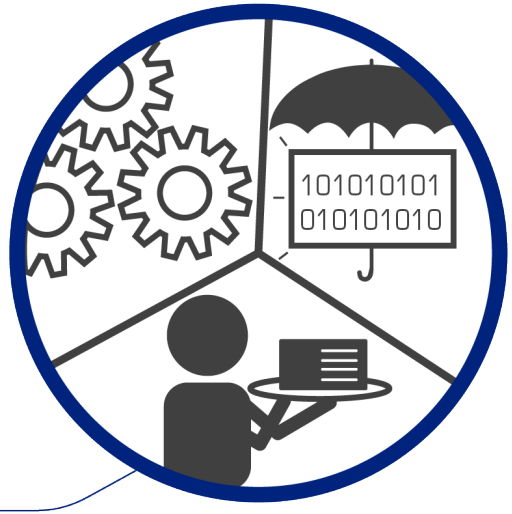
Immer diese verfluchten Passwörter…

Katja Dörlemann & Jakob Dhondt
cert@switch.ch

Zürich, 27. Februar 2021

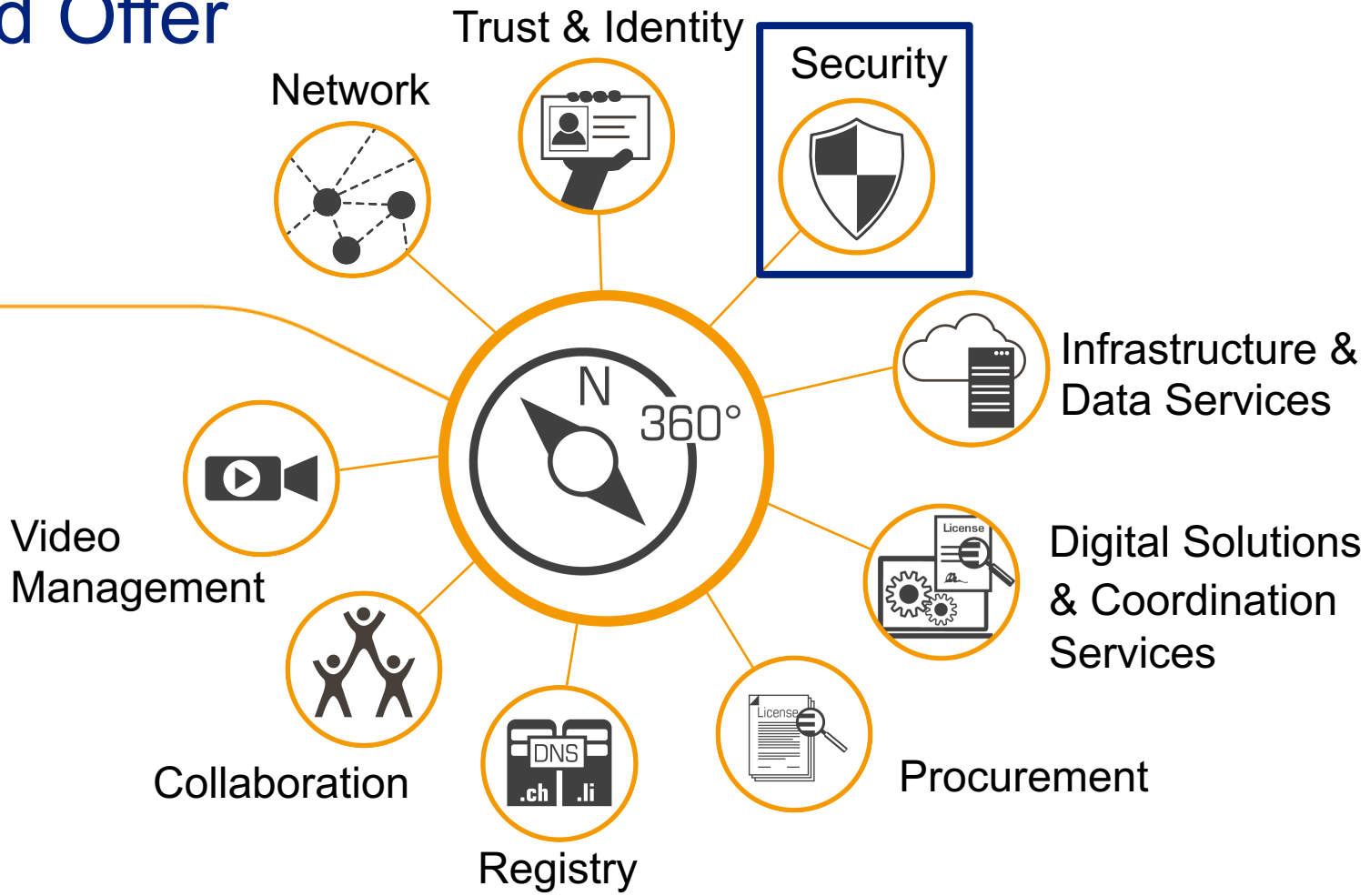
Was wir machen



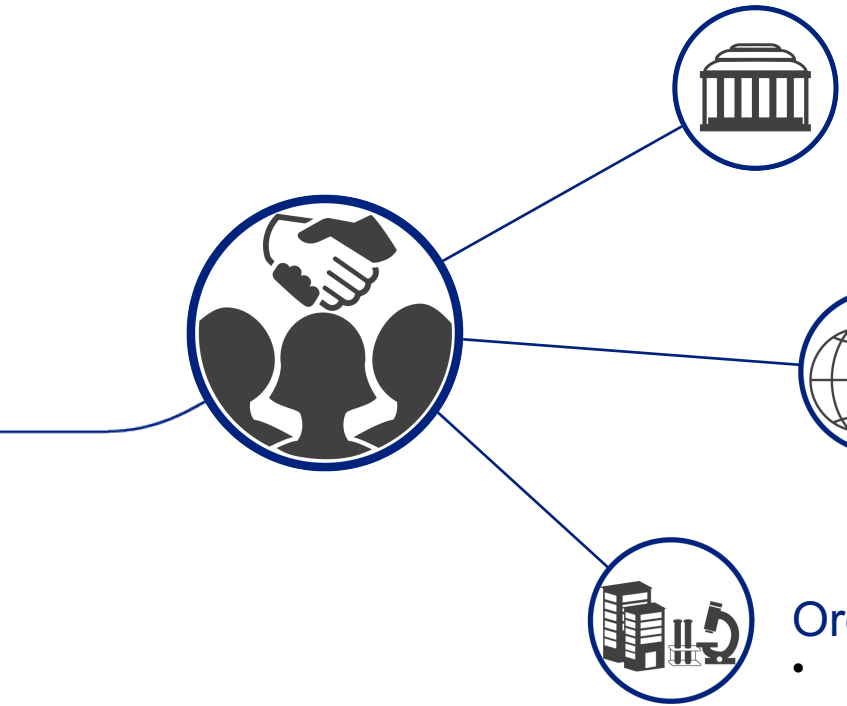
NREN (National Research und Education Network)

Registry für .ch/.li - cc TLDs

Integrated Offer



Unsere Kunden



Bildungs-, Forschungs- & Innovations- (BFI) Community

- Schweizer Hochschulen sowie Forschungsanstalten des ETH-Bereichs
- Erweiterte BFI Community

