Fantastische Maßnahmen und wo sie (nicht) zu finden sind

Mache Updates

Gebe deine Passwörter nicht weiter

Nutze Ad-Blocker

Verschlüssle deine Daten

Achte auf deine Datenschutz-Einstellungen

Verwende Virenscanner

Nutze VPN

Nutze extra privatsphäre-freundliche Apps

MACHE BACKUPS

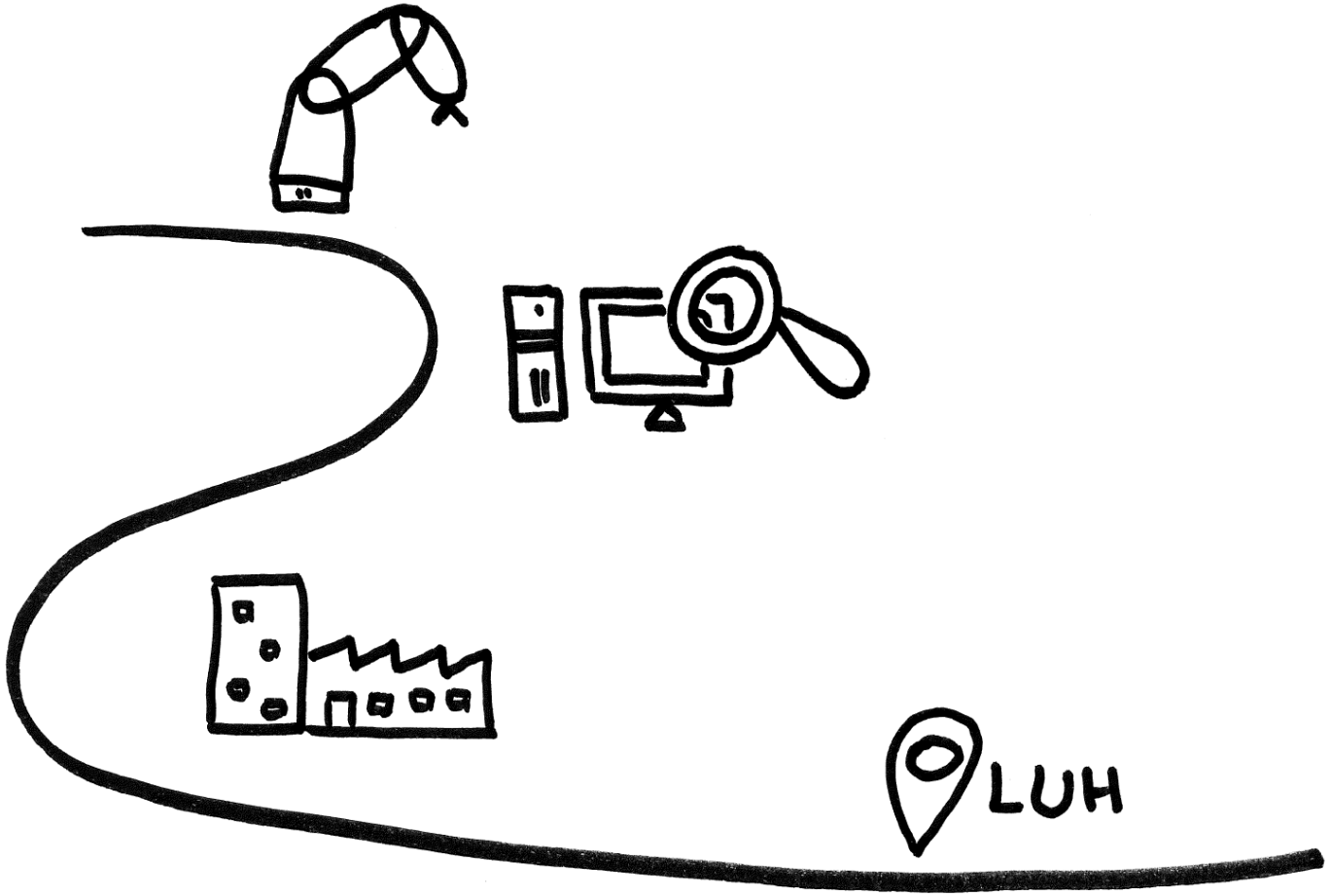
Lehne Cookies immer ab

Nutze unterschiedliche Passwörter für unterschiedliche Accounts

Benutze den Inkognito-Modus

Und welche Maßnahmen machst du (nicht)?

Maike M. Raphael


LUH

Unsere heutigen Themen...

Wie kommt man eigentlich an Maßnahmen?

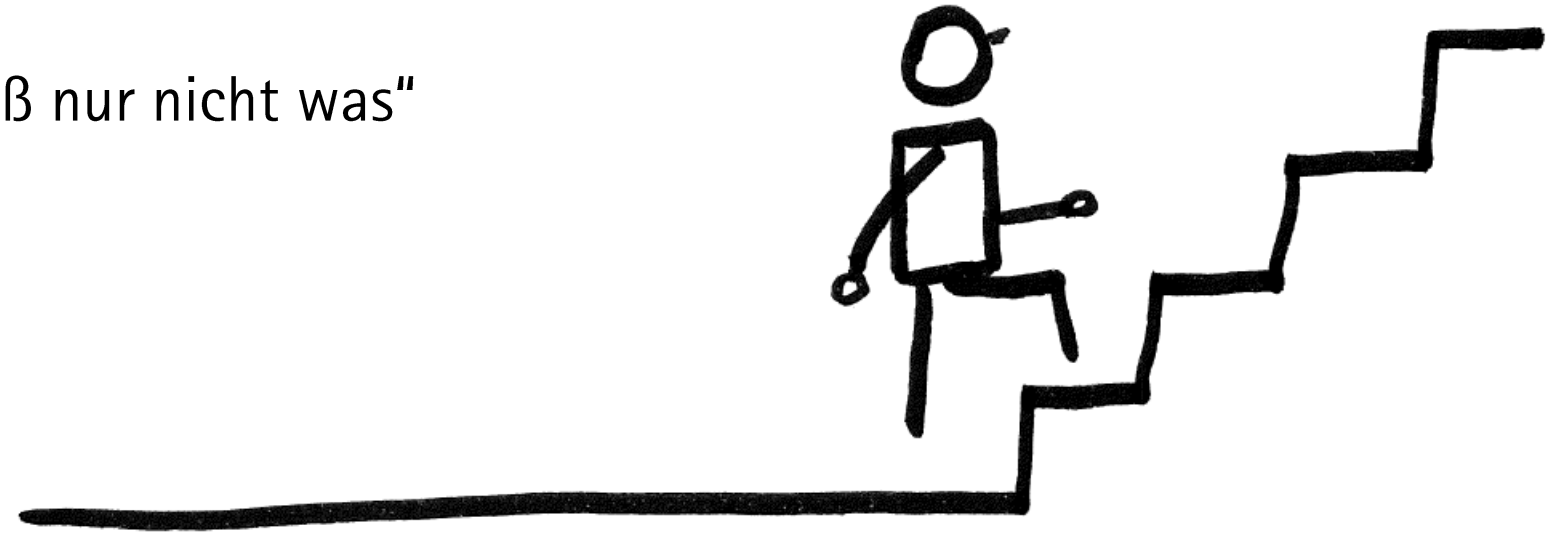
Was kann alles schief gehen?

Was kann ich machen?

Am Anfang …

„Ich will ja was tun…

…ich weiß nur nicht was“



Wie komme ich ran an die Maßnahmen?

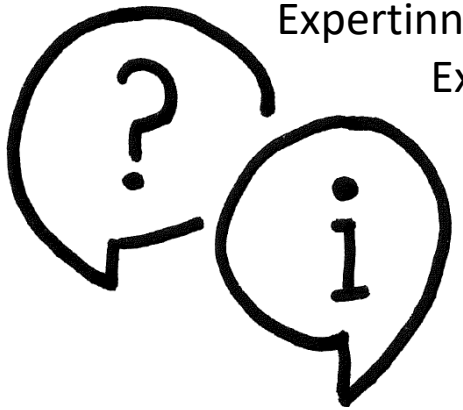
Welche Maßnahmen gibt es?

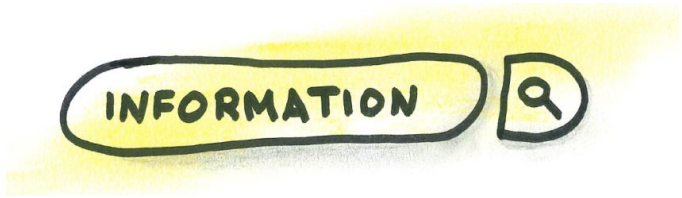
Wie geht diese Maßnahme?

