Vortrag

Passwörter &
Digitaler Nachlass

Ziel & Zweck des Vortrages

- Sichere Passwörter erstellen
- Passwörter verwalten und Zettelchaos vermeiden
- Informationen für die Erben bereitstellen

Inhalt / Ablauf

- Grundlagen
- Authentifizierungsmethoden
- 2FA (Zwei Faktoren Authentifizierung)
- 1FA (Ein Faktor Authentifizierung)
- Passwörter erstellen
- Spezialfälle
- Verwalten von Passwörter
- Sicherheitsaspekte
- Digitaler Nachlass

- QR-Rechnungen

Computeria Wallisellen

Digitale Identität

Personenbezogene Daten

allgemeine Personendaten
(Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer, Foto, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, religiöse oder politische Einstellungen, Sexualität, Gesundheitsdaten, Urlaubsplanung, Vorstrafen)

Kennnummern
(Sozialversicherungsnummer, Steueridentifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer, Matrikelnummer usf.)

Bankdaten
(Kontonummer, Kreditinformationen, Kontostände usf.)

Onlinedaten
(IP-Adresse, Standortdaten usf.)

physische Merkmale
(Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usf.)

Besitzmerkmale
(Fahrzeug- und Immobilieneigentum, Grundbucheintragung, Kfz-Kennzeichen, Zulassungsdaten usf.)

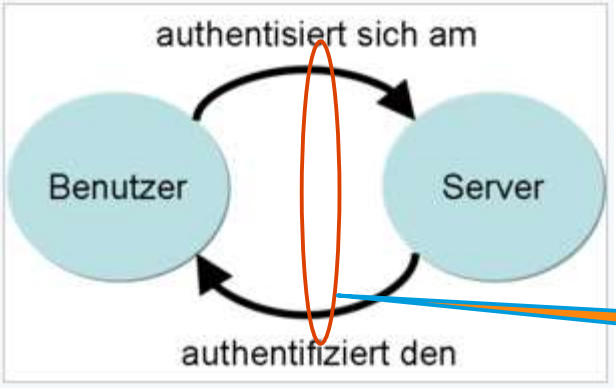
Kundendaten
(Bestellungen, Adressdaten, Kontodaten, usf.)

Werturteile
(Schul- und Arbeitszeugnisse usf.)

sachliche Verhältnisse
(Einkommen, Kapitalvermögen, Schulden, Eigentum (Haus, Wohung, Auto etc.)

bestimmbare Daten, d.h. erst mit weiteren Informationen kann man auf eine Person rückschließen (Personalnummer, IP-Adresse, Kfz-Nummer usf.)

Authentifizierung



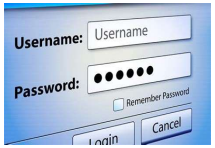
Authentifizierung ist die Verifizierung der Behauptung der Authentizität (Identitätsfeststellung) einer Entität (in unserem Kontext Mensch)
→ Autorisierung / Ablehnung

Angriff

Computeria Wallisellen

Authentifizierungsmethoden basieren auf

Wissen
Kann dupliziert, weitergegeben und verraten werden.



- Login (UserID / Passwort)
- Pin
- Muster
- Antwort auf Fragen
- Zero-Knowledge Beweis

Besitz
Erstellung aufwendig
Verwaltung unsicher
Kann verloren gehen

- Chipkarte
- Magnetstreifenkarte
- RFID-Karte
- Physischer Schlüssel
- Schlüssel-Codes auf HDD
- SIM-Karte beim mTAN-Verfahren
- Zertifikat (SSL-Verfahren)
- TAN- und iTAN-Liste
- One Time PIN Token
- USB-Stick mit Passworttresor
- USB-Festplatte mit integrierter PIN-Eingabetastatur

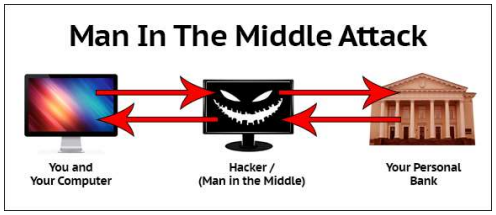
Körp. Merkmal/Biometrie
Gehören zu einer Person

- Fingerabdruck
- Gesichtserkennung
- Tippverhalten
- Stimmerkennung
- Iriserkennung
- Retinamerkmale
- Handschrift (Unterschrift)
- Handgeometrie
- Handlinienstruktur
- Erbinformation (DNS)

Computeria Wallisellen

Methoden

Bei Einsatz einer der Methoden spricht man von **Ein-Faktor-Authentisierung (1FA)**



Gefahren
Während der Authentifikation werden Daten übertragen. Werden diese Daten abgehört können sie von einem Angreifer verwendet werden, um eine falsche Identität vorzuspiegeln

Diese Defizit können durch geeignete Kombination der Methoden **vermindert** werden:

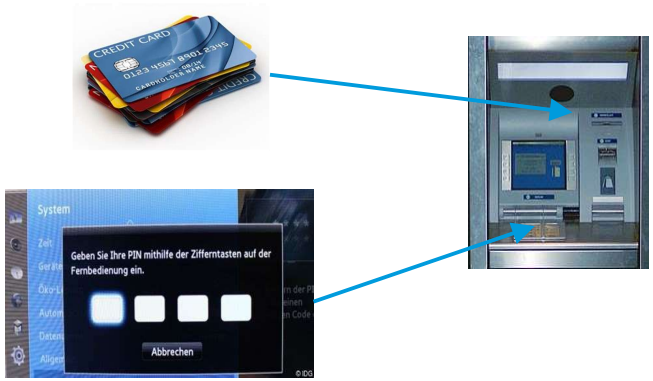
Bei einer Kombination von zwei Methoden spricht man von einer

Zwei-Faktor-Authentisierung (2FA)

oder auch Zwei-Stufen-Authentifikation, mit mehr als 2 Faktoren nennt man von

Multi-Faktoren-Authentisierung

2FA



Ein typisches Beispiel für die Kombination von Wissen und Besitz ist ein Geldautomat:
Man besitzt die **Bankkarte** und weiß die **persönliche Identifikationsnummer (PIN)**.

bitwarden

Beispiel bitwarden

Als Authentifizierungsfaktoren, die im Rahmen der 2FA über gesondert abgefragte Benutzerdaten im Rahmen der Authentifizierung verbunden und geprüft werden, sind möglich:

+ Informationen, die nur der Benutzer kennt
  (zum Beispiel Benutzername und Kennwort oder PIN und TAN)
+ Ein Informationselement, das nur der Anwender besitzt (zum Beispiel ein Smartphone oder Tablet beziehungsweise ein Token wie Plastikkarte, USB-Stick oder Schlüssel)
+ Ein körperliches Merkmal (Fingerabdruck, Iris, Stimme)

Online-Anbieter von 2FA

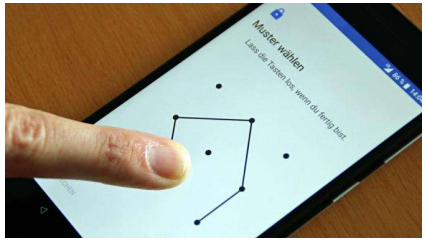
Apple	PlayStation Network	CH-Krankenkassen	
Amazon	Snapchat	……	
Dropbox	Twitter		
Evernote	Twitch		
Facebook	WhatsApp		
Google	WordPress		
LinkedIn	Yahoo		
Microsoft	-> E-Banking CH		
PayPal	…..		

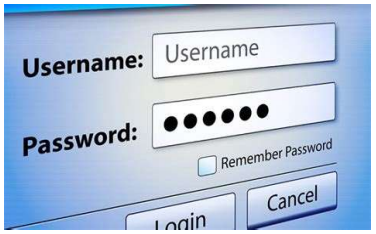
Die oben aufgeführten Anbieter sind nicht abschliessend aufgeführt.
Sie verwenden auch unterschiedlichen 2FA Verfahren.
Weiterführende Informationen:
https://www.verbraucherschutz.com/ratgeber/zwei-faktor-authentifizierung-wer-bietet-sicherheit/

Nutzen Sie das Angebot !

Computeria Wallisellen

Ein Faktor Authentifizierung 1FA



Für den üblichen 1FA Gebrauch werden PIN,Gesichtserkennung, Muster, Fingerabdruck, User / Passwort eingesetzt.