Internet Community

- Internet Service Provider, Hoster, Domain Registrare

Organisationen der kritischen Infrastrukturen

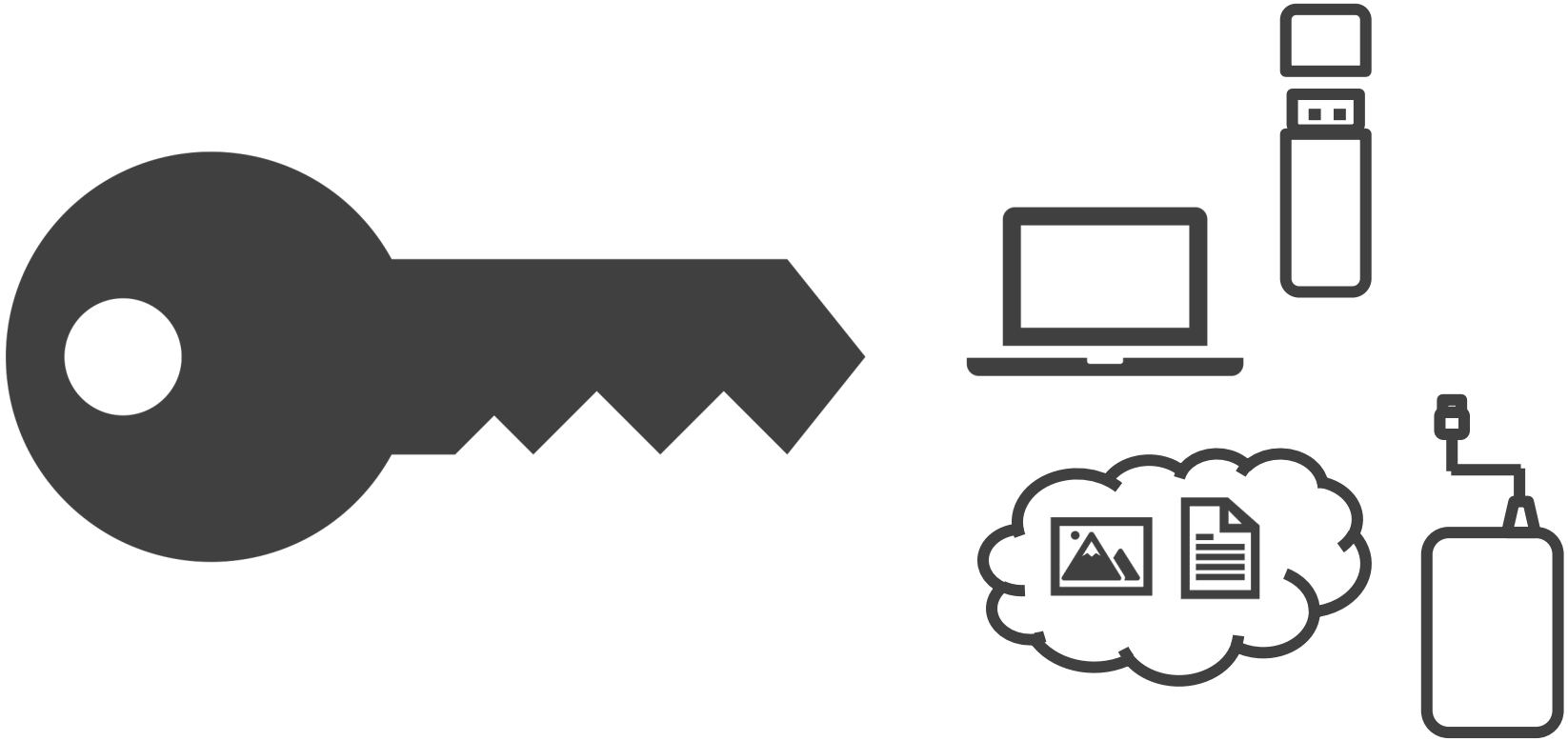
- Banken, Industrie & Logistik, Energie, Gesundheitswesen, Behörden und Verwaltungen

80% der Sicherheitsvorfälle gehen auf gestohlene oder mit der Brute-Force-Methode geknackte Passwörter zurück.

– 2020 Data Breach Investigations Report | Verizon

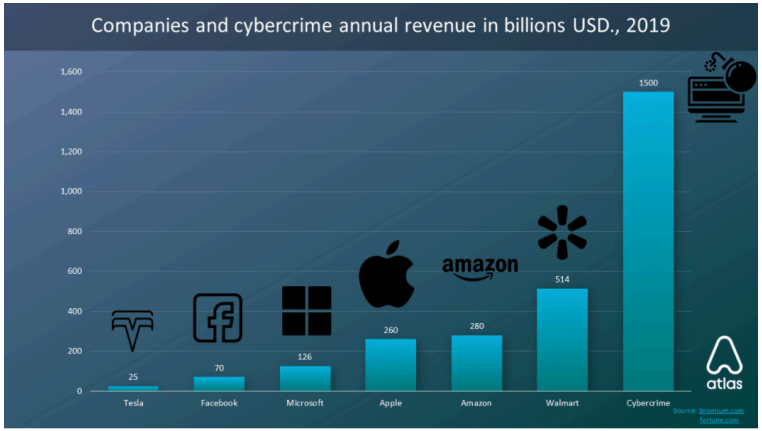
https://enterprise.verizon.com/resources/reports/dbir/