Welche Maßnahmen bringen was?

Internetrecherche

Expertinnen und Experten fragen





https://www.informatik-aktuell.de/betrieb/sicherheit/sinnvolle-massnahmen-zur-erhoehung-der-it-sicherheit.html

Informatik Aktuell

Call for Papers — Die große IT-Konferenz 09. - 12.12.2024 in Frankfurt am Main

Über uns | Media | Kontakt | Impressum

Newsletter abonnieren

Entwicklung | Betrieb | Management und Recht | News | Termine | IT-Jobs | IT-Bücher | Suchbegriff

Künstliche Intelligenz | Digitalisierung | Agile | Nachhaltigkeit | DevOps | Microservices | Cloud | IoT | IT-Security | Datenbanken | Java

» Betrieb » IT-Security

Christian Tacke & Gesche Wiebe *03. Dezember 2014*

Sinnvolle Maßnahmen zur Erhöhung der IT-Sicherheit

Wie begegnet man dem Thema IT-Sicherheit? © depositphotos.com / mitarart

Der Satz, dass Daten heute eine wichtige Rolle spielen, ist weder neu noch besonders originell. Der Wahrheitsgehalt und die Tragweite dieses Satzes sind jedoch enorm. Kaum jemand bestreitet, dass sensible Daten geschützt werden müssen und dass Bedrohungen durch Cyberkriminalität rasant wachsen. Doch wie begegnet man dem Thema IT-Sicherheit, das auf der einen Seite so wichtig und auf der anderen Seite so komplex ist?

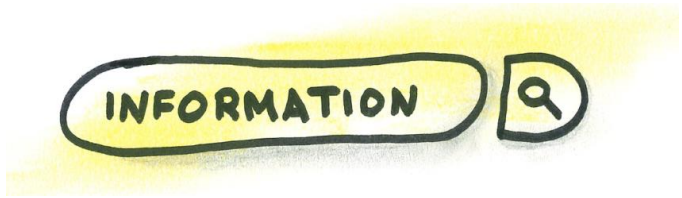
Sensible Daten müssen heutzutage vor unbefugten Zugriffen geschützt werden. In Anbetracht der jüngsten Angaben des Bundeskriminalamtes, dass die Zahl der Verbrechen im Internet weiter gestiegen ist auf rund 64.500 Fälle, steht der Schutz der Vertraulichkeit der Daten im Fokus. Aber auch die Integrität der Daten spielt eine wichtige Rolle. Daten müssen korrekt und unversehrt sein und es muss ausgeschlossen werden, dass sie unerlaubt verändert worden sind. Und trotzdem müssen Daten verfügbar sein.

Geht es um sinnvolle Maßnahmen zur Erhöhung der IT-Sicherheit, sollten sich diese im Rahmen der drei genannten Kategorien Vertraulichkeit, Integrität und Verfügbarkeit bewegen.

Autoren

Gesche Wiebe

Gesche Wiebe unterstützt seit 2014 das Team von CosmoKey. Im Rahmen der Marketing- und Kommunikationsmaßnahmen arbeitet sie für den... >> Weiterlesen



Zehn wirksame Maßnahmen für Ihre IT-Sicherheit

Die Fülle der möglichen Maßnahmen kann Unternehmen, die sich dem Thema IT-Sicherheit neu zuwenden, organisatorisch und finanziell überfordern. Im Folgenden werden zehn wirksame Maßnahmen vorgestellt, die die eigene Angriffsfläche signifikant reduzieren. Natürlich wird dadurch kein umfassendes Management zur IT-Sicherheit ersetzt. Es bietet jedoch konkrete Ansatzpunkte, von denen aus gestartet werden kann.

1. Sensibilisierung der Mitarbeiter und Schulung

Informierte und geschulte Mitarbeiter sind Voraussetzung dafür, dass ein Unternehmen seine Ziele erreichen kann. Nur durch Information und Schulung kann sichergestellt werden, dass alle Mitarbeiter die Folgen und Auswirkungen ihrer Tätigkeit im beruflichen (und privaten) Umfeld einschätzen können. Ziel der Sensibilisierung für Informationssicherheit ist es, das Bewusstsein der Mitarbeiter für Sicherheitsprobleme zu schärfen und entsprechende Handlungsempfehlungen herauszugeben.

2. Zwei-Faktor-Authentifizierung

Eine Authentifizierung allein mit Nutzername und Passwort ist heute nicht ausreichend. Schadprogramme wie Trojanische Pferde oder Keylogger greifen unmittelbar die Passwörter ab, sodass auch komplexe Passwörter oder ein häufiger Passwortwechsel keinen hinreichenden Schutz bieten. Wirksam abgewehrt werden solche Angriffe erst mittels eines zweiten, außerhalb des Systems liegenden Faktors wie z.B. eines Hardwaretokens.

3. VPN

Mit einem VPN (Virtual Private Network) verschlüsseln Sie die Kommunikation und sichern das Netzwerk ab, auch wenn von außen darauf zugegriffen wird. Ihre Kommunikation bewegt sich sozusagen in einem Tunnel und ist von außen nicht einsehbar. Doch auch ein VPN ist angreifbar, weshalb ein zweiter Faktor zur Authentifizierung unbedingt sinnvoll ist.

4. Klassifizierung der Daten

Analysieren Sie, welche Daten welchen Grad an Vertraulichkeit haben. Wie wertvoll und damit schützenswert ist die Kundenliste ihres Unternehmens? Wie sieht es mit der Gehaltliste ihrer Mitarbeiter aus? Konstruktionspläne, Daten im Einkauf und in der Buchhaltung – wie vertraulich sind diese Daten? Empfehlenswert ist, die Vertraulichkeit in einer Skala – zum Beispiel von eins bis zehn – zu definieren.

5. Berechtigungskonzept

Haben Sie die Daten nach ihrem Grad der Vertraulichkeit klassifiziert, schließt sich daran die Frage an, wer aus dem Unternehmen Zugang zu diesen Daten haben sollte. Nicht jeder Mitarbeiter muss alle Daten zur Verfügung haben – welche Daten der einzelne Mitarbeiter in

onpulson
Das Fachportal für Entscheider im Mittelstand

KÖPFE + INTERVIEWS STELLENMARKT NEWSLETTER WIRTSCHAFTSLEXIKON

Gründung Unternehmensführung Marketing + Vertrieb Digitalisierung Personal Finanzen Karriere

Startseite ▸ Digitalisierung ▸ Grundlagen der IT-Sicherheit – Grundsätze, Bedrohungen und Maßnahmen

IT-SICHERHEIT IM UNTERNEHMEN

Grundlagen der IT-Sicherheit – Grundsätze, Bedrohungen und Maßnahmen

Von Onpulson Redaktion
Am 31. Januar 2023

In einem von Globalisierung und weltweiter Vernetzung geprägten Umfeld hängt die Wettbewerbsfähigkeit der Unternehmen zunehmend von einem sicheren und zuverlässigen Betrieb der Unternehmens-IT ab. Der Schutz sensibler Daten spielt mit der sich verschärfenden Bedrohungslage durch Internetkriminalität und Wirtschaftsspionage eine besondere Rolle.

Inhaltsverzeichnis

1. Was ist IT-Sicherheit?
2. Die Grundsätze der IT-Sicherheit
3. Warum ist IT-Sicherheit für Unternehmen wichtig?
4. Die größten Bedrohungen der IT-Sicherheit für Unternehmen

Stellenanzeigen

KÖLN
Verwaltungsleitung (m/w/d) in den katholischen Kirchengemeinden St. Theodor und St. Elisabeth in Köln-Vingst/ Höhenberg sowie St. Marien und St. Engelbert in Köln-Kalk
Erzbistum Köln

HARTMANNSDORF BEI CHEMNITZ
Team Manager Buchhaltung (m/w/d)
KOMSA AG

STUTTGART, AUGSBURG
Manager Zeitarbeitsunternehmen (m/w/x)
Go-Ahead Verkehrsgesellschaft Deutschland GmbH

VERSCHIEDENE STANDORTE
Managing Consultant ServiceNow - ITSM (m/w/d)
operational services GmbH & Co. KG

VERSCHIEDENE STANDORTE
Managing Consultant ServiceNow - HRSD (m/w/d)
operational services GmbH & Co. KG

Zum Stellenmarkt

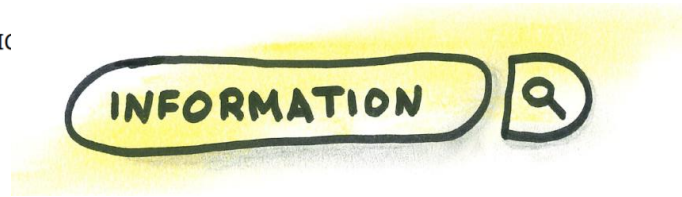
Neue Fachbeiträge

Cyberattacken nehmen zu: So schützen Sie Ihr Business effektiv - ANZEIGE -

https://www.onpulson.de/68072/grundlagen-der-it-sicherheit-fuer-unternehmen-grundsaetze-bedrohungen-und-massnahmen/