Ein absolut unknackbares Authentifizierungssystem gibt es nicht!

Eine komplexe Authentifizierung soll vielmehr den Zugang erheblich erschweren, denn: Je mehr Zeit für den digitalen Einbruch aufgewendet werden muss, desto größer ist die Wahrscheinlichkeit, dass Datendiebe von dem Vorhaben abweichen.

1FA Detail I

PIN (bequem aber relativ einfach zu knacken)

Die Eingabe von Ziffern ist bequem und viele Reihenfolgen lassen sich relativ leicht merken

Wie für die SIM-Karte lässt sich auch als Displaysperre ein PIN-Code festlegen.
Er kann z.B. bei Android-Geräten zwischen 4 und 17 Ziffern lang sein

- Die Eingabe von Ziffern ist bequem
- Reihenfolgen lassen sich relativ leicht merken
- Kann notiert und aufbewahrt werden

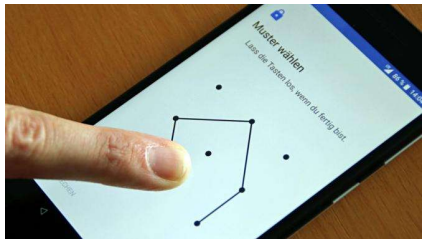
- Erratbar
- Fingerspuren auf dem Display

- Verwenden Sie mehr als vier Ziffern
- Verwenden Sie eine andere Kombination als für Ihre SIM-Karte
- Keinesfalls Ihr Geburtsdatum
- Vermeiden Sie einfache Kombinationen (wie 123456...)

1FA Detail II

Gesichtserkennung	(relativ sicher)
Am Gesicht erkennen wir andere Menschen am schnellsten wieder. Auch seinem Smartphone kann man beibringen, den Nutzer über die Selfie-Kamera wiederzuerkennen und somit das Display freizugeben.	• Das Entsperren ist bequem • Ein Gerät mit 3D-Kamera ist schwer zu überlisten • Keine Spuren auf Dispay
	• Funktioniert nicht immer zuverlässig. • Schwaches Licht, Maske, Sonnenbrillen oder wehende Haare können die Entsperrung des Displays verhindern. • Viele Selfie-Kameras lassen sich mit Fotos überlisten
• Nicht sicher bei einfachen Selfie Kamera • Kann nicht übergeben werden (digitaler Nachlass) • Kombination mit PW oder anderen Merkmale ist besser	

1FA Detail III



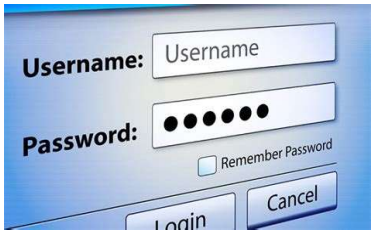
Muster	(bequem aber relativ einfach zu knacken)
An einem Raster mit 9 Punkten müssen mindestens 4 Punkte verbunden werden. Das angelegte Muster sollte man sich gut merken. Verbindet man die falschen Punkte oder auch die richtigen in der falschen Reihenfolge, wird das Smartphone nicht freigegeben. In der Regel gibt es dann die Möglichkeiten, in so einem Fall durch eine PIN oder ein Passwort das Display entsperren zu können.	• Das Entsperren ist bequem • Muster lassen sich schnell und einfach zeichnen. • komplexes Muster ist schwerer zu erraten
	• Wischspuren auf dem Display

- Wenn Sie Muster nutzen möchten, verwenden Sie keine einfachen wie Buchstaben (M oder Z)
- Verbinden Sie mehr als 4 Punkte miteinander und verwischen Sie Ihre Fingerspuren auf dem Display nach jeder Nutzung.
- Kann nicht übergeben werden (digitaler Nachlass)
- Kombination mit PW oder anderen Merkmale ist besser

1FA Detail IV

Fingerabdruck	(relativ sicher)
Einen Finger auf den Sensor legen und schon ist das Smartphone wieder nutzbar. Der Fingerabdrucksensor ist bei vielen aktuellen Geräten schon Standard. Beim Einrichten des Fingerabdrucks erfordert das Gerät meistens eine zweite Entsperr-Variante, für den Fall dass der Abdruck mal nicht erkannt werden kann.	• Das Entsperren ist bequem • Schwer zu knacken
	• Funktioniert nicht immer zuverlässig. • Verletzung • Kann nicht übergeben werden (digitaler Nachlass) • Abdruck auf Display
• In der Regel ist in solchen Fällen aber auch alternativ ein Entsperren mit PIN oder Passwort empfehlenswert • Muster sollten nur lokal gespeichert sein, nicht auf Server • Empfehlenswert 2 Fingerabdrücke speichern	

1FA Detail V



User-ID / Passwort	(bedingt sicher)
Beim Passwort kommt es darauf an, wie stark es ist. Kombinationen aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen machen es einem Unbefugten schwer, das Gerät zu nutzen. Wichtigster Faktor ist die Länge: Mit jeder weiteren Stelle erhöht sich die Zahl möglicher Kombinationen.	• Gute Passwörter sind sehr sicher • Kann gut verwaltet werden
	• Phishing • Schwache Passwörter leicht knackbar • Komplexe PW schwer zu merken • Eingabe von langen PW

- Pro Benutzerkonto 1 Passwort
- Ein langes Passwort ist gut, ein längeres ist in der Regel noch besser
- Verwenden von Passwort-Manager wo möglich
- Passphrasen sind besser merkbar als komplexe Passwörter
- Für wichtige Zugänge (Finanzen etc.) setzen Sie Multi-Faktoren-Authentisierungen ein (MFA)
- **Passwörter dem Nutzen anpassen**

Computeria Wallisellen

Stärke von Passwörter

Schwache PW

hallo
passwort
hallo123
schalke04
passwort1
qwertz
schatz
hallo1

Komplexe PW

Selber definiert | Passphrase | Sichere eMail Adresse | Passwort Manager | 2FA | Links | Impressum

Bezeichnung	Passwort	Sicherheit
Große/kleine Buchstaben / Zahlen / Sonderzeichen / Umlaute:	6]}1ÄzahQi2rMH,5	99%✓
Große/kleine Buchstaben / Zahlen / Sonderzeichen:	FPJ@[jHKZ#[7WeA}	99%✓
Gut zu merken sicherer:	?Modematidot387-	90%
Gut zu merken:	Vetigilixifem656	72%
Nur große/kleine Buchstaben und Zahlen:	LMmozR5exZh4D1dX	72%
Nur kleine und große Buchstaben mit Umlauten:	GsfÜrhwCpoaaüIWÜ	63%
Nur große Buchstaben und Umlaute:	ÜRBLÄLSOYPÜTZÜÄD	54%
Nur kleine Buchstaben und Umlaute:	üiacqcifpoäjxtrx	54%
Nur große Buchstaben und Zahlen:	L7N090YU75K0GKIQ	54%
Nur kleine Buchstaben und Zahlen:	fp4w2iez1n15a3pv	54%
Nur große Buchstaben:	PORCGJZFFNPQMYGC	36%
Nur Zahlen und Sonderzeichen:	/,~&92_-86\1}/[&	36%
Nur kleine Buchstaben:	hgjbybqxwfgieqyu	36%
Nur Zahlen:	2193192411861580	18%
Nur Sonderzeichen:	-@=~#,-]&?\-&=@}	18%

Erlaubte Sonderzeichen: !?@(){}[]\/=~$%&#*-+.,_ Passwortlänge: 16 Neu generieren

Präferenzen Sonderzeichen !?@(){}[]\/=~$%&#*-+.,_ und Passwortlänge (16) als Cookie speichern

Passphrasen

konsole-gestrüpp-bronchiale-verschiedene-hausbewohner
Broadways&Schwimmer&Streiten7&Entsprechend&Dramatisieren
Wackelig Ausgabe Oxidationsmittel Erachten Makellos
unbewacht3 superkleber evakuierter paddelnd düster schleifend
absonderung.braten.hacken.unbewertet9.streiten.krankhaft.planen

Beispiel k&Uy5>~_

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0–9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a–z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A–Z; a–z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A–Z; a–z; 0–9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Computeria Wallisellen

Goldene Regeln für ein sicheres Passwörter

- Pro Login ein eigenes Passwort
- Mindestens 8 Zeichen lang
- Wichtige Passwörter mind. 20 Zeichen (Verschlüsselung,...)
- Vermeiden Sie Wiederholungen oder Tastaturmuster
- Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter.
- Von qwertz bis 1234321 immer Abstand nehmen
- Umlaute vermeiden (Ausland!)
- Wortkombinationen oder logische Zahlen- oder Buchstabenreihen vermeiden
- Neben Buchstaben sollten auch immer Zahlen und insbesondere Sonderzeichen wie /[(%&§$_:?!+#)] aufgenommen werden
- Ein sicheres Passwort sollte sowohl Groß- als auch Kleinbuchstaben enthalten.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist nicht empfehlenswert.