Bluewin



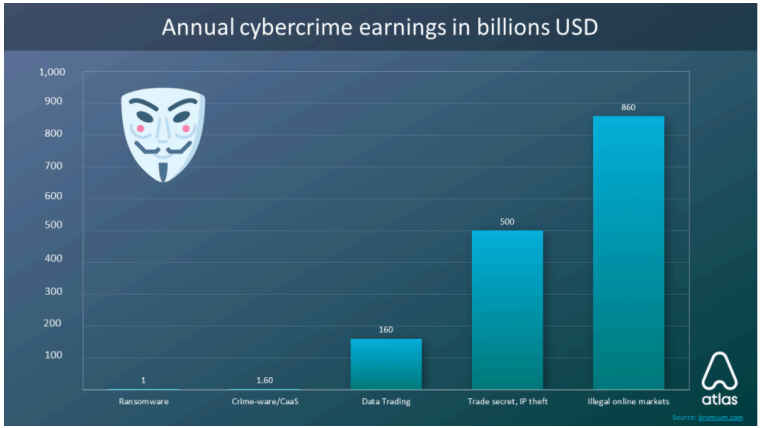
Cybercrime

1.5 Billionen Dollar



Data Trading

160 Milliarden Dollar



https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts

Dashlane’s Worst Password Offenders of 2020

1. Twitter	Juli	130 bestätigte Accounts posteten Bitcoin scams.
2. Zoom	April	500’000 Zugangsdaten standen zum Verkauf.
3. EasyJet	Januar/April	9 Mio. E-Mail-Adressen und Flugdaten, über 2’000 Kreditkartendaten.

https://blog.dashlane.com/twitter-employees-and-zoom-users-top-dashlanes-list-of-2020s-worst-password-offenders/

> *Putting a password on for each individual user as a lock seemed like a very **straightforward** solution.*
>
> – Fernando Corbató, US-amerikanischer Informatiker

https://www.wired.com/2012/01/computer-password/

- 1961 -
Erster Computer mit Passwortfunktion

- Compatible Time-Sharing System (CTSS)
- MIT
- genutzt bis 1973.

- 1962 -
Erster Passwort-Diebstahl

- Doktorand Allan Scherr benötigt mehr Rechenzeit für Simulationen.
- druckt Passwort-Datei aus.

https://www.wired.com/2012/01/computer-password/

- 1961 -
Allens Passwörter

1

- 1961 - Allens Passwörter	1
- 2021 - Katjas Passwörter	79
- 2021 - Jakobs Passwörter	103

Steigende Cyberkriminalität

Steigende Cyberkriminalität

- Längere Passwörter!
- Komplexere Passwörter!
- Regelmässiger Passwortwechsel!

Nutzer:innenfreundlich?

- 1999 -
Studie zeigt, Passwortwechsel macht keinen Sinn

«Users required to frequently change their passwords were found to be producing passwords with less secure content and disclosing their passwords more frequently.»
- Sasse, Adams, Lundt: Making Passwords Secure and Usable.

- 2017 -
Update NIST Guidelines

«Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.»
- Update: NIST SP 800-63B Digital Identity Guidelines.

https://www.researchgate.net/publication/2320831_Making_Passwords_Secure_and_Usable
https://pages.nist.gov/800-63-FAQ/#q-b05

IT-Experten küren Mb2.r50Hf-0t zum sichersten Passwort der Welt

– Der Postillon. Zum Passworttag.

https://www.der-postillon.com/2014/04/sicherstes-passwort.html

Internet of Shit gefällt das

Adrienne Porter Felt
@__apf__

what's your favorite password and why?

Tweet übersetzen

03:21 · 31.12.20 · Twitter for Android

150 Retweets **112** Zitierte Tweets

1.729 „Gefällt mir"-Angaben

Antony Jones @antony · 1T
Antwort an @__apf__

I've got a serious answer, sorry :(

We wanted a team password which was secure but memorable. Before password managers were common.

So we took one of our "team norms" we had on the wall. We md5d it and took the last 16 chars.

Hidden in plain sight.

2 11

w00t @wmertens · 1T
16 chars of an md5 is memorable? 🤔

3

QAnton gefällt das

John Opdenakker
@j_opdenakker

Don't forget to increase the year in your password.