Bundesamt für Sicherheit in der Informationstechnik

KONTAKT ENGLISH GEBÄRDENSPRACHE LEIC



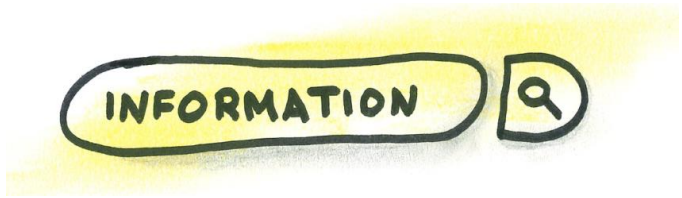
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/TOP-12-Massnahmen/top-12-massnahmen.html

Das BSI Themen IT-Sicherheitsvorfall Ka

... > Unternehmen allgemein > IT-Notfallkarte > TOP 12 Maßnahmen > TOP 12 Maßnahmen bei Cyber-Angriffen

TOP 12 Maßnahmen bei Cyber-Angriffen

Die konkreten Maßnahmen zur Bewältigung eines Cyber-Angriffs können nicht pauschalisiert werden. Stattdessen müssen die individuellen Rahmenbedingungen – wie IT-Infrastruktur vor Ort, Art des Angriffs und Zielsetzungen der Organisation betrachtet werden.



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/TOP-12-Massnahmen/top-12-massnahmen.html

TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

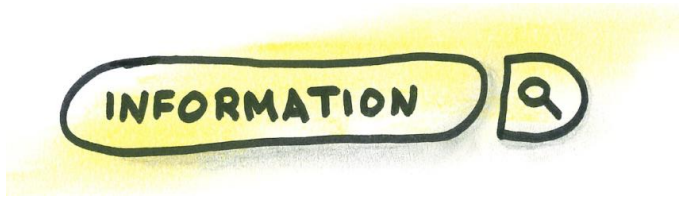
Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, *University of Maryland;* Sean Kross, *University of California, San Diego;* Miraida Morales, *Rutgers University;* Rock Stevens and Michelle L. Mazurek, *University of Maryland*

https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

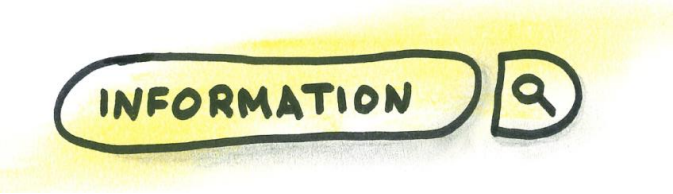
This paper is included in the Proceedings of the 29th USENIX Security Symposium.