Computeria Wallisellen

Testen von Passwörter

Nie Originalpasswörter im Internet testen

Mit System

Systematische Passwörter

Diese Methode erlaubt Passwörter nach einem System zu generieren und zu merken

- Länge des Passwortes bestimmen 10
- Grundpasswort mit mind. 8 alphanumerischen Zeichen ausdenken und auswendig lernen.
  Beispiel: dU4%K/8§
- Seitenschlüssel für die spezielle Nutzung erzeugen (nach eigenen Regeln)
  Beispiel für ebay: ey34
- Das neue, kombinierte Passwort lautet:
  dU4%K/8§ey34 oder ey34dU4%K/8§

• Muss nicht verwaltet werden • Sicher	• Gefahr von Vergessen • Anpassung der Methodik kann aufwendig

- Methodik muss für den Digitalen Nachlass aufgeschrieben werden.

Computeria Wallisellen

Online Generatoren

https://www.datenschutz.org/passwort-erstellen/

https://sicheres-passwort-generator.de/gutes-passwort-beispiele

Auch Passwort-Manager Apps können Passwörter generieren

Computeria Wallisellen

Passwortkarte

Papiergenerator

- Eine Passwortkarte ist eine vom Besitzer definierte Tabelle aus Ziffern, Buchstaben und Sonderzeichen.
- Mit Hilfe einer Regel kann der Besitzer Zeichenfolgen aus der Tabelle ablesen, die er als Passwörter verwendet.
- Wähle ein Feld in der Tabelle als Startfeld
- Bewege dich vom Startfeld mit Hilfe der geheimen Regel von Feld zu Feld
- Notiere dabei die Zeichen auf den Feldern
- Ergebnis ist dein Passwort

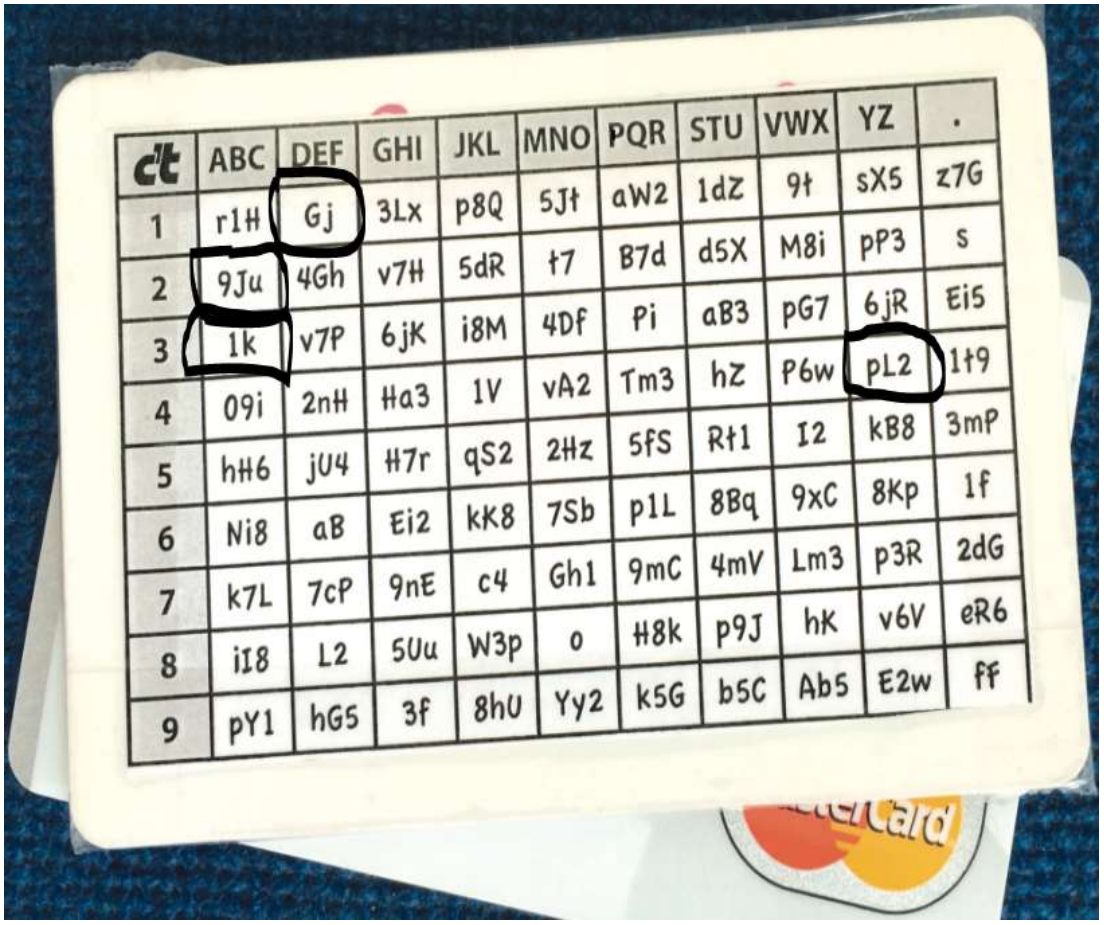
- Komplexe, sichere, Passwörter
- Keine Verwaltung nötig

- Tabelle muss mitgeführt werden (wie Credit Card)
- Passwort muss abgelesen werden
- Kann verloren gehen
- Anwendung bei langen langen Webseiten.

- Viele Varianten möglich, im Internet nach Passkarte suchen
- Kann übergeben werden (digitaler Nachlass)
- Unbedingt selber erstellen

Mehr Infos: https://www.e-passwordcard.com/de/passwortkarten-konzepte-und-generatoren/

Passwortkarte Beispiel

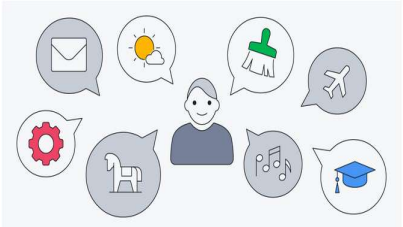


ct	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
1	r1H	Gj	3Lx	p8Q	5Jt	aW2	1dZ	9t	sX5	z7G
2	9Ju	4Gh	v7H	5dR	t7	B7d	d5X	M8i	pP3	s
3	1k	v7P	6jK	i8M	4Df	Pi	aB3	pG7	6jR	Ei5
4	09i	2nH	Ha3	1V	vA2	Tm3	hZ	P6w	pL2	1t9
5	hH6	jU4	H7r	qS2	2Hz	5fS	Rt1	I2	kB8	3mP
6	Ni8	aB	Ei2	kK8	7Sb	p1L	8Bq	9xC	8Kp	1f
7	k7L	7cP	9nE	c4	Gh1	9mC	4mV	Lm3	p3R	2dG
8	iI8	L2	5Uu	W3p	o	H8k	p9J	hK	v6V	eR6
9	pY1	hG5	3f	8hU	Yy2	k5G	b5C	Ab5	E2w	ff

- Regeln
  - max. 5 Zeichen der Webseite
  - wenn länger dann alternierend 2 alle 5 Zeichen
  - Erster Teil bei Zeile 1 usw.