Tweet übersetzen

18:39 · 01.01.21 · Twitter for iPhone

212 Retweets **32** Zitierte Tweets

742 „Gefällt mir"-Angaben

Michal Špaček @spazef0rze · 5h
Antwort an @j_opdenakker

Just use your birthyear

Ed Tucker @Teddybreath · 5h
Antwort an @j_opdenakker

I'm not falling for that! I'll only have to change it again when the twats in security force me to! Better to wait for them and then change it!

4

unix-ninja @unix_ninja · 2h
Antwort an @j_opdenakker

Or don't. It doesn't matter to hashcat either way. 😇

3

Abhay Shah @_abhayshah · 1h
Antwort an @j_opdenakker und @JustinList

Huh, must be nice to only change your password 1x a year

1 1

Justin List @JustinList · 1h
Myname2021 now . Like clockwork

1

Antworten anzeigen

Top 10 CH-Passwörter

2019

1. 123456
2. 123456789
3. 12345678
4. password
5. 1234567
6. abc123
7. 123123
8. 1234567890
9. Switzerland
10. 111111

Datengrundlage sind 1,7 Millionen Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers, die auf E-Mail-Adressen mit .ch-Domäne registriert sind und 2019 geleakt wurden.

Top 10 CH-Passwörter

2019

1. 123456
2. 123456789
3. 12345678
4. password
5. 1234567
6. abc123
7. 123123
8. 1234567890
9. Switzerland
10. 111111

Datengrundlage sind 1,7 Millionen Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers, die auf E-Mail-Adressen mit .ch-Domäne registriert sind und 2019 geleakt wurden.

2020

1. 123456
2. 123456789
3. passwort
4. 12345678
5. 1234567890
6. hallo123
7. qwertzuiop
8. 1234567
9. lolipop
10. Passwort

Datengrundlage sind 45’882 Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers, die auf E-Mail-Adressen mit .ch-Domäne registriert sind und 2020 geleakt wurden.

Data Breaches!!!

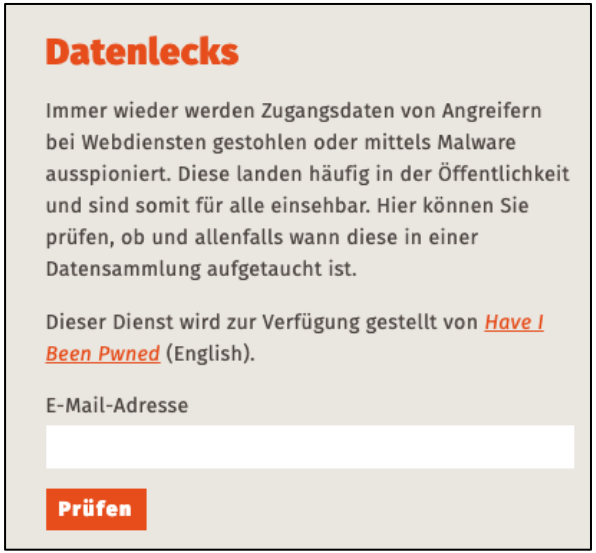
Entity	Year	Records
Animal Jam	2020	46,000,000
Betsson Group	2020	unknown
CheckPeople	2020	56,000,000
Clearview AI	2020	unknown (client list)
FireEye	2020	Unknown
Instagram	2020	200,000,000
Koodo Mobile	2020	unknown
Marriott International	2020	5,200,000
Nintendo (Nintendo Account)	2020	160,000
Now:Pensions	2020	30,000
ShopBack	2020	unknown
SlickWraps	2020	377,428
Solarwinds	2020	Unknown
Tetrad	2020	120,000,000
TikTok	2020	42,000,000
U.S. federal government (2020 United States federal government data breach)	2020	TBC
Virgin Media	2020	900,000
Wattpad	2020	270,000,000
Wawa (company)	2020	30,000,000
YouTube	2020	4,000,000
Unknown agency (believed to be tied to United States Census Bureau)	2020	200,000,000
National Health Information Center (NCZI) of Slovakia	2020	391,250
Les Éditions Protégez-vous	2020	380,000

https://en.wikipedia.org/wiki/List_of_data_breaches

Have I been pawnd? Melani Checktool

https://haveibeenpwned.com/

https://www.checktool.ch/



https://www.ibarry.ch/de/sicherheits-checks/

Methoden zum Passwortdiebstahl

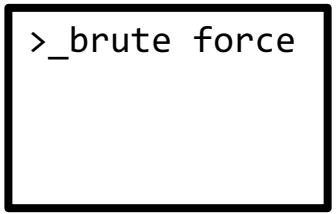
Social Engineering	• Phishing • CEO-Fraud • IT-Scam
Raten	• Kombination • Notizzettel • Brute-Force-Angriffe • Dictionary Attacks

