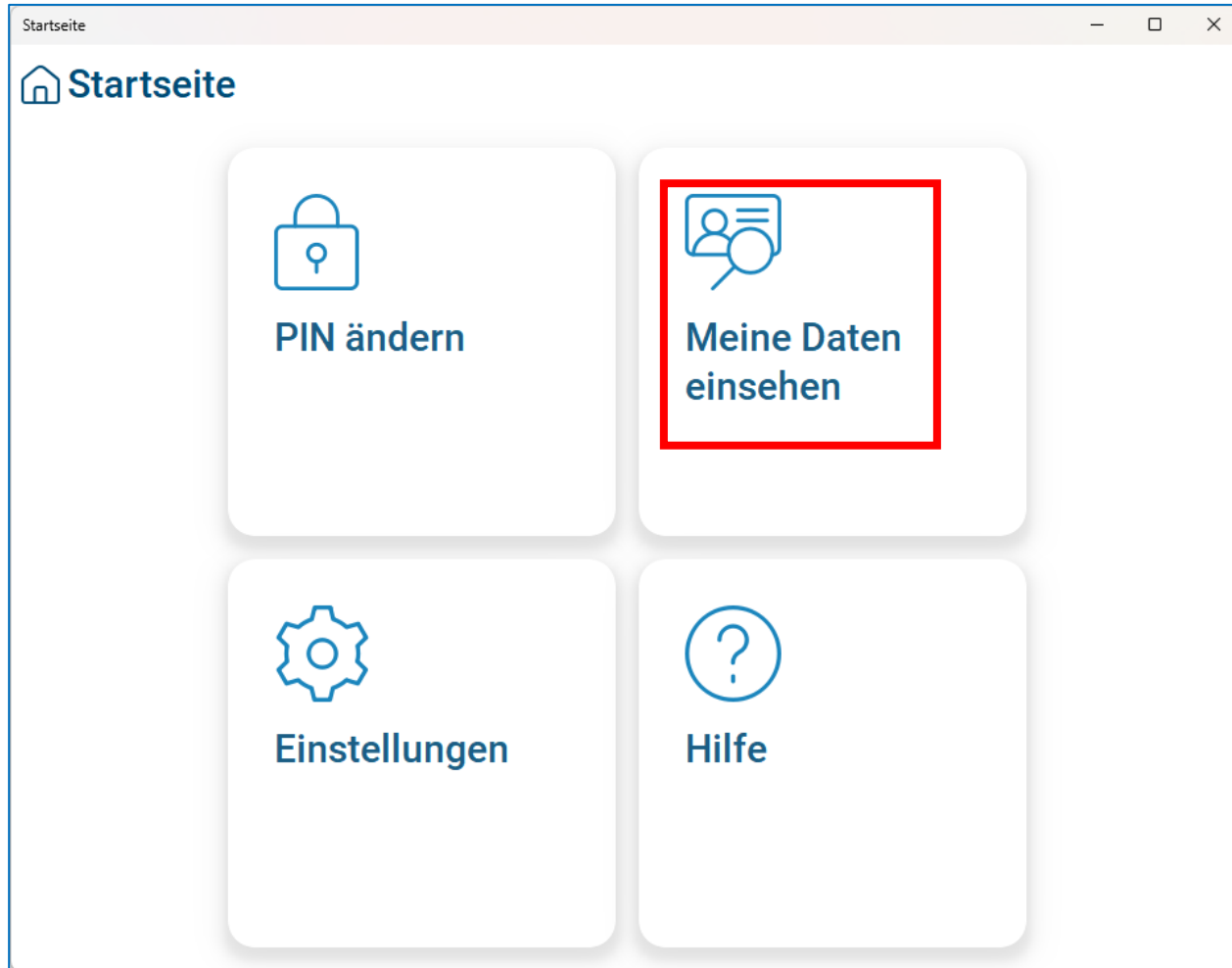
Zugang mit externem Kartenlesegerät 1/2



- Kartenlesegerät über USB mit dem Computer verbinden
- Personalausweis einstecken
- AusweisApp auf dem Computer starten

ca. 120 Euro!