- Beispiel
  www.ebay.ch ==> ebay
  Aus der Tabelle
  e = Gj
  b = 9Ju
  a = 1k
  y = pL2 ==> Gj9Ju1kpL2

Passphrasen



Passphrasen

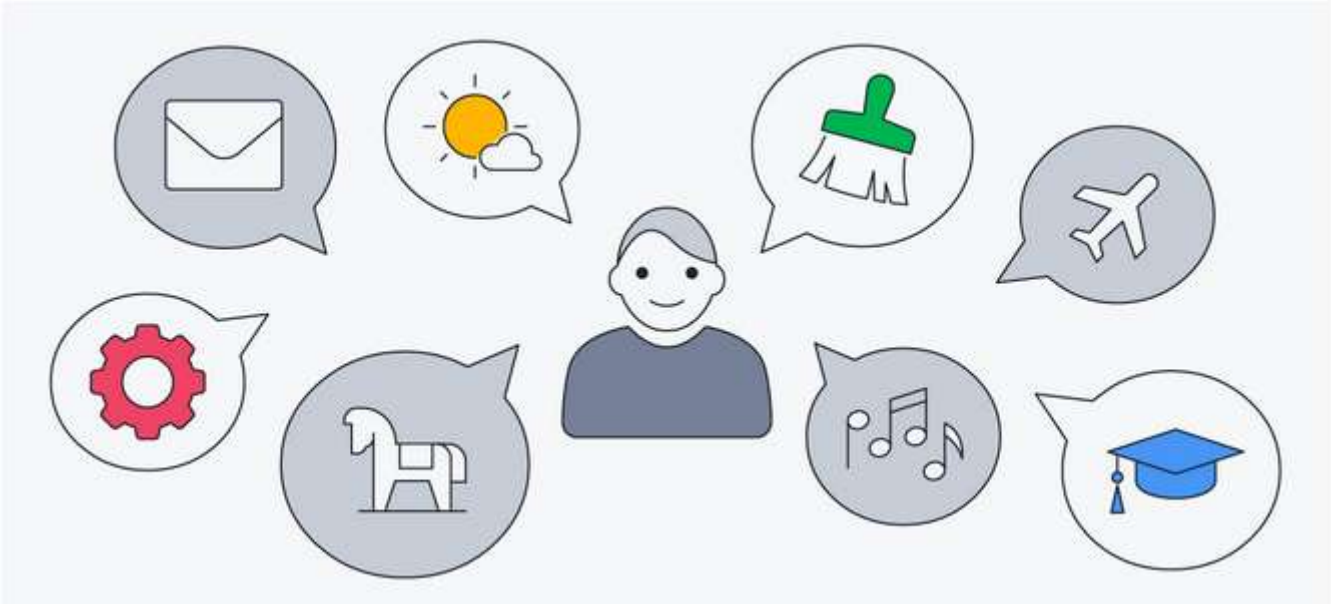
- Sollte Mindestens 15 Zeichen lang
- Sie können die Wörter mit Bindestrichen, Leerzeichen, Punkten, durch Großschreibung des ersten Buchstabens, mit einer Zahl usw. voneinander trennen, um eine starke Passphrase zu erstellen.
- Der Schlüssel zu einer guten Passphrase ist die Zufälligkeit – die Wörter, die Sie zur Erstellung einer Passphrase verwenden, sollten keinen offensichtlichen Zusammenhang aufweisen. Ein gutes Beispiel für eine Passphrase ist überreif-Trekker-Winkel-vorstellen-Brief, während eine Passphrase wie Apfel-Birne-Banane-Orange viel leichter zu knacken wäre.

- Es ist die schiere Länge einer guten Passphrase sowie die Zufälligkeit der Wörter, die sie so sicher macht
- Leichter merkbar als kryptische Passwörter

- Eingabe

- Es gibt Passphrasen-Generatoren im Internet
- Auch Passwort-Manager können Passphrasen generieren

Passphrasen Beispiele



Gut
SonnigBesenFlugzeugPferdAbitur
Sonnig-Besen-Flugzeug-Pferd-Abitur
überreif-Trekker-Winkel-vorstellen-Brief

Eher leicht zu erraten
Apfel-Birne-Banane-Orange

Umgang mit Passwörter

- Nach Nutzung, sich von einem Account immer abmelden
- Passwörter unter Verschluss halten, Passwort-Manager sind eine gute Hilfe
- Passörter spätestens bei Verdacht auf Missbrauch ändern
- Keine einheitlichen Passwörter für Accounts verwenden
- Voreingestellte Passwörter ändern
- Passwörter nicht an Dritte weitergeben nund nicht per E-Mail versenden
- Wenn ein Account nicht mehr benötigt wird, dann löschen lassen
- Vor jedem neuen Account sich die Frage stellen «Brauche ich die Registrierung?»
- Vorsicht mit der Beantwortung von Sicherheitsfragen, man gibt persönliche Daten bekannt (hier sind Fake-Daten erlaubt)
- Wenn möglich Browser im «Private Modus» verwenden

Auch das beste Passwort nützt nichts, wenn die IT-Infrastruktur (Handy, Tablet, PC, Firewall…) nicht auf dem neusten Stand ist (OS, Virenscan, Apps, Treiber...)

Apps & gespeicherte Passwörter

Auf dem Smartphone ist es besonders bequem, Passwörter in den Apps abspeichern zu lassen, sodass man sie nicht bei jedem Start neu eingeben muss.

Das birgt zusätzliche Risiken

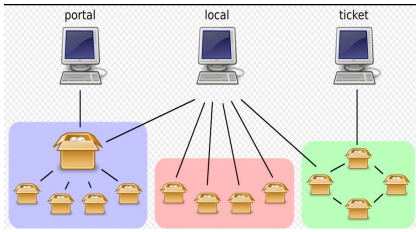
Wird das Smartphone gestohlen, könnte der Dieb Zugang zu Online-Banking und anderen Konten bekommen.

- PW nie speichern
- PW mit gewissem Risiko speichern
- PW kann gespeichert werden

- Möglichst wenige Passwörter auf dem Smartphone
- Smartphones verschlüsseln
- Automatische Bildschirmsperre einrichten

Computeria Wallisellen

Single Sign On (SSO)



Single Sign On

- ein System für eine einmalige Anmeldung an einem Arbeitsplatz mit Zugriff auf weitere Apps, Services und/oder anderweitige Ressourcen.
- Varianten
  - Portallösung
  - Ticketsystem
  - Lokallösung

- Nur 1x Authentifizierung
- Nur ein Passwort, kann komplizierter sein.
- Keine Liste mit Kennw.
- Änderungen der PW nur an 1 Ort

- Systeme müssen SSO verarbeiten
- Vorgabe der Apps die verwendet werden können
- Grösserer Schaden wenn Zugangsdaten gestohlen
- Wenn defekt, alle betroffen.

- Abwandlung durch SSO-Allianzen, Bsp. Nachfolgend
- Wird in der Wirtschaft vermehrt angewendet

Login-Allianzen am Beispiel Facebook Single Sign On

Facebook, Google, Amazon, Apple oder auch "Verimi" sowie "NetID" bieten Lösungen an, sich bei anderen Apps und Seiten mit deren Login-Daten anzumelden.

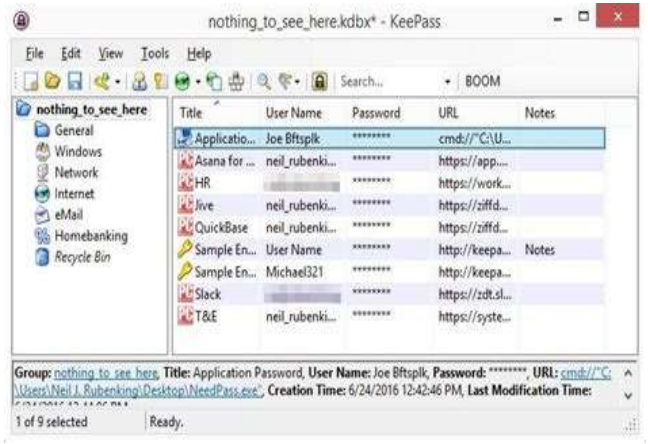
• Anmeldung mit Facebook-Passwort, bequemer •	• Konzentration Nutzerdaten bei Facebook • Nutzerdaten können vom Dienst abgerufen werden. • Nutzerdaten des Dienstes werden in Facebook gespeichert • Gefahr Hack des Facebook-Kontos • Abmeldung bei Facebook löscht alle Logins und Daten des Dienstes in Facebook

https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/singlesignon-riskanter-login-fuer-alle-internetseiten-13704

Verwenden Sie wo möglich (und sinnvoll) eine 2 Faktoren Authentifizierung !