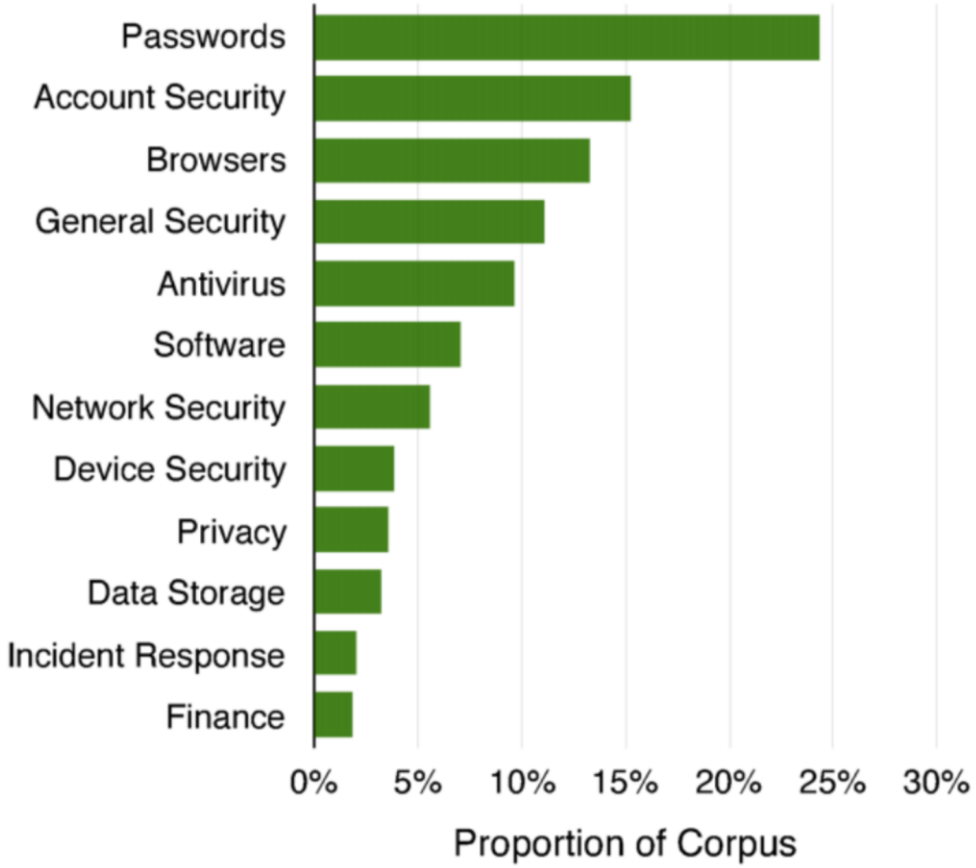
August 12–14, 2020

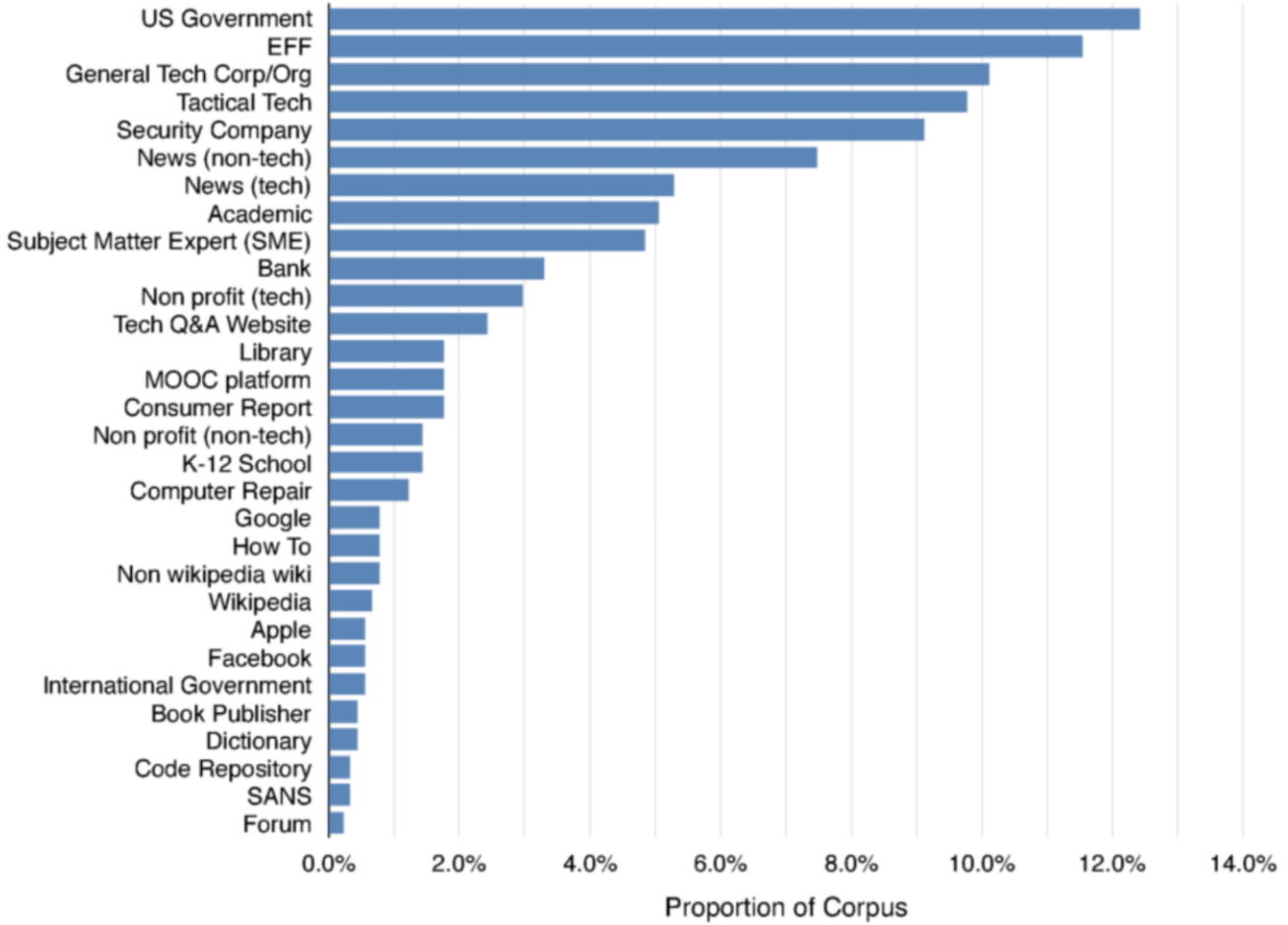
978-1-939133-17-5

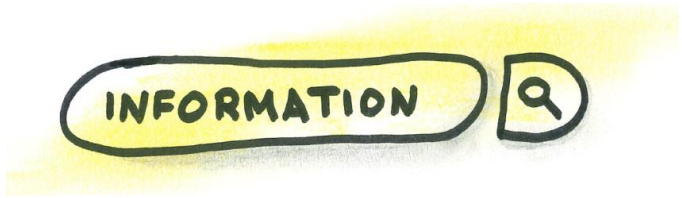


Topic	Examples
Account Security	Identify compromise on your social media account, Avoid spam in your email account, don't sign up for "unnecessary" accounts (this does *not* include mechanisms for authentication, e.g., passwords, 2FA)
Browsers	Clear browser history, only download things you are looking for, verify website signatures and certificates
Data Storage	Keep sensitive information on removable storage media, use backups and SSDs, encrypt data
Device Security	Cover your webcam, keep your devices with you, lock your smartphone
Finance	Do online banking only on certain devices, use secure payment methods, type banking links manually
General Security	Seek out expert help, avoid overconfidence online, use parental controls for children
Incident Response	Cancel or change accounts, report suspicious incidents to IT/support, document the incident
Network Security	Use a password to protect your wifi, change your router name from the default, turn off Bluetooth, how to set up firewalls
Passwords	Use strong passwords (including specific imperatives regarding how to construct such a password), use unique passwords, how to store passwords, use 2FA
Privacy	Use Tor, read privacy policies, and act anonymously online
Software	Update applications, only install trusted software, remove unnecessary programs


INFORMATION


Passwords
Account Security
Browsers
General Security
Antivirus
Software
Network Security
Device Security
Privacy
Data Storage
Incident Response
Finance
0%
5%
10%
15%
20%
25%
30%
Proportion of Corpus

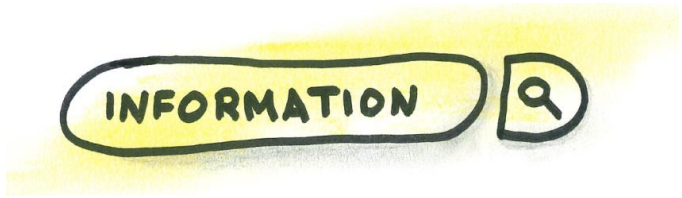

US Government
EFF
General Tech Corp/Org
Tactical Tech
Security Company
News (non-tech)
News (tech)
Academic
Subject Matter Expert (SME)
Bank
Non profit (tech)
Tech Q&A Website
Library
MOOC platform
Consumer Report
Non profit (non-tech)
K-12 School
Computer Repair
Google
How To
Non wikipedia wiki
Wikipedia
Apple
Facebook
International Government
Book Publisher
Dictionary
Code Repository
SANS
Forum
0.0%
2.0%
4.0%
6.0%
8.0%
10.0%
12.0%
14.0%
Proportion of Corpus



You should ...

- Use unique passwords for different accounts, 1.81
- Update devices, 1.88
- Use anti-malware software, 1.91
- Scan attachments you open for viruses, 1.99
- Use different passwords, 2.06
- Encourage others to use strong passwords, 2.17
- Not tell anyone your passwords, even IT, 2.18
- Use end-to-end encryption for communication, 2.19
- Remember your passwords, 2.22
- Keep passwords safe if written down, 2.35

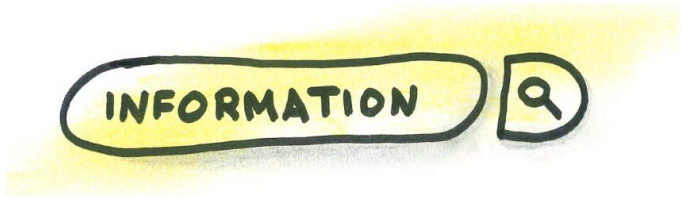
Top 10 nach Priorität der Expertinnen und Experten



Ranking der Experten (Ausschnitt): Unnütze Maßnahmen

You should ...

- consider opening a credit card for online use only [all experts agree]
- let your children teach you about the Internet too [all experts agree]
- use an unbranded smartphone [all experts agree]
- carry laptops in something other than laptop cases
- install software in phases



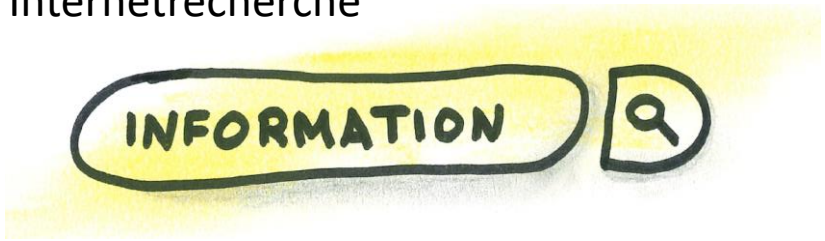
You should ...

- change passwords often
- keep sensitive information on removable storage media
- not change browser security settings
- not download or execute any files
- not identify yourself to websites
- not open attachments from unknown senders
- not shut down your computer
- not use a password manager, extensions or plugins
- turn off automatic downloads
- use less common software

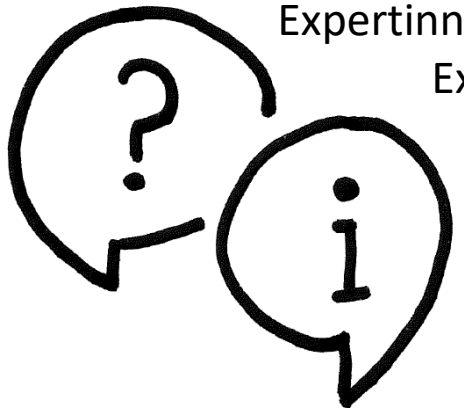
Ranking der Experten (Ausschnitt): Gefährlich und Schädlich

Wie komme ich ran an die Maßnahmen?