Zugang mit externem Kartenlesegerät 2/2



Ausweisen



Überall, wo Sie dieses Logo sehen, können Sie Ihren Ausweis einsetzen.

Über die Schaltfläche "Meine Daten einsehen" können Sie den Selbstauskunftsdienst des Herstellers der AusweisApp aufrufen, um sich die im Chip Ihres Ausweises gespeicherten Daten anzeigen zu lassen.

Es erfolgt keine Speicherung oder Weiterverarbeitung Ihrer persönlichen Daten. Näheres dazu erfahren Sie in unserer Datenschutzerklärung.

Meine Daten einsehen



Sie möchten sich bei folgendem Anbieter

ausweisen:

Governikus GmbH & Co. KG



Details zum Anbieter

Weiter zur PIN-Eingabe

Passwörter im Browser

- Alle gängigen Browser bieten die Möglichkeit, Zugangsdaten zu speichern. Beim nächsten Zugriff ist eine Anmeldung nicht mehr erforderlich oder Benutzername/Passwort müssen nur noch mit OK bestätigt werden
- Sehr praktisch, aber ist das auch sicher?
- NEIN!
Jede Person, die am PC sitzt, kann die Passwörter im Klartext einsehen
- Die Möglichkeit, Passwörter im Browser zu speichern, sollte nur genutzt werden, wenn der PC selbst geschützt ist
 - Anmeldung in Windows mit Passwort (alternativ Fingerabdruck, FaceID)
 - Windows PC sperren, wenn man nicht mehr am PC arbeitet

Gibt es keine Alternativen?

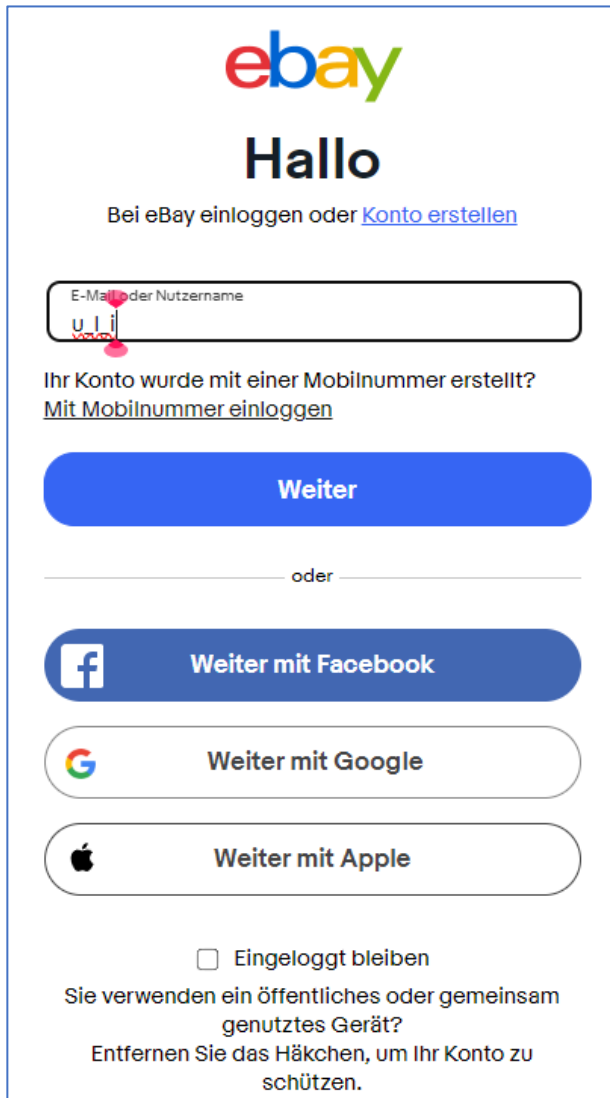
- **FIDO** = **F**ast **I**Dentity **O**nline
 - Übersetzt: schnelle Identität bei digitalen Verbindungen
 - 2013 offiziell gegründet
 - Offener, lizenzfreier Industriestandard
 - Kein Passwort erforderlich
 - Starke Verschlüsselung basierend auf einem privaten und einem öffentlichen Schlüssel
 - Authentifizierung
 - Biometrische Merkmale (Fingerabdruck, Gesichtserkennung, Stimme)
 - Hardware Schlüssel (FIDO2 Token)
 - Smart Cards
 - TPM Module (Trusted Platform Module), in aktuellen Computern vorhanden
 - Nachteil: geringer Verbreitungsgrad