Computeria Wallisellen

Passwort-Verwaltungen

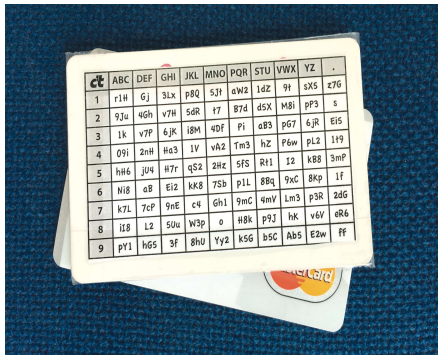


Kopf

Auswendig lernen	
• Die Passwörter werden memorisiert	• Keine Verwaltung
	• Begrenzte Speicherfähigkeit • Vergessen / Unfall • Änderung
• Unsichere Methode, Mensch kann max. 8 bis 20 PW memorisieren	

Computeria Wallisellen

Passwortkarte / System



Karte / System

- Passwort wird jedesmal nach nur dem Anwender bekannten Regeln zusammengestellt
- Regeln müssen auswendig gelernt werden

- Es braucht keine Verwaltung

- Änderung der Regeln
- Verlust der Karte
- Langsame Anwendung

- Regeln sowie Karte sind niederzuschreiben / archivieren

Computeria Wallisellen

Listen

Niederschreiben

- Ergänzenden Daten wichtig
  - Thema
  - Internet Adresse / Software
  - Benutzername
  - Kennwort/Serienummer
  - Eingerichtet am
  - Sicherheitsfragen
  - Bemerkungen
  - ...

- Unabhängig vom PC
- Relativ Sicher
- Portierbar

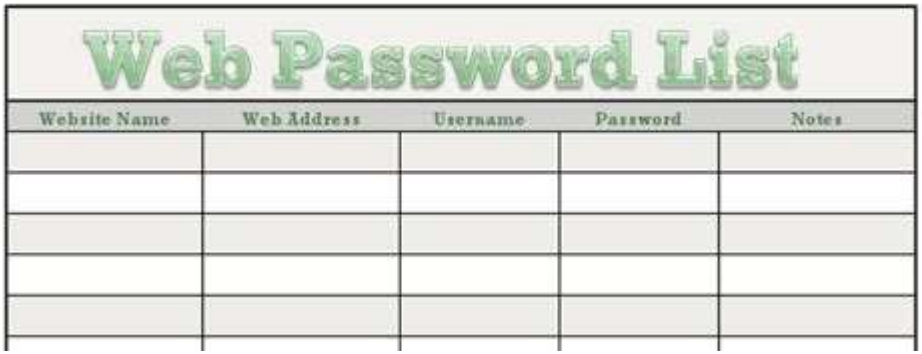
- Änderungen nachführen
- Verlust / Diebstahl

- Auch die Aufbewahrung ist wichtig (z. B. in einen Kennwort-Tresor)
- Kann als Backup der elektronischen Manager SW verw. Werden
- Kann als «Zugriffsliste für den Digitaler Nachlass» genutzt werden

Computeria Wallisellen

Beispiele

PASSWORT-LISTE					
Thema	Internetadresse/Software	Benutzername	Kennwort/Serienummer	Eingerichtet am	Bemerkungen
Soziale Medien	https://facebook.de	Max2017	123!myPassword:	1.12.2017	
Software	https://outlook.de	Max2016	myPasswordxkwe	2.5.2016	
Soziale Medien	https://twitter.de	Max!2016	+3fvqlö)+	3.7.2016	
Soziale Medien	https://instagram.de	5Max2017	$234!agmB:	8.12.2017	
Software	Office	-	1224 3456 2341 5674		



Computeria Wallisellen

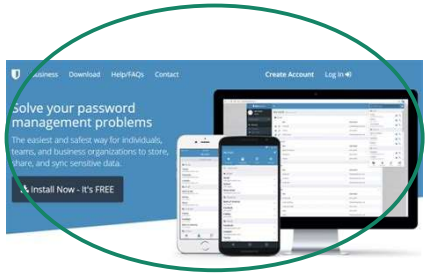
Browser / Konto -Passwort Manager

Browser-Add On / Konto	
• Je mehr Passwörter, desto schwerer ist es, sich diese auch tatsächlich zu merken. Browser wie Chrome oder Firefox bieten dann den vermeintlichen Luxus, die Passwörter automatisch zu speichern.	• Automatisch speichern
	• Wechsel Browser • Verlust / Diebstahl • Auf Web-Dienste beschr. • Nicht sicher • PW teilweise entschlüsselt gespeichert (ausser Apple) • Datenleck
• Sync zwischen gleichen Browser möglich • Sync zwischen verschiedene Geräte mit gleichen Browser möglich • Löschen von nicht gebrauchten Logins empfohlen • Empfehlung: Funktion «Passwort speichern» deaktivieren • Unbedingt ein Masterpasswort verwenden !	