Internetrecherche

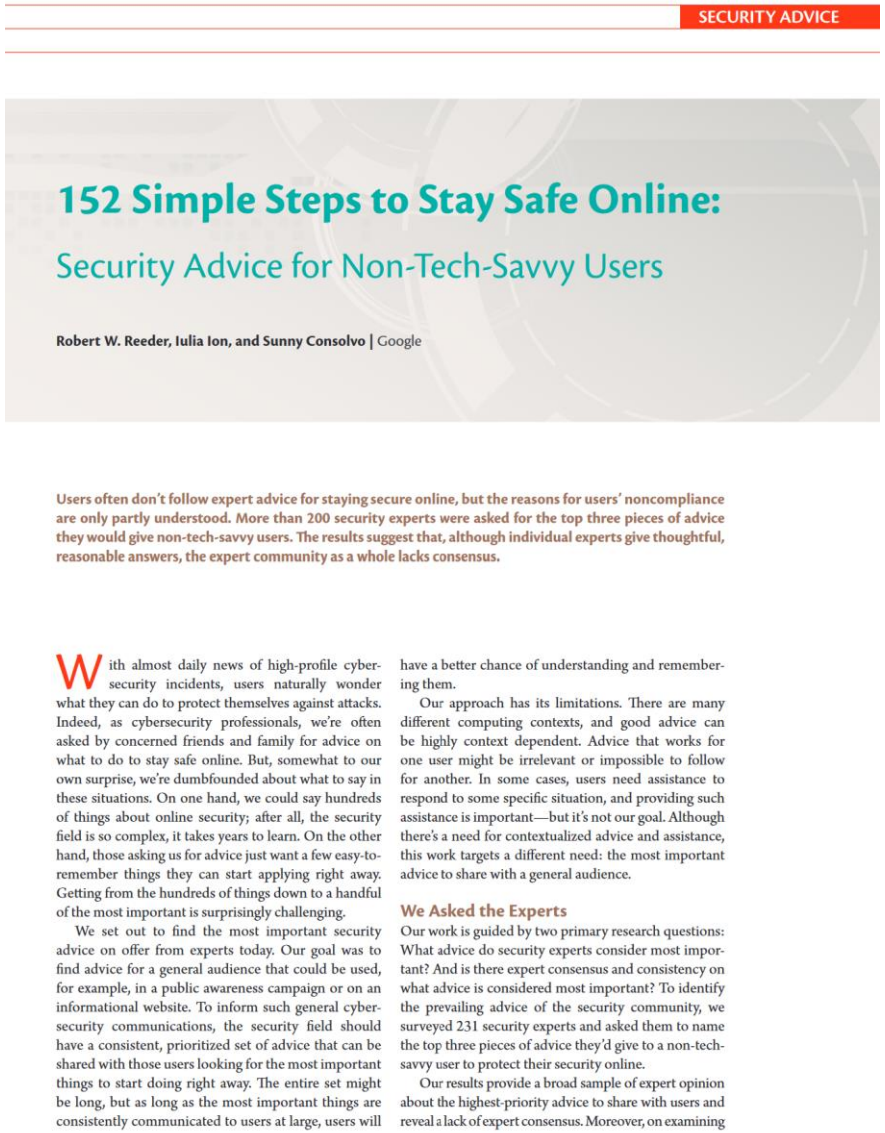


Expertinnen und Experten fragen



231 Expertinnen und Experten

„Welche Top 3 Maßnahmen würdest du empfehlen?“



SECURITY ADVICE

152 Simple Steps to Stay Safe Online:

Security Advice for Non-Tech-Savvy Users

Robert W. Reeder, Iulia Ion, and Sunny Consolvo | Google

Users often don't follow expert advice for staying secure online, but the reasons for users' noncompliance are only partly understood. More than 200 security experts were asked for the top three pieces of advice they would give non-tech-savvy users. The results suggest that, although individual experts give thoughtful, reasonable answers, the expert community as a whole lacks consensus.

With almost daily news of high-profile cybersecurity incidents, users naturally wonder what they can do to protect themselves against attacks. Indeed, as cybersecurity professionals, we're often asked by concerned friends and family for advice on what to do to stay safe online. But, somewhat to our own surprise, we're dumbfounded about what to say in these situations. On one hand, we could say hundreds of things about online security; after all, the security field is so complex, it takes years to learn. On the other hand, those asking us for advice just want a few easy-to-remember things they can start applying right away. Getting from the hundreds of things down to a handful of the most important is surprisingly challenging.

We set out to find the most important security advice on offer from experts today. Our goal was to find advice for a general audience that could be used, for example, in a public awareness campaign or on an informational website. To inform such general cybersecurity communications, the security field should have a consistent, prioritized set of advice that can be shared with those users looking for the most important things to start doing right away. The entire set might be long, but as long as the most important things are consistently communicated to users at large, users will have a better chance of understanding and remembering them.

Our approach has its limitations. There are many different computing contexts, and good advice can be highly context dependent. Advice that works for one user might be irrelevant or impossible to follow for another. In some cases, users need assistance to respond to some specific situation, and providing such assistance is important—but it's not our goal. Although there's a need for contextualized advice and assistance, this work targets a different need: the most important advice to share with a general audience.

We Asked the Experts

Our work is guided by two primary research questions: What advice do security experts consider most important? And is there expert consensus and consistency on what advice is considered most important? To identify the prevailing advice of the security community, we surveyed 231 security experts and asked them to name the top three pieces of advice they'd give to a non-tech-savvy user to protect their security online.

Our results provide a broad sample of expert opinion about the highest-priority advice to share with users and reveal a lack of expert consensus. Moreover, on examining

Advice	Count	Representative quotes
Account security	**128**	
Use unique passwords	68	Different passwords everywhere. Do not reuse passwords on multiple sites.
Use strong passwords	58	Choose a strong password. Complex password for every site.
Use multifactor authentication	36	Enable multifactor authentication features, if available.
Use a password manager	33	Forget your password—use a password manager to remember it for you.
Use a passphrase	7	Use a passphrase. Use long-form plain language passwords.
Write passwords down	5	Write them down in a notebook and keep it safe.
Updates	**97**	
Keep systems and software up to date	90	Always be updating (OS and applications). Patch, patch, patch.
Use automatic updates	19	Activate autoupdate.
Browsing habits	**76**	
Use HTTPS	24	Use HTTPS if available. Watch for and understand why HTTPS is important.
Be careful/think before you click	19	Think before you click. Be careful what you click on.

Email habits	**59**	
Don't open unexpected attachments	19	If you didn't ask for the attachment, don't open it.
Don't click links in emails at all	11	Never click on a link in an email.
Don't click links in email from unknown sender	9	Don't click on links or images in an email from an unknown source.
Be suspicious of email in general	7	Don't trust email. Be skeptical about email.
Be alert for phishing emails	5	Beware spam and phishing emails. Don't fall for phishing attempts.
Beware emails requesting private data	5	No legitimate financial institution will ask for your personal or financial information through email.
Be suspicious even of email from known sender	4	Don't blindly trust every message even if it came from someone you know and trust.
Be suspicious of links in email	4	Be careful following links, especially in email.
Other email habits	19	If a message you receive seems strange, pick up the phone and verify it.
Mindfulness	**42**	
Be suspicious in general	16	Be skeptical. Always be suspicious; don't trust everybody.
Too good to be true probably is	15	If it seems too good to be true, it likely is. Be aware of "too-good-to-be-true" offers.

Always browse in private mode, and delete cache after each browsing session.

Don't write down passwords.

Don't click on ads.

Don't look for porn.

Install Microsoft EMET (Enhanced Mitigation Experience Toolkit) and turn the systemwide settings up to maximum.

Let Gmail render your mail attachments instead of opening them locally.

Make sure to set up account recovery options for your Google account.

Advice	Count	Repre
Account security	**128**	
Use unique passwords	68	Differe Do not
Use strong passwords	58	Choos Compl
Use multifactor authentication	36	Enable
Use a password manager	33	Forget
Use a passphrase	7	Use a p Use lor
Write passwords down	5	Write t

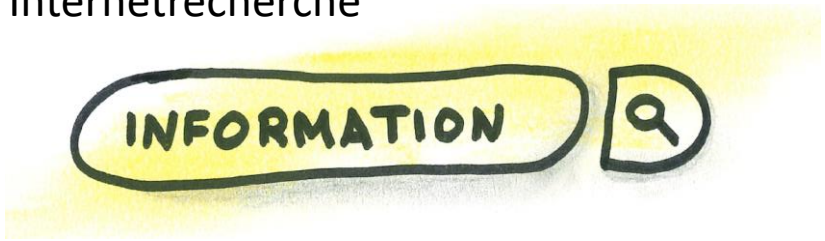
Always browse in private mode, and delete cache after each browsing session.

Don't write down passwords.

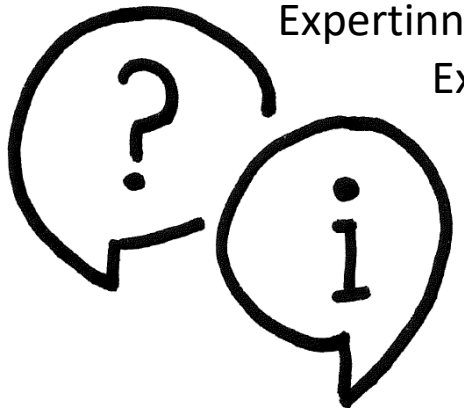
Don't click on ads.

Wie komme ich ran an die Maßnahmen?