Beispiel FIDO2 Token YubiKey 5C NFC



- Hardware Token von der Firma Yubico gibt es mehreren Ausführungen
- In der USB-C Variante mit NFC kostet dieser ca. 60 Euro
- Ein zweiter Token wird empfohlen (Backup)

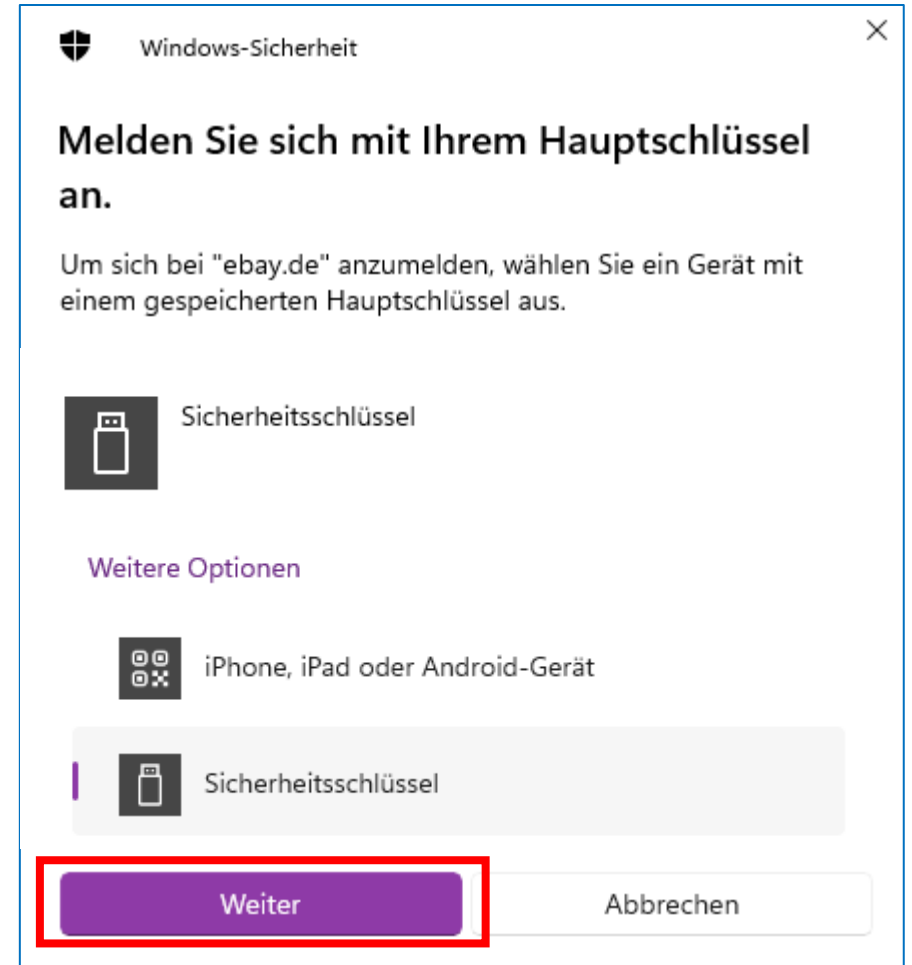
Zugang zu eBay mit FIDO2 Token 1/2



The eBay login page features the eBay logo at the top, followed by the greeting 'Hallo'. Below