Computeria Wallisellen

Passwort Manager

KeePass

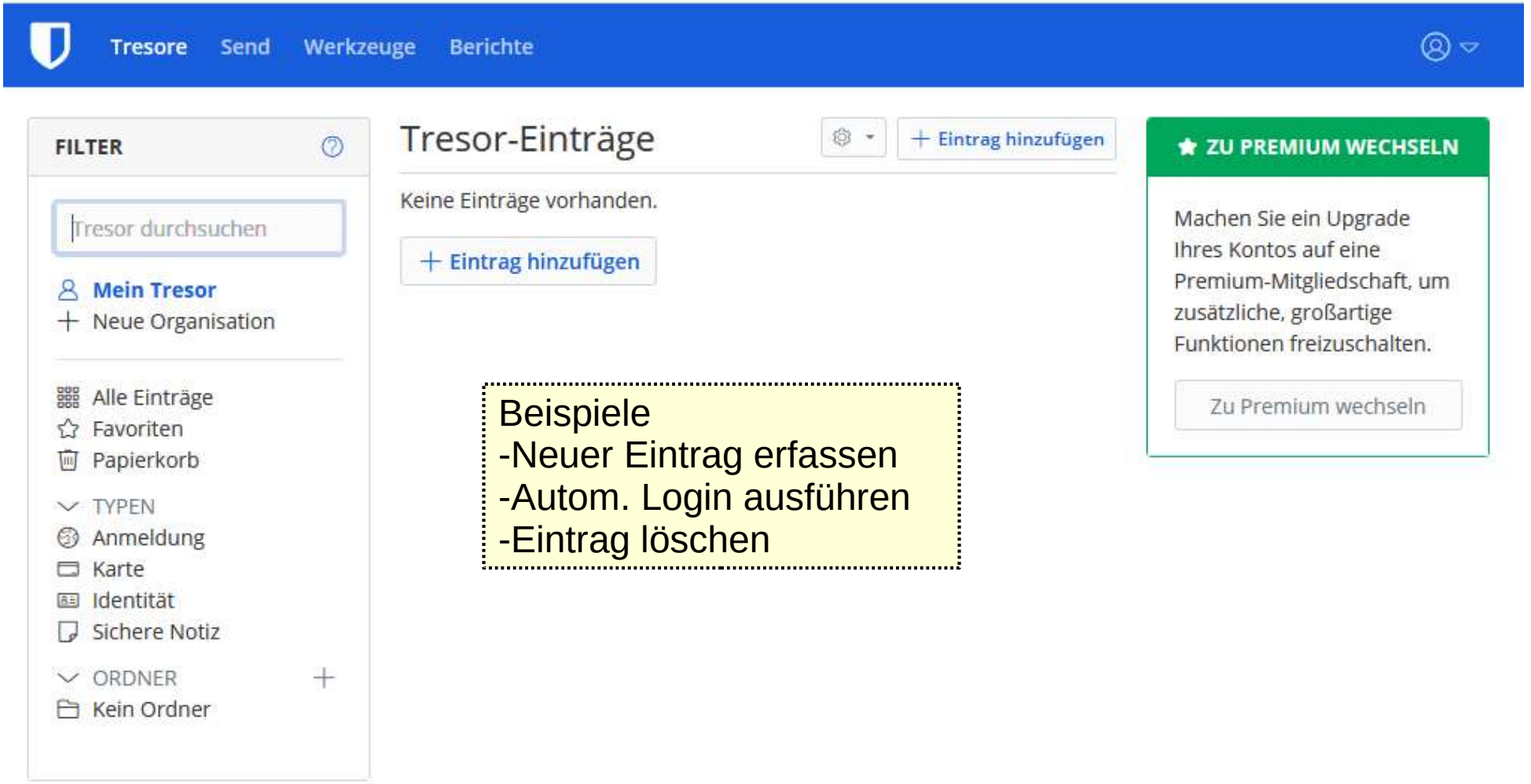


LastPass ****

1Password

- **Funktionen**
  - Passwörter generieren
  - Passwörter checken
  - Warnung vor gefährdeten Websites
  - übliche Verwaltung von PW
  - Familien-Funktion
  - Copy/Paste oder autom. Füllen (Autofill)
  - Nicht nur PW, sondern auch Bezahldaten, Ausweise, Dateien, Notizen,
    SSH Keys, SW-Lizenzen, Mitgliedschaften, ...
- **Konsequenzen**
  - Pro Gerät (PC, Tablet, Handy,..) ist Installation notwendig
  - Für einzelne Browser ein Add-On notwendig
  - Dauerhaft Zugriff auf DB nötig, Sicherung oder Claud
  - Lokale Installationen Immer aktuell halten
- **Vorteile**
  - Nur 1 Masterpasswort muss bekannt sein.
  - Liste PW als Backup drucken
- **Nachteile**
  - Bei erfolgreichen Cyberangriff → alle Zugriffe geknackt
  - Vergessen Masterpasswort → Verlust der Daten
  - Von der DB abhängig
  - Autom. Füllen funktioniert nicht immer
  - Claud-Lösung = Abhängig vom Provider
  - Wechsel vom Passwort Manager aufwendig

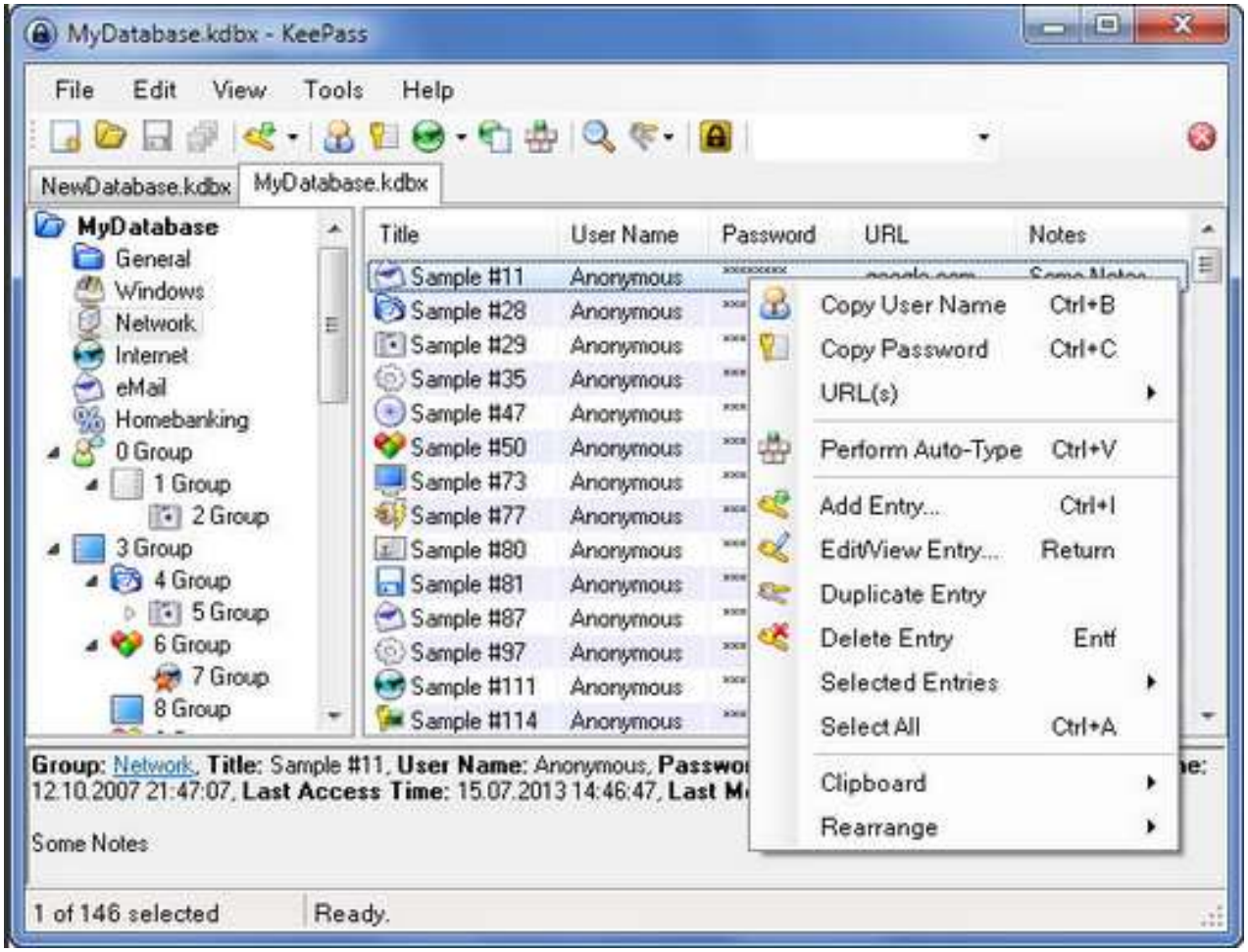
bitWarden



Beispiele
-Neuer Eintrag erfassen
-Autom. Login ausführen
-Eintrag löschen

Computeria Wallisellen

Keepass



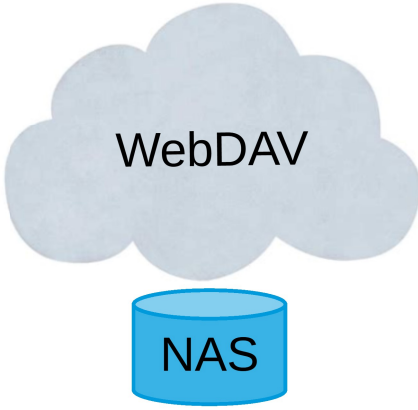
Passwörter Synchronisation

Synchronisation über das Konto
Google
Apple
Facebook

Synchronisieren Sie alle Ihre Geräte

Mit Bitwarden's sicheren Cloud-Synchronisierungsfunktionen können Sie von überall und von jedem Gerät aus auf Ihre Daten zugreifen! Ihr Tresor ist bequem für die Verwendung auf Desktop-, Laptop-, Tablet- und Telefongeräten optimiert.

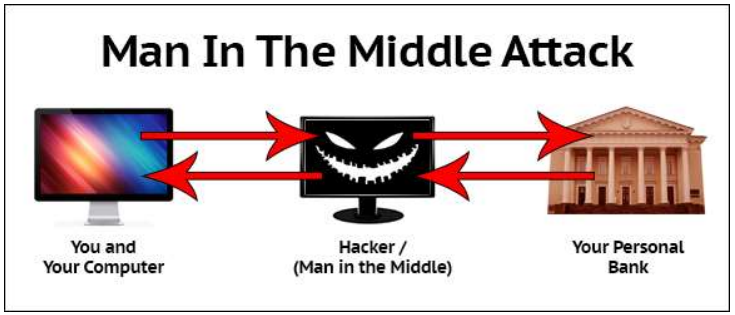
Da alle Ihre Daten vollständig verschlüsselt sind, bevor Sie Ihr Gerät verlassen, haben nur Sie Zugriff darauf. Nicht einmal das Team von Bitwarden kann Ihre Daten lesen, auch wenn sie wollten. Ihre Daten sind mit einer AES-256-Bit-Ende-zu-Ende-Verschlüsselung , Salted Hashing und PBKDF2 SHA-256 versiegelt.