Mehr Info: https://www.security-insider.de/die-spannende-geschichte-der-passwoerter-a-930811/

Data breaches – hash

ooops

password hash:
`4579c2a3a3b3a0b4870521a8bbdea3f5`



PW: *****

< 2 min.

PW: ooops

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

Cybersecurity that's approachable.

Find out more at hivesystems.io

Empfehlungen für Passwörter

1. Einzigartige Passwörter	Passwortmanager!
2. min. 12 Zeichen	Gross-, Kleinbuchstaben, Sonderzeichen und Zahlen
3. Multi-Faktor-Authentifizierung	MFA, 2FA etc.

Lastpass-Studie

Was Menschen wissen

- 91% wissen, dass das Recyclen von Passwörtern riskant ist
- 80% sind besorgt, dass ihre Passwörter gestohlen werden
- 77% wissen Bescheid über Passwort Best Practices

Was Menschen tun

- 66% recyclen immer oder meistens das gleiche Passwort oder Variationen
- 48% ändern nie ihr Passwort
- 54% merken sich all ihre Passwörter auswendig

https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/de/LastPass-B2C-Assets-Ebook-FINAL-de-screen.pdf

Woran scheitert’s?

Passwortwahl vs. -umgang	Mit der Wahl eines starken Passworts ist es nicht getan.
Vorurteile gegenüber Passwort-Managern	Die Frage ist, wem wir vertrauen wollen.
Begriffe: 2FA? MFA? TwoFA?	Uneinheitliche Verwendung von Begriffen sorgt für Verwirrung.
Priorität ≠ Security.	Klassiker.

Aktuelle Alternativen?

Biometrie	• Fingerabdruck • FaceID
SSO Single Sign On	• EduID • SwissPass • SwissID …
FIDO 2 Fast IDentity Online	• Physischer Token • App • Mehrere Anbieter

https://www.security-insider.de/die-spannende-geschichte-der-passwoerter-a-930811/
https://www.heise.de/select/ct/2019/18/1566917336782380

Device Biometrics (z.B. Touch-ID)

Die Device Biometrics sind am Markt schon längst bekannt und akzeptiert. Fast jeder Nutzer eines Smartphones hatte bereits einmal Touch-ID, den Android Fingerprint oder andere Verfahren für den Zugang zum Smartphone benutzt. Überraschen Sie Ihren Nutzer mit Device-Biometrics auf Ihren digitalen Kanäle, im Portal oder der App.

Gesichtserkennung

Mit der Gesichtserkennung können Sie Ihre Nutzer sicher und bequem an jedem kamerafähigen Gerät identifizieren. Ob an der Tür, der Maschine oder am Handy, die Einsatzszenarien für die geräteunabhängige Gesichtserkennung sind vielzählig.

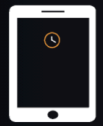
WebAuthn (Fido2)

Per WebAuthn kann der Nutzer sicher und komfortabel im Webbrowser authentifiziert werden. Der Nutzer kann einfach das biometrische Verfahren des Devices nutzen, beispielsweise die Touch-ID des Mac, den Android Fingerprint oder Windows Hello, um seine Identität zu bestätigen.

Voice ID (Stimmerkennung)

Durch die cidaas Stimmerkennung kann der Nutzer sich bequem über sein Stimmprofils authentifizieren.

Time-based one-time Passwort



Beim TOTP (Time-based One-time Password) erhält der Nutzer einen temporären, sechs- oder achtstelligen Zugangscode. Unter Berücksichtigung der Uhrzeit und des Geräts wird der Benutzer sicher und passwortlos authentifiziert. Da er nur zeitweise gültig ist, wird ebenfalls das Schadenspotential reduziert, falls er zum Beispiel durch Phishing in falsche Hände gerät.