this, there is a link to 'Bei eBay einloggen oder Konto erstellen'. A text input field for 'E-Mail oder Nutzername' contains the text 'u_li'. Below the input field, there is a note: 'Ihr Konto wurde mit einer Mobilnummer erstellt? Mit Mobilnummer einloggen'. There are three main buttons: a blue 'Weiter' button, a blue 'Weiter mit Facebook' button, and a white 'Weiter mit Google' button. At the bottom, there is a white 'Weiter mit Apple' button. A checkbox labeled 'Eingeloggt bleiben' is present, with a note: 'Sie verwenden ein öffentliches oder gemeinsam genutztes Gerät? Entfernen Sie das Häkchen, um Ihr Konto zu schützen.'

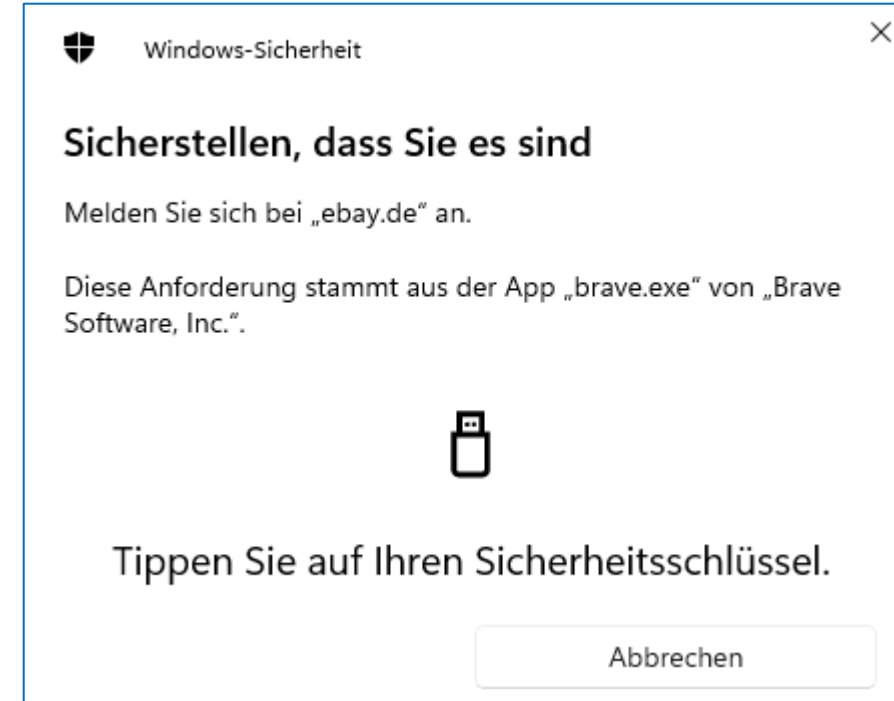
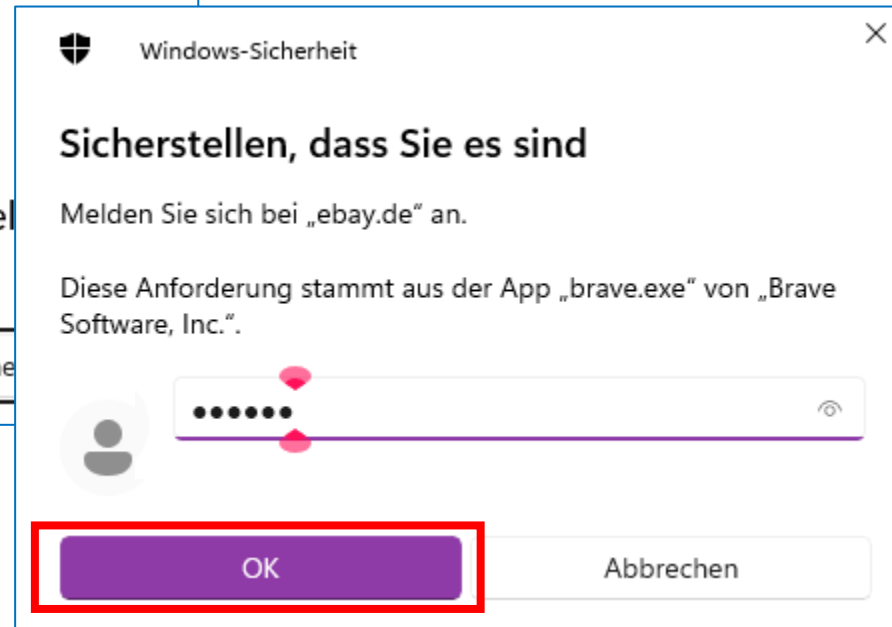
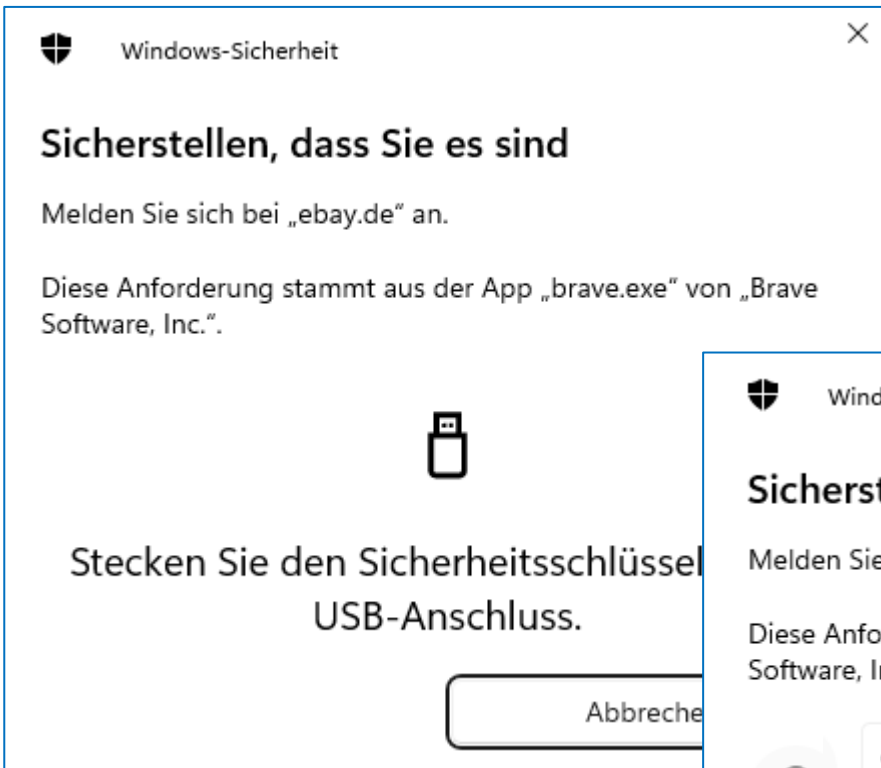