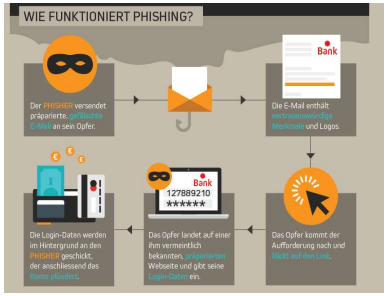
Computeria Wallisellen

Bedrohungen

Brute Force



Angriff der Wörterbücher



Phishing

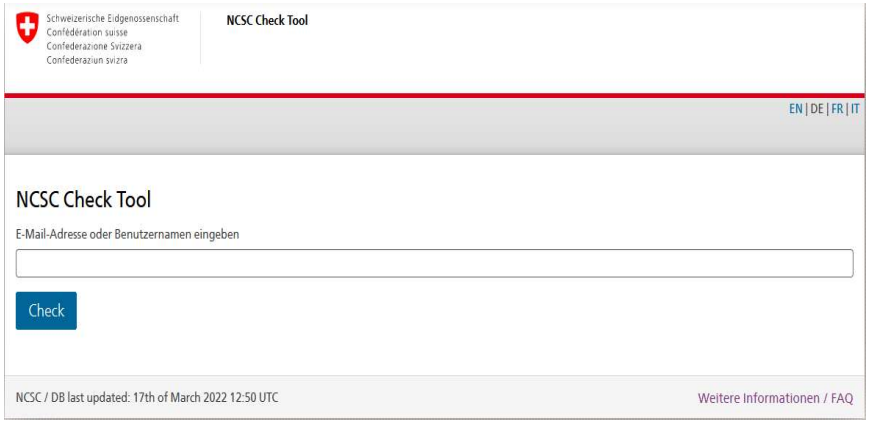
Skimming

Passwort verloren / vergessen

- Ein hektisches „Durchprobieren“ von verschiedenen Kombinationen sollte unbedingt unterlassen werden (Kontosperrung)
- Ganz gleich, um welches Passwort es sich handelt, in der Regel gibt es stets Möglichkeiten, ein vergessenes Kennwort zurückzusetzen.
- Anstatt wild rumzuprobieren, sollten entsprechend Dienst bzw. Gerät gezielte Lösungen gesucht oder ein entsprechender Kundendienst kontaktiert werden, um Sperrungen oder Löschungen zu vermeiden
- Systematisch vorgehen
  - Eingaben korrekt? (Feststelltaste / Rechtschreibefehler / Tastaturlayout)
  - Liegt keine Fehlfunktion der App vor?
  - Nutzen der Hilfefunktion des Anbieters (Passwort vergessen)
  - Bei Computer-Passwörter helfen Work-Arounds oder Systembackups
- Wenn Alles korrekt ist, dann könnte das Konto gehackt worden sein

Computeria Wallisellen

Passwort geknackt?



https://www.checktool.ch/

https://sec.hpi.de/ilc/

- Überblick verschaffen
- Reihenfolge festlegen
- Betroffene Passwörter der Reihe nach ändern
- Zuerst E-Mail Postfach
- Dann Single Sign On
- Dann die anderen Logins
- Rasch durchführen
- Einstellungen der Onlinekonten prüfen
- Verfolgen der Einstellungen
- Informieren

Computeria Wallisellen

Ansprech-/Informationsstellen

https://www.ncsc.admin.ch/ncsc/de/home.html

https://www.cybercrimepolice.ch/

Haben Sie Fragen zum Vortrag oder brauchen Sie Hilfe beim Handling von Passwörter?

Wir sind für Sie da

Computeria Wallisellen

https://www.computeria-wallisellen.ch/

Quellen

- Wikipedia (Authentifizierung,)
- https://www.verbraucherschutz.com/ratgeber/zwei-faktor-authentifizierung-wer-bietet-sicherheit/
- https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/smartphones-sicher-sperren-13788
- https://sicheres-passwort-generator.de/gutes-passwort-beispiele
- https://unsicherheitsblog.de/sicherheitsvorsorgeplan/passwoerter_kennwoerter
- https://unsicherheitsblog.de/tag/phishing
- https://www.antiphishing.ch/de/
- https://www.melani.admin.ch/melani/de/home.html
- https://krebsonsecurity.com/
- https://www.govcert.ch/statistics/
- https://sicheres-passwort-generator.de/
- https://www.google.de/search?&q=sex4me+rosebud+joshua+letmein+password
- https://sicheres-passwort-generator.de/passphrase.html
- https://haveibeenpwned.com/Passwords
- https://monitor.firefox.com/
- https://passwords.google.com/checkup/start
- https://www.heise.de/ct/ausgabe/2014-18-Kennwoerter-mit-Zettel-und-Stift-verwalten-2283904.html
- https://100woerter.de/die-100-haeufigsten-passwoerter

Veranlassung

Digitalisierung lässt Aktenordner verschwinden, durch die Nutzung der zahlreichen sozialen Netzwerke, die Kommunikation via E-Mail und Messaging-Diensten, den Austausch von Fotos entstehen neue Ablagearten.

Und tschüss...!

Was passiert mit meinen Daten / Accounts ?

Wie ist es geregelt wenn Sie durch Demenz, oder Tod Ihre Online-Accounts nicht mehr verwalten können?

Computeria Wallisellen

Rechtliches

Im Schweizer Erbrecht ist geregelt, dass eine Erbschaft als Ganzes auf die Erben übergeht. Somit fallen nicht nur alle vererblichen Vermögenswerte, sondern auch der digitale Nachlass in die Erbmasse. Aus rechtlicher Sicht besteht heute keine klare Regelung bezüglich der Persönlichkeitsrechte im Internet.

Immer öfter haben sich die nahestehenden Personen auch um das digitale Erbe des Verstorbenen oder Handlungsunfähigen zu kümmern.
Nach dem Tod kommt eine grosse Arbeit auf die Erben resp. auf den digitalen Willensvollstrecker zu. Denn es müssen unter anderem…

Social-Media-Profile gelöscht werden Verträge und Abos, die sich automatisch verlängern, gekündigt werden
Rechnungen bezahlt werden

Und daher sollten wir uns schon zu Lebzeiten über unseren digitalen Nachlass Gedanken machen.