Internetrecherche



Expertinnen und Experten fragen



AUFGABE

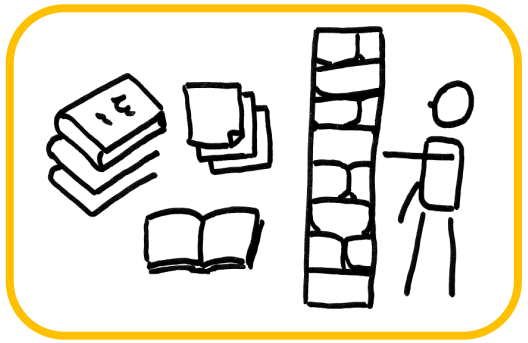
Schreibe dir auf oder diskutiere mit deinem Nachbar oder deiner Nachbarin

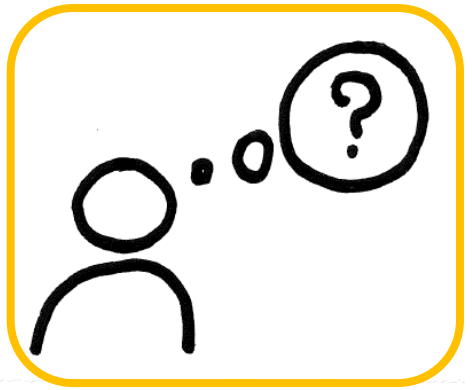
(3) Maßnahmen, die du privat im täglichen Leben umsetzt

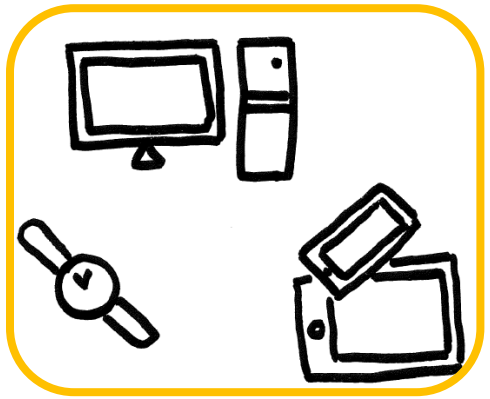
und (3) Maßnahmen, die du nicht umsetzt

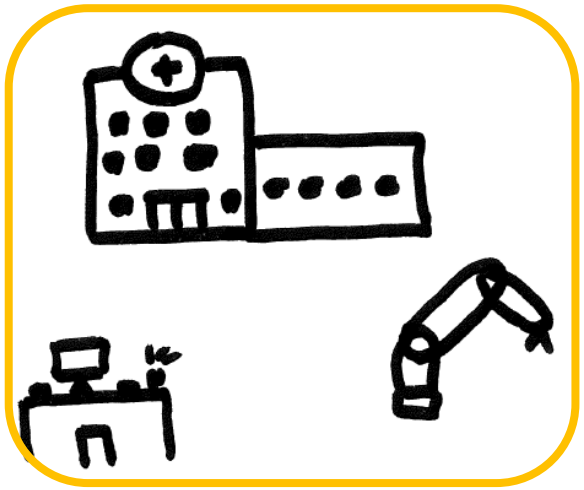
Gibt es besondere Gründe, warum du gerade diese Maßnahmen durchführst?
Warum führst du die anderen Maßnahmen nicht durch?

Probleme









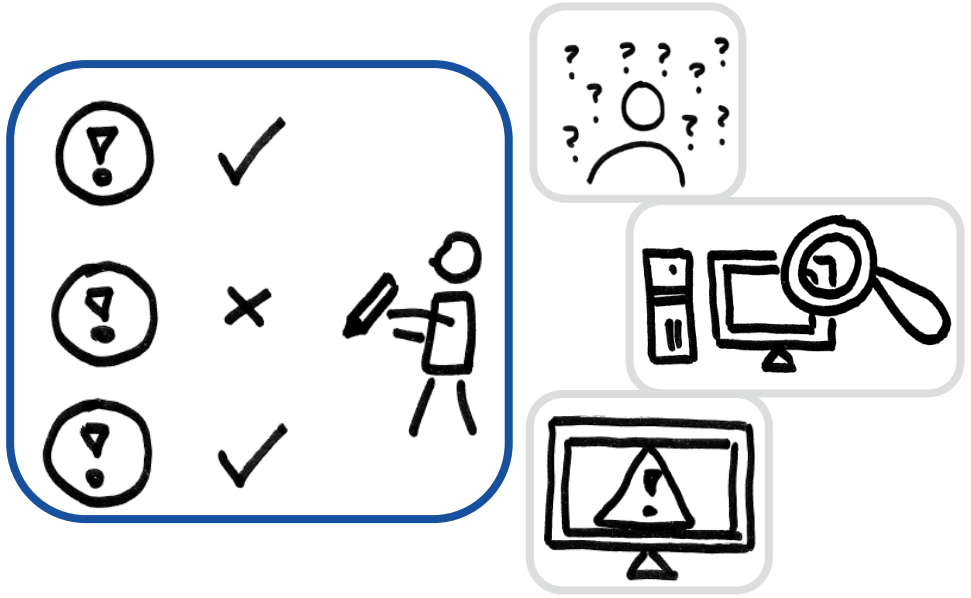
AUFGABE

Suche dir eine Maßnahme raus die du durchführst und eine, die du nicht durchführst.

Bewerte verschiedene Gründe, die dagegen sprechen, diese Maßnahme umzusetzen

- Technische Realisierbarkeit
- Situationsabhängigkeit
- Menschliche Realisierbarkeit
- Fehlender Nutzen, Aufwand, Kosten, Effektivität

Lösungen?



Die RICHTIGEN Maßnahmen auswählen

Was will ich **gegen wen oder was** beschützen?

Schutzziele,
Geräte,
Daten,
Dateien,
...

Risikoanalyse

Die RICHTIGEN Maßnahmen auswählen

Risikoanalyse

Die große Frage: **Was könnte alles passieren?**

Risikobewertung: Wahrscheinlichkeit und Schadenshöhe

AUFGABE

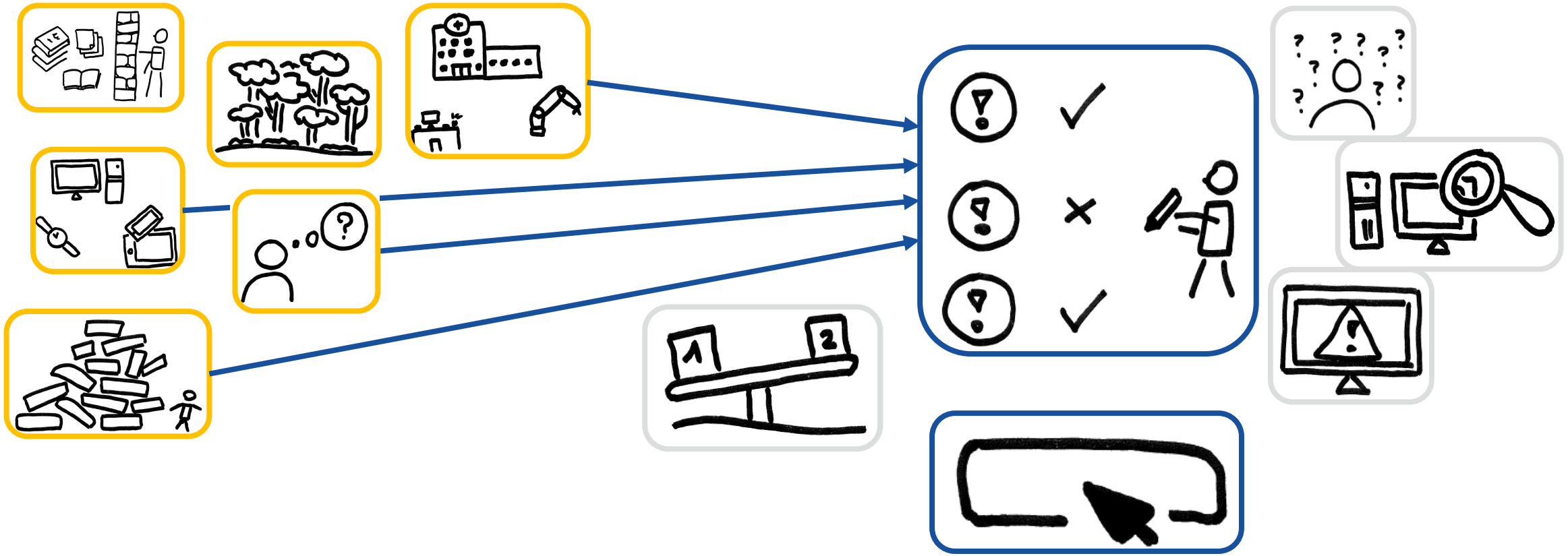
Bestandsaufnahme: Welche Geräte / Daten / Anwendungsfälle habe ich?

Was will ich beschützen?

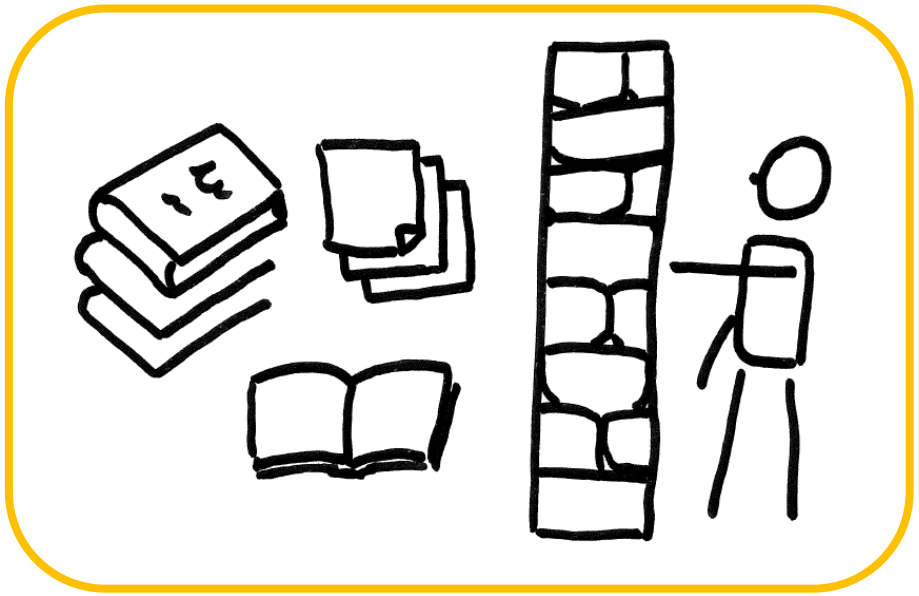
Gegen wen oder was will ich mich schützen?