Smart-Push

Bei Smart-Push wird dem Nutzer eine Push-Benachrichtigung an das registrierte Mobilgerät gesendet. Der Nutzer kann sich darüber problemlos und sicher über Ihre App oder einer Authenticator-App identifizieren.

E-Mail

Anstatt sich Passwörter zu merken, erhält der Nutzer anlassbezogen, bei einem Authentifizierungsevent per E-Mail einen Code. Da mittlerweile fast jeder ein E-Mail Konto besitzt, ist diese Verfahren weit verbreitet und eine gute Alternative.

SMS

Bequem per SMS erhält der Nutzer über seine angegebene Mobilfunknummer einen Code, den er im entsprechenden Authentifizierungsfeld eingibt. Das Verfahren ist bereits in vielen Branchen Normalität und kann einfach unterwegs verwendet werden. Zusammen mit der cidaas Betrugserkennung wird es zu einem praktischen, passwortlosen Authentifizierungsalternative.

https://www.tschuesspasswort.de/

> *Meine Meinung zu Passwörtern ist, dass sie sterben müssen.*
>
> – Rolf Brugger, SWITCH eduID

Forschung & Dienstleistung, Information & Cyber Security, Privacy

«Auf passwortfreie IT-Sicherheit werden wir noch einige Jahre warten»

Prognosen von unseren Expertinnen und Experten: Teil 4

Was ist im Bereich Information & Cyber Security | Privacy in nächster Zeit zu erwarten? Björn Näf spricht in diesem Interview über die verschärfte Cybersicherheits-Lage, malewarefreies Internet und die Utopie der totalen Sicherheit.

Worauf werden wir noch sehr lange warten müssen?

Auf passwortfreie IT-Sicherheit werden wir sicherlich noch einige Jahre warten müssen. Auf ein malware-freies Internet noch länger.

https://hub.hslu.ch/informatik/auf-passwortfreie-it-sicherheit-werden-wir-noch-einige-jahre-warten/

Biometrische Daten	Schon im Einsatz. Schwäche: Nicht ersetzbar.
Zero-Login	Login auf Basis von Verhalten Schwäche: Logout? Datenspeicherung?
Mikrochip-Implantate	Physischer Eingriff
Brain Password	Gehirnaktivitäten
DNA-Identifikation	Datenpool ist da Technologie fehlt (noch)

https://www.it-daily.net/it-sicherheit/datenschutz-grc/21315-fuenf-passwort-alternativen-der-zukunft

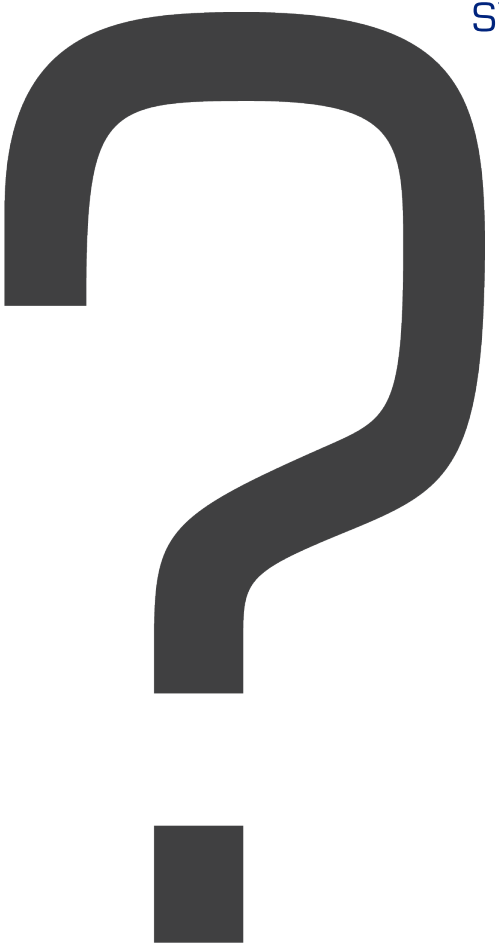
eduID

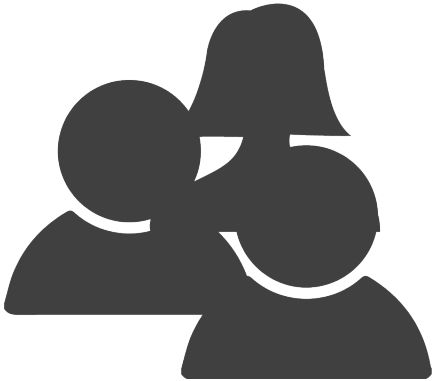
Facebook

One ID to rule them all?