The eBay login page shows the 'Willkommen' section with the username 'u_li'. Below the username, there is a link: 'Nicht Ihr Nutzername? Konto wechseln'. A password input field is visible. Below the password field, there is a grey 'Einloggen' button. Below the button, there is a link: 'Mit Sicherheitsschlüssel einloggen' which is highlighted with a red box. At the bottom, there is a link: 'Sie benötigen Hilfe beim Einloggen?' with a dropdown arrow.



The Windows security dialog is titled 'Windows-Sicherheit' and contains the text: 'Melden Sie sich mit Ihrem Hauptschlüssel an.' Below this, there is a message: 'Um sich bei "ebay.de" anzumelden, wählen Sie ein Gerät mit einem gespeicherten Hauptschlüssel aus.' There are two device options: 'Sicherheitsschlüssel' (highlighted with a red box) and 'Weitere Optionen'. Under 'Weitere Optionen', there is an option for 'iPhone, iPad oder Android-Gerät' and another for 'Sicherheitsschlüssel'. At the bottom, there are two buttons: a purple 'Weiter' button (highlighted with a red box) and a white 'Abbrechen' button.

Zugang zu eBay mit FIDO2 Token 2/2



Zusammenfassung

- Nutzen Sie immer ein starkes Passwort
- Verwalten Sie die Passwörter mit einem Passwort Manager, nicht in einer ungeschützten Textdatei, nicht auf dem Zettel unter der Tastatur oder an der Pinwand
- Nutzen Sie für jeden Dienst unterschiedliche Passwörter
- Wenn möglich, richten Sie 2FA (Zwei-Faktor-Authentifizierung) ein
- Ändern Sie regelmäßig Ihre Kennwörter
- Verzichten Sie auf die Möglichkeit, Passwörter im Browser zu speichern
- Denken Sie an die Erben

Sicheres Onlinebanking

Warum Online-Banking?

- Verfügbarkeit (24 Stunden täglich), unabhängig von den Öffnungszeiten der Bankfilialen
- Bequem von zu Hause oder unterwegs mit Computer, Tablet oder Smartphone
- Kostengünstig
- Schnell („Sofort-Überweisung“)
- Elektronische Kontoauszüge (PDF Datei, Datenexport für die Weiterverarbeitung)
- Hoher Sicherheitsstandard durch moderne TAN Verfahren
- Papierlos (Umwelt! Entsorgung Kontoauszüge?)
- Alarmfunktionen (Soll/Haben Buchungen ab Betrag x) per E-Mail/SMS

TAN = Transaktionsnummer

- Warum brauche ich eine TAN?
- Der Zugang zum Onlinebanking erfolgt in der Regel über einen Benutzernamen und ein Passwort
- Verschafft sich ein Krimineller Zugang zu diesen Anmeldedaten, könnte dieser ohne zusätzliche Schutzmaßnahmen das Konto „leer räumen“
- Die TAN ist nur einmalig gültig und schützt einen Onlinebanking Vorgang (z.B. eine Überweisung)

Klassische TAN Liste

iTAN-Liste

1	398162	11	085965	21	131798	31	630279	41	902319	51	266639	61	983337	71	159498	81	743813	91	752623
2	383537	12	984371	22	363427	32	256543	42	727818	52	112486	62	938374	72	647477	82	683830	92	198872
3	355832	13	540739	23	387440	33	193699	43	639528	53	007796	63	007715	73	740333	83	510731	93	658932
4	508084	14	245641	24	703982	34	729497	44	967701	54	658908	64	508267	74	970998	84	293124	94	831589
5	061305	15	606378	25	857364	35	365724	45	362942	55	151717	65	864090	75	278121	85	887540	95	583415
6	496675	16	327938	26	166482	36	967352	46	755010	56	344267	66	158858	76	724795	86	937629	96	413993
7	715597	17	243838	27	974595	37	070744	47	807567	57	706303	67	789798	77	179679	87	892658	97	029990
8	162311	18	341311	28	485544	38	773818	48	822150	58	118741	68	276331	78	254291	88	850191	98	219733
9	787205	19	031779	29	092738	39	686180	49	548329	59	865555	69	393587	79	413586	89	884138	99	454021
10	213953	20	595164	30	010575	40	313037	50	964987	60	864467	70	634144	80	244968	90	340408	100	366297

- Nach Eingabe Empfänger Daten (Name, IBAN, Verwendungszweck) wird der Onlinebanking Benutzer nach einer TAN gefragt
- Gehört der Vergangenheit an

EU-Zahlungsdiensterichtlinie PSD2

- Seit dem 14. September 2019 sind die Kreditinstitute durch die EU-Richtlinie PSD2 (Payment Services Directive 2) zur starken Kundenauthentifizierung verpflichtet
- Mindestens zwei Faktoren aus den drei Kategorien müssen benutzt werden:
 - Wissen (Benutzername, Passwort, PIN)
 - Besitz (Smartphone, TAN-Generator, Bankkarte)
 - Biometrische Daten (Fingerabdruck, Gesichtserkennung, Stimme)