Welche Risiken gibt es? Wie ist das Risiko (Eintrittswahrscheinlichkeit und Schadenshöhe)?

Lösungen?



Hilfe! Der Zugang zum Wissen...



- Vorsicht beim Teilen auf Social Media
- Adblocker verwenden
- Cookies löschen bzw. ablehnen
- Wenige persönliche Daten weitergeben
- Nicht den echten Namen verwenden
- Privatsphäre Einstellungen auf Social Media nutzen
- Nur auf sicheren Seiten surfen
- VPN nutzen
- Inkognito Modus nutzen
- Tracking in den Browsereinstellungen verbieten

Maßnahme	Nützlichkeit
Wenige persönliche Daten weitergeben	1.0
Nicht den echten Namen verwenden	1.5
Vorsicht beim Teilen auf Social Media	1.83
Inkognito Modus nutzen	2.0
Privatsphäre Einstellungen auf Social Media nutzen	2.0
Adblocker verwenden	2.0
Tracking in den Browsereinstellungen verbieten	2.0
Nur auf sicheren Seiten surfen	2.5
Cookies ablehnen	2.66
VPN nutzen	3.5

Maßnahme	Benutzerfreundlichkeit
Inkognito Modus nutzen	1.0
Nur auf sicheren Seiten surfen	1.5
Adblocker verwenden	1.75
Privatsphäre Einstellungen auf Social Media nutzen	2.0
Nicht den echten Namen verwenden	2.5
Vorsicht beim Teilen auf Social Media	2.5
Wenige persönliche Daten weitergeben	2.66
VPN nutzen	3.0
Cookies ablehnen	3.66
Tracking in den Browsereinstellungen verbieten	4.0

Inkognito Modus nutzen

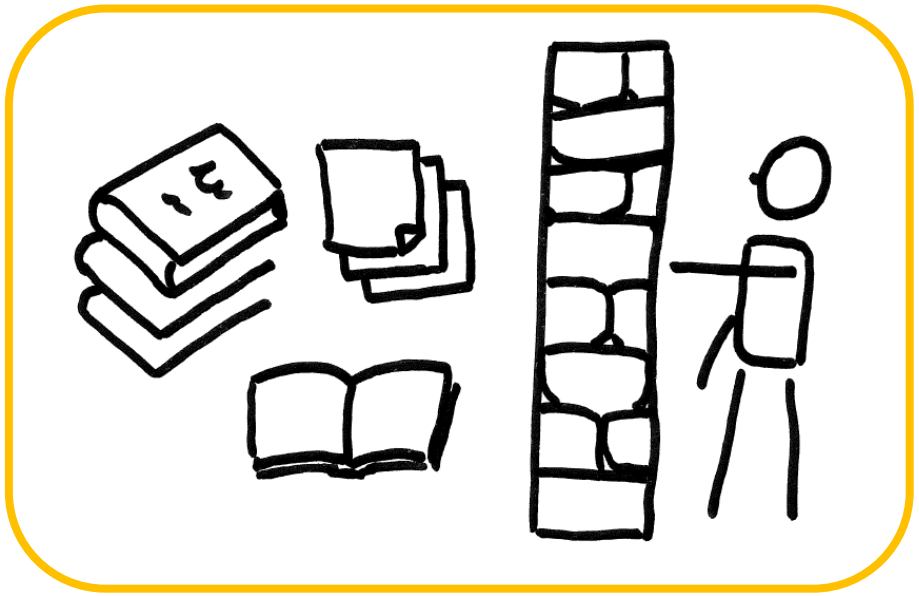
N: 2.00 B: 1.00 T: Jeder #:2

Bei der Nutzung des Inkognito Modus vom Browser werden beim Beenden des Browsers alle lokal gesammelten Daten wie Cookies und Suchverlauf gelöscht.

Entgegen den Erwartungen bei dem Wort „Inkognito“ (lat. inc¯ognitus: unter fremdem Namen, unerkannt, heimlich), welches von vielen Browsern genutzt wird, ist man gegenüber Webseiten nicht inkognito unterwegs und auch wenn man sich auf Webseiten anmeldet und mit seinem Benutzerkonto Beiträge verfasst, ist man auch gegenüber anderen Nutzern nicht inkognito unterwegs. Manche Browser verwenden daher auch die Bezeichnung „Privates Browsen“ [43]

Die Nutzung des Inkognito Modus im Browser ist daher nur wirklich effektiv gegen Personen, die direkten Zugriff auf das Endgerät haben, falls das Gerät von mehreren Personen genutzt wird, man nicht möchte, dass Familienmitglieder, Freude o.Ä. durch Ansehen des Browserverlaufs oder der Cookies wissen auf welchen Seiten man war, oder gegenüber Hackerinnen und Hackern, die Dateien von dem Gerät auslesen können, welche aber wahrscheinlich eh schon alles mitlesen können.

Hilfe! Der Zugang zum Wissen...



Es gibt auch schon echt viel Gutes zu finden ...

Tipps und Tricks

Smartphone Privatsphäre: Tipps und Tricks im Internet

https://kattascha.de/erstehilfe - Sammlung von Erste-Hilfe Maßnahmen, Tipps und weiteren Links

https://www.wu.ac.at/ec/projects/privacy-brochure-a-benchmark-study/ Bewertungsschema und Empfehlungen für Messenger, Social Networks und andere Apps

https://privacy-handbuch.de/index.htm Genereller Überblick über das Thema mit vielen Erklärungen, Beschreibungen und Anleitungen für PC und Smartphone

https://mobilsicher.de/ Umfangreiche Informationsseite mit App-Chacker, Empfehlungen für Apps und Anleitungen für Smartphone-Privatsphäre

https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz Informationen, Anleitungen, Beschreibungen der Rechte und Vorlagen für Datenlöschung und -anfrage

Tipps und Tricks

https://www.klicksafe.de Themen rund um das Internet, darunter einfach erklärte Verträge mit Messengern und ähnlichen Diensten. Zielgruppe: Kinder, Eltern, Lehrer

https://www.handysektor.de/datenschutz-und-recht/ Themen rund um das Smartphone. Zielgruppe: Jugendliche

https://forum.kuketz-blog.de/ Forum und Blog mit Themen rund um die Privatsphäre. Enthält einfache aber auch sehr fortschrittliche Privatsphäre-Maßnahmen zu quasi allen Themen der Privatsphäre

https://www.youtube.com/user/TheMorpheus407 YouTube-Kanal mit Themen zur Anonymität im Internet

Studien und Forschungsarbeiten

Alessandro Acquisti and Jens Grossklags. Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, (1540-7993/05):26–33, 2005.

Alessandro Acquisti, Leslie K. John, and George Loewenstein. What is privacy worth? 2009.

Alessandro Acquisti, Laura Brandimarte, and George Lowenstein. Privacy and Human Behavior in the Information Age. In Evan Selinger, Jules Polonetsky, and Omer Tene, editors, The Cambridge handbook of consumer privacy. Cambridge University Press, Cambridge, 2018. ISBN 978-1-107-18110-6.

Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. Commun. ACM, 42(12):40–46, 1999. ISSN 0001-0782. doi: 10.1145/322796.322806.

Susanne Barth and Menno D.T. de Jong. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics, 34(7):1038–1058, 2017. ISSN 07365853. doi: 10.1016/j.tele.2017.04.013.

Studien und Forschungsarbeiten

Acquisti, A., und J. Grossklags. „Privacy and Rationality in Individual Decision Making". IEEE Security and Privacy Magazine 3, Nr. 1 (Januar 2005): 26–33. https://doi.org/10.1109/MSP.2005.22.