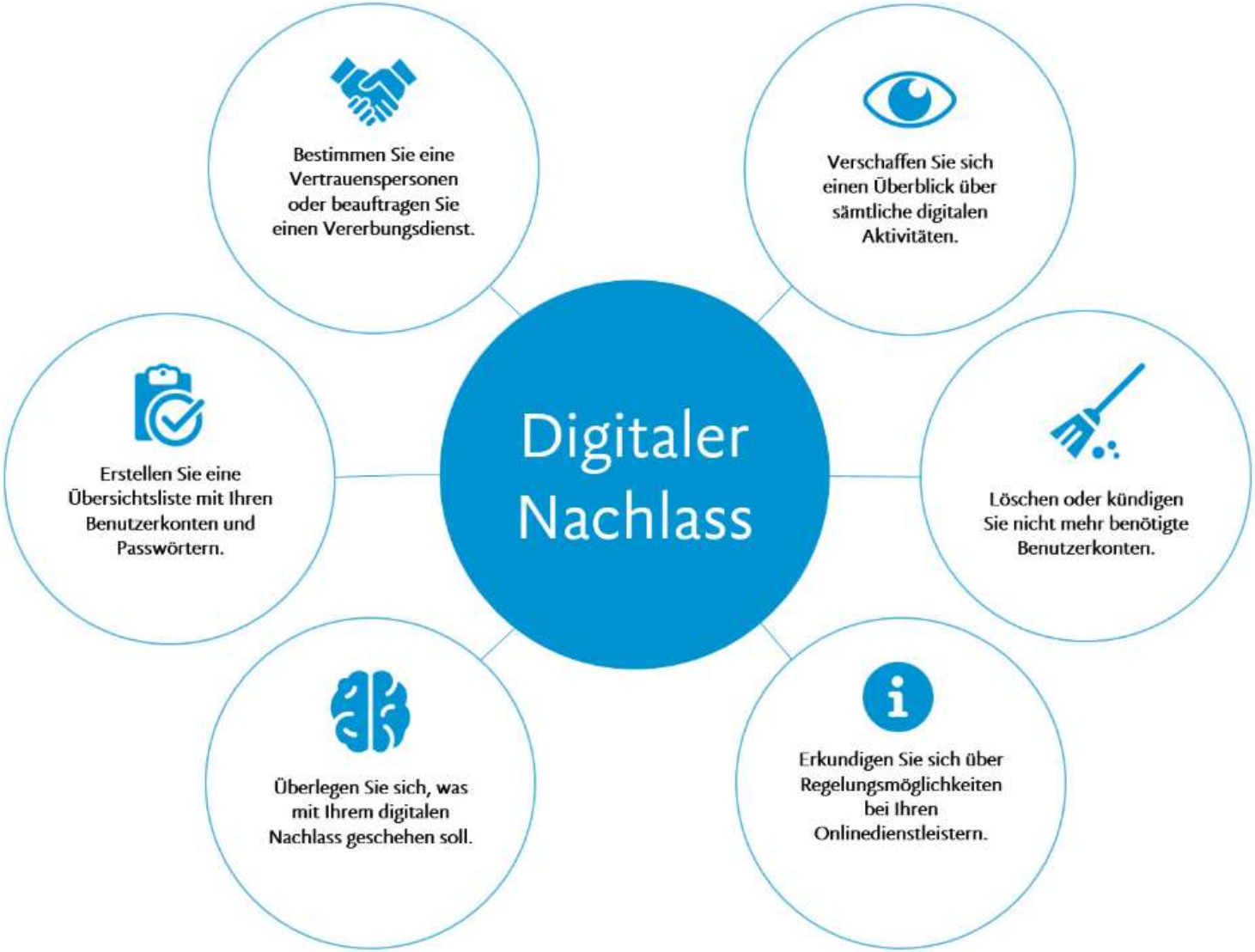
Umfang

Die Positionen eines verstorbenen Internetnutzers, insbesondere dessen

- Vertragsbeziehungen zu Host-, Access- oder E-Mail-Providern
- Vertragsbeziehungen zu Anbietern sozialer Netzwerke
  Beispiel: Facebook, Xing, Linkedin, Twitter usw.
- Vertragsbeziehungen zu Dating-Plattformen
  (eDarling, Parship, ElitePartner, Verlieb-dich, C-Date usw.),
  mit Kundennummer und Verträge inkl. Kündigungshinweisen.
- Name der Online-Shops inkl. allfälliger Bonusprogramme.
- Eigentumsrechte des Verstorbenen an Hardware, Clouddienst, bei dem Multimediadateien wie Fotos und Videos abgelegt sind.
- Nutzungsrechte an der Software, (lizenzen, Kostspielige Spiele mit Kündigungsinformationen)
- Urheberrechte und Rechte an hinterlegten Bildern, Foreneinträgen und Blogs dazu.
- Online-Banking bei einer bestimmten Bank inkl. Vertragsart, Vertragsnummer und mit Kündigungshinweisen.
- Weitere Online-Vermögen wie Paypal und digitale Währungen (Kryptowährungen!)
- Rechte an Webseiten "www."

usw..

Vorkehrungen



Computeria Wallisellen

Vorkehrungen

- Erstellen Sie eine **Liste der von Ihnen in Anspruch genommenen digitale Dienstleistungen**
- Was soll damit geschehen? Bsp: Der Account soll gelöscht werden.
  Die YouTube-Videos sollen online belassen werden.
  Eine Website soll durch eine andere Person weitergeführt werden.
- Bestimmen Sie ebenfalls, was mit Ihren Endgeräten (Computer, Smartphone, Tablet) und den dort gespeicherten Daten geschehen soll

1. @ E-Mail-Dienste:

Name des Anbieters:	*[hier nennen Sie den Namen des Anbieters oder der Webseite, z.B. Google (gmail), Posteo oder web.de]*
Benutzername:	*[hier den Namen und/oder Alias eintragen, unter dem das E-Mail-Konto geführt wird, z.B. Max.Mustermann@posteo.de]*
Passwort:	*[hier geben Sie das Passwort für das E-Mail-Konto an, z.B. Ht7w1?LhK!; Tipps zu sicheren Passwörtern finden Sie unter: www.verbraucherzentrale.nrw]*
Mit Konto soll passieren:	*[hier sollten Sie so genau wie möglich festlegen, was mit dem E-Mail-Konto passieren soll, wie z.B. "Account löschen" oder im Fall eines Accounts mit kostenpflichtigem Premium-Zugang (z.B. WEB.de Club-Mitgliedschaft): "Account kündigen und Account löschen"]*

- Kann in bereits existierenden Passwort-Verwaltungsmethodik integriert werden.
- WICHTIG Sämtlich Zugangsdaten wie E-Mail und Passwörter müssen sicher aufbewahrt werden

Computeria Wallisellen

Vorkehrungen ff

- Bestimmen Sie einen Verwalter des digitalen Nachlassens
  Diese Vertrauensperson benötigt nach Ihrem Ableben Zugriff auf Ihre Passwortliste und muss gute EDV- und Internetkenntnisse besitzen. Dies kann zum Beispiel der gewählte Willensvollstrecker sein.
  Orientieren Sie diese Person unbedingt im Voraus

- Erstellen Sie eine handschriftliche Vollmacht, mit einem Datum versehen und unterschrieben.
  Unabdingbar ist ausserdem, dass sie „über den Tod hinaus“ gilt.

- Falls «Patientenverfügung» und / oder «Vorsorgeauftrag» existieren, dieses entsprechend ergänzen

Muster-Vollmacht für digitale Konten

Ich, [*Vor- und Zuname*], geboren am [*Geburtsdatum*] in [*Geburtsort*], wohnhaft in [*Anschrift mit Straße, Hausnr., PLZ und Ort*]

erteile ich hiermit eine Vollmacht für die Verwaltung meiner digitalen Vorsorge und meines digitalen Nachlasses :

Herrn/Frau [*Vor- und Zuname*] - nachfolgend Vertrauensperson genannt - geboren am [*Geburtsdatum*] in [*Geburtsort*], wohnhaft in [*Anschrift mit Straße, Hausnr., PLZ und Ort*]

Meine Vertrauensperson wird bevollmächtigt, meine digitale Vorsorge zu Lebzeiten und auch meinen digitalen Nachlass im Falle meines Todes so zu regeln, wie ich es in der hinterlegten Liste meiner Accounts festgelegt habe. Die Vertrauensperson kennt den Aufbewahrungsort dieser Liste. Diese Vollmacht ist nur wirksam, wenn die Vertrauensperson das Original dieser Vollmachtsurkunde besitzt und sie auf Verlangen vorlegen kann. Diese Vollmacht gilt über meinen Tod hinaus.

_____ _____

Ort, Datum Unterschrift

Tipps für Betroffene

- Halten Sie die Liste der Accounts aktuell
- Hinterlegen Sie das Dokument auf Papier oder doppeltem Datenträger an einer Stelle, auf die Ihr Erbe Zugriff hat.
  Am besten werden diese Informationen zusammen mit der Vorsorgevollmacht und dem Testament aufbewahrt
- Löschen Sie bereits jetzt Accounts, die Sie nicht mehr verwenden.
  Folgender Link kann Ihnen dabei helfen: http://backgroundchecks.org/justdeleteme/de.html
- Einige Provider im Internet (Google, Facebook) bieten die Möglichkeit an, Vorkehrungen für das Ableben zu treffen. Nutzen Sie diese Möglichkeiten
- Sensible Zugangsdaten können auch auf einem USB-Stick gespeichert werden.
- Falls Sie Kryptowährungen besitzen, denken Sie an die Sicherung der Zugangsdaten/Key

Tipps für Hinterbliebene / digitaler Nachlassverwalter

- Geben Sie keine Endgeräte wie Tablets, Handy, Computer aus der Hand, ohne vorher die Daten analysiert und entfernt zu haben (Krypto!).
- Suchen Sie die Passwortliste
- Versuchen Sie, Zugang zum E-Mail-Konto zu erhalten.
  Darin lassen sich viele weitere Online-Konten entdecken.
  Ausserdem laufen viele Verträge und Transaktionen über den E-Mail-Verkehr ab
-
- Schaffen Sie sich einen Überblick über die Onlineaktivitäten des Verstorbenen
- Ermitteln Sie die kostenpflichtigen Dienste, denn diese müssen von den Erben weiterhin bezahlt werden. Kündigen Sie diese so rasch als möglich und löschen Sie die Benutzerkonti.
- Kündigen oder löschen Sie anschliessend auch die übrigen Online-Zugänge
- Verfahren Sie nach den Vorgaben des Erblassers und löschen bzw. sichern Sie den digitalen Nachlass nach seinen Wünschen
- Ohne Zugangsdaten sind Erben auf die Hilfe der Webanbieter angewiesen. Kontaktieren Sie diese.

Quellen/Weiterführende Links

- https://www.erbplaner.ch/erbtipp/ihr-erbplan/der-digitale-nachlass/
- http://backgroundchecks.org/justdeleteme/de.html

Vielen Dank