Google

Passwortmanager





Human centered Security

Research

Human-Centred Security: Addressing psychological vulnerabilities

RESEARCH-ARTICLE

Passwords and the evolution of imperfect authentication

Authors: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano

Authors Info & Affiliations

Publication: Communications of the ACM • June 2015 • https://doi.org/10.1145/2699390

"Information security should put humans at the centre. If they truly are security's 'weak point' then start by understanding their vulnerabilities and managing them"

ELSEVIER

Journal of Information Security and Applications

Volume 34, Part 1, June 2017, Pages 76-81

Contemplating human-centred security & privacy research: Suggesting future directions

Karen Renaud [a] ✉, Stephen Flowerday [b] ✉

Human-Centred Security: Positively influencing security behaviour

About this webinar

Human error and negligence still contribute to a significant number of security incidents, yet current approaches to mitigating this risk are failing to have the desired impact. Many organisations have not always prioritised the effective management of this risk and have historically relied upon security awareness to influence security behaviour. Yet this only resolves a small part of the problem and neglects other factors. A robust human-centred security programme is required.

Why human-centred cyber security is the future

Superscript Nov 27, 2017 · 4 min read

https://www.researchgate.net/publication/318284979_Contemplating_human-centred_security_privacy_research_Suggesting_future_directions
https://www.securityforum.org/research/human-centred-security/
https://www.brighttalk.com/webcast/9923/456327/human-centred-security-positively-influencing-security-behaviour
https://gosuperscript.com/blog/why-human-centred-cyber-security-is-the-future/
https://dl.acm.org/doi/10.1145/2699390

RUHR-UNIVERSITÄT BOCHUM

A-Z | OVERVIEW | SEARCH | CONTACT

RUB

MOBILE SECURITY

TEACHING

RUB » EI » MOBSEC » Teaching » Courses » Usable Security and Privacy

INTRODUCTION TO USABLE SECURITY AND PRIVACY (BACHELOR)

Die Studierenden verstehen die grundsätzliche Problematik und Wichtigkeit der Benutzbarkeit von technischen Systemen durch Menschen, insbesondere im Umgang mit IT Sicherheitstechnik. Darüber hinaus erlangen sie ein grundlegendes Verständnis von Methoden und zentralen Erkenntnissen der Usable Security und Privacy Forschung, sowie grundlegende Handreichungen für die Praxis. Die Vorlesung behandelt insbesondere folgende Themen:

- **Einführung**
  - Überblick
  - Entstehung des Forschungsgebietes
  - Grundlagen menschlichen Verhaltens in der IT Sicherheit
- **Methodische Grundlagen**
  - Einführung Quantitative Methoden (z. B. Usability-Experimente)
  - Einführung Qualitative Methoden (z. B. Interviews/Umfragen)
  - Statistische Methoden (deskriptive Statistik, statistische Tests)
- **Zentrale Anwendungen**
  - Benutzbare Authentifizierung
  - Warndialoge/Phishing
  - Verschlüsselungstechniken von Dateien und Kommunikation
  - Security Awareness
  - Developers
  - Operators

Lecture: Introduction to Usable Security and Privacy

USABLE SECURITY AND PRIVACY (MASTER)

Diese Veranstaltung vermittelt Kenntnisse der Usable Security und Privacy. Die Studierenden verstehen, warum die Usability technischer Systeme entscheidenden Einfluss auf deren Sicherheit haben kann. Darüber hinaus sollen Sie in die Lage versetzt werden, einfache Studien zur Usability selbst durchzuführen. Die Vorlesung behandelt insbesondere folgende Themen:

- **Überblick**
  - Benutzbare Authentifizierung
  - Nutzer und Phishing
  - Vertrauen/Trust, PKI, PGP
  - Privatheit und Tor
  - Privacy policies
  - Design und Auswertung von Benutzerstudien

Lecture: Usable Security and Privacy

https://www.mobsec.ruhr-uni-bochum.de/lehre/courses/usable_security_and_privacy/

SWITCH

Working for a better digital world

Katja Dörlemann & Jakob Dhondt
cert@switch.ch