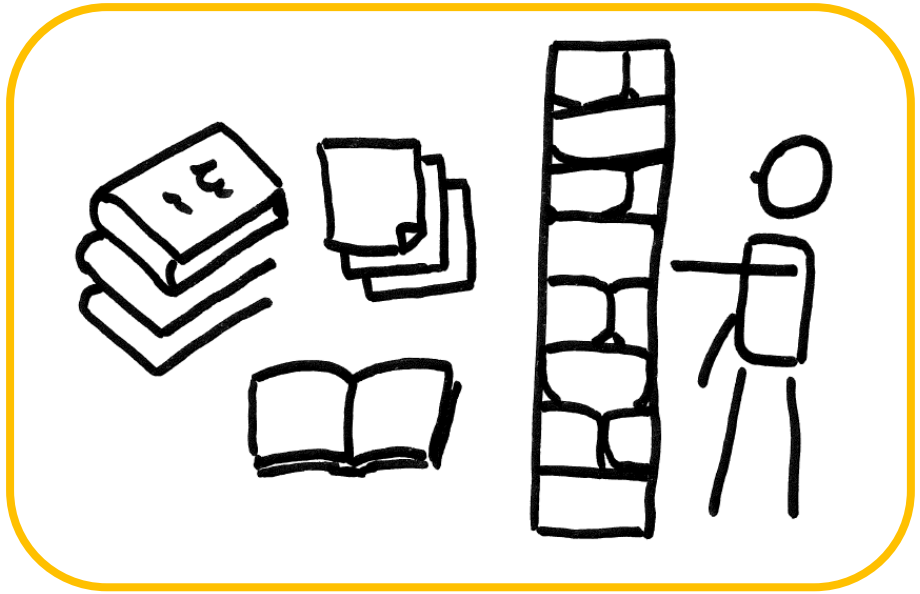
Reeder, Robert W., Iulia Ion, und Sunny Consolvo. „152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users". IEEE Security & Privacy 15, Nr. 5 (2017): 55–64. https://doi.org/10.1109/MSP.2017.3681050.

Herley, Cormac. „So long, and no thanks for the externalities: the rational rejection of security advice by users". In *Proceedings of the 2009 workshop on New security paradigms workshop*, 133–44. NSPW '09. New York, NY, USA: Association for Computing Machinery, 2009. https://doi.org/10.1145/1719030.1719050.

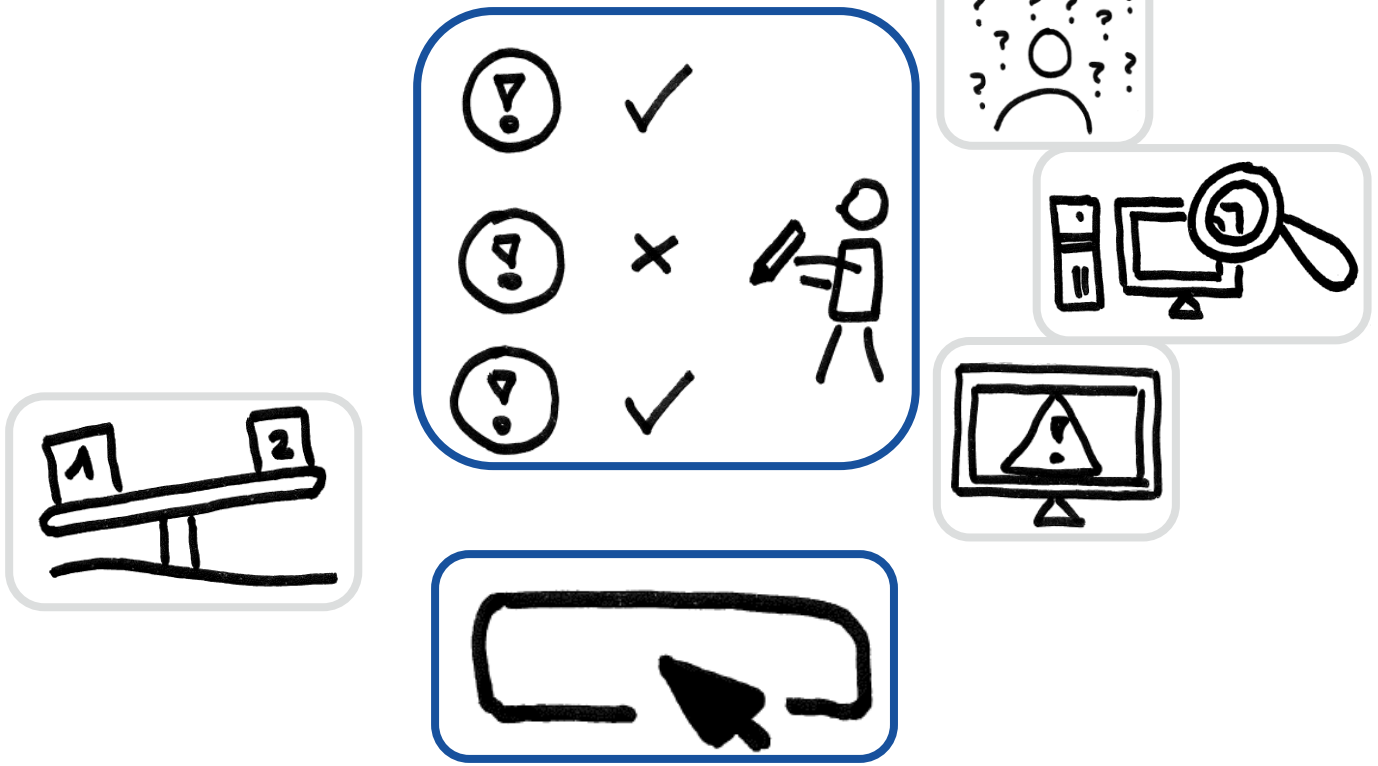
Ion, Iulia, Rob Reeder, und Sunny Consolvo. "...No One Can Hack My Mind": Comparing Expert and {Non-Expert} Security Practices", 327–46, 2015. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion.

Redmiles, Elissa M., Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, und Michelle L. Mazurek. „A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web", 89–108, 2020. https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles.

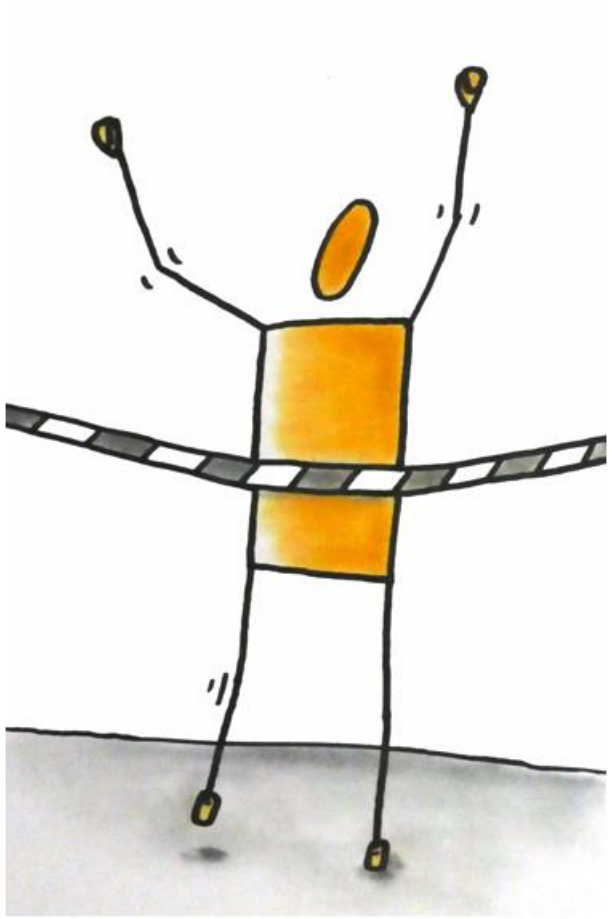
Und auch wir forschen weiter...



Lösungen?



Gesunder Umgang mit Maßnahmen



Arbeitssaal Honeypot / Fachrat Informatik

Leibniz Universität Hannover

SCHALTE BLUETOOTH AUS, WENN DU ES NICHT BENUTZT

Verwende Passwort-Manager

Nutze HTTPS

Verwende Spam-Mailadressen und falsche Namen

Klicke nicht auf unbekannte Links

Sei skeptisch bei Telefon-anrufen von „Der IT“

Mache Updates

Gebe deine Passwörter nicht weiter

Nutze Ad-Blocker

Verschlüssle deine Daten

Achte auf deine Datenschutz-Einstellungen

Verwende Virenscanner

Nutze VPN

Nutze extra privatsphäre-freundliche Apps

MACHE BACKUPS

Lehne Cookies immer ab

Benutze den Inkognito-Modus

Nutze unterschiedliche Passwörter für unterschiedliche Accounts

Und welche Maßnahmen machst du (nicht)?

Maike M. Raphael