Sicherheit im Onlinebanking

- In den letzten Jahren haben alle Banken sichere Verfahren für das Onlinebanking eingeführt
- Mobile TAN (mTAN, smsTAN)
 - Die TAN wird per SMS verschickt und ist nur eine begrenzte Zeit gültig)
- pushTAN
 - TAN wird an eine Smartphone App geschickt
- chipTAN
 - Zusätzliche Hardware (TAN-Generator), teilweise mit Lesegerät für Bankkarte
- photoTAN
 - Eine bunte Grafik mit Punkten wird mit dem Smartphone gescannt und zeigt die TAN an

smsTAN

- In der Vergangenheit ein sehr sicheres Verfahren, da die Vorbereitung der Überweisung über das Internet erfolgt, die SMS über das Mobilfunknetz verschickt wird (zwei unterschiedliche, physikalische Übertragungswege)
- Die Zeiten, dass man mit einem Mobiltelefon nur telefonieren und SMS senden/empfangen konnte, gehören - mit wenigen Ausnahmen - der Vergangenheit an
- Auf einem Smartphone könnte eine SMS mit einem Trojaner abgefangen werden
- Einige Banken bieten smsTAN nicht mehr an

pushTAN

- Gilt als sicher wenn Onlinebanking und TAN Empfang mit unterschiedlichen Endgeräten durchgeführt wird: Überweisung wird am Computer vorbereitet, die Freigabe erfolgt über Smartphone App
- Wird von den meisten Banken angeboten

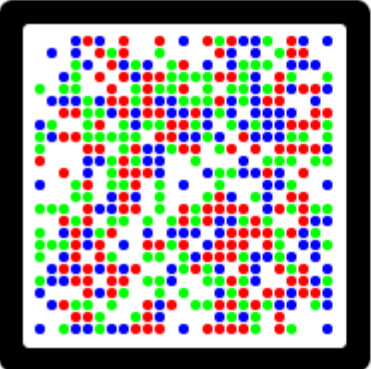
chipTAN

- Sehr sicher, da zusätzliche Hardware (TAN-Generator) benötigt wird
- Bei mehreren Bankkonten sind eventuell mehrere TAN-Generatoren notwendig
- Überweisungen unterwegs sind nicht möglich wenn der TAN-Generator zu Hause liegt

photoTAN

- Das photoTAN Verfahren gilt als sicher, wird aber nur von wenigen Banken angeboten

photoTAN push **photoTAN** mobileTAN



Auftrag mit photoTAN bestätigen


Bitte scannen Sie die nebenstehende Grafik mit Ihrer photoTAN-App oder Ihrem photoTAN-Lesegerät. Vergleichen Sie die auf Ihrem Smartphone oder Lesegerät angezeigten Daten mit Ihren Eingaben und geben Sie dann die angezeigte TAN ein.

photoTAN

photoTAN scannen

Auftragsdaten:

ÜBERWEISUNG

IBAN 

BETRAG 13,69 EUR

photoTAN

5195742

Zusammenfassung

- Die aktuellen TAN Verfahren erlauben sicheres Onlinebanking
- Immer prüfen, ob die Internet Adresse zur Bank passt
- Selbstverständlich sollte der Zugang mit einem komplexen Passwort gesichert sein
- Wenn möglich für Überweisung und TAN unterschiedliche Hardware benutzen (Computer und Smartphone, Computer und TAN Generator)
- Soweit angeboten Alarmierung im Onlinebanking aktivieren
- Bei Unregelmäßigkeiten oder Hardware Verlust unverzüglich die Bank informieren
- Geeignetes Kontomodell wählen

**Danke für Ihre
Aufmerksamkeit**

Fragen?

Nächster Termin

Donnerstag, 22.2.2024 um 16 Uhr

Veranstaltungsort: MGH Johannesberg

Thema:

Browser, Cookies, Suchmaschinen

Präsentationen zu finden unter:

<https://repair-cafe-johannesberg.de/digitalessofa>