Info Kurs:
Sicher surfen im Internet

In Zusammenarbeit mit dem Jugendhaus Hohbuch

organisiert von Philip Engler & Rodion Kraft

Agenda

1. Allgemeines
    1. Digitalbarometer 2021
2. Gefahren und Lösungen beim Internetzugriff
    1. Internetzugriff allgemein
    2. Öffentliche WLAN-Netze
    3. VPNs
    4. Umgang mit dem Browser
3. Gefahren und Lösungen beim Zugriff auf Konten & Social Media
    1. Passwortsicherheit & -Manager
    2. Zwei-Fakor-Authentifizierung
    3. Umgang mit Medien
    4. Identitätsdiebstahl
    5. Phishing & Smishing
4. Wichtiges
    1. Sicherheit von mobilen Betriebssystemen
    2. Antivirenprogramme

1. Allgemeines

Aktueller Stand (Digitalbarometer 2021)

„Zwei Drittel (67 %) kennen Schutzempfehlungen.“

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.html?nn=520690

Aktueller Stand (Digitalbarometer 2021)

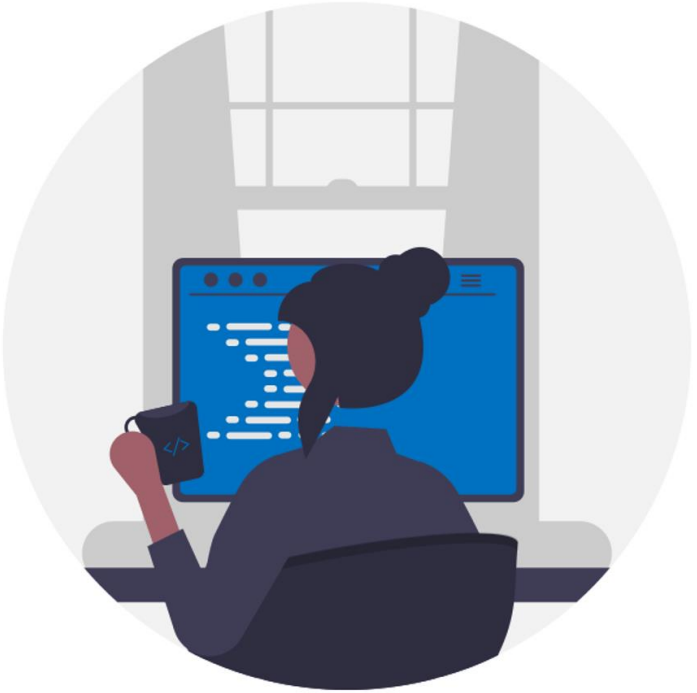
„Viele (79 %) erlitten durch Cyberkriminalität einen Schaden.“

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.html?nn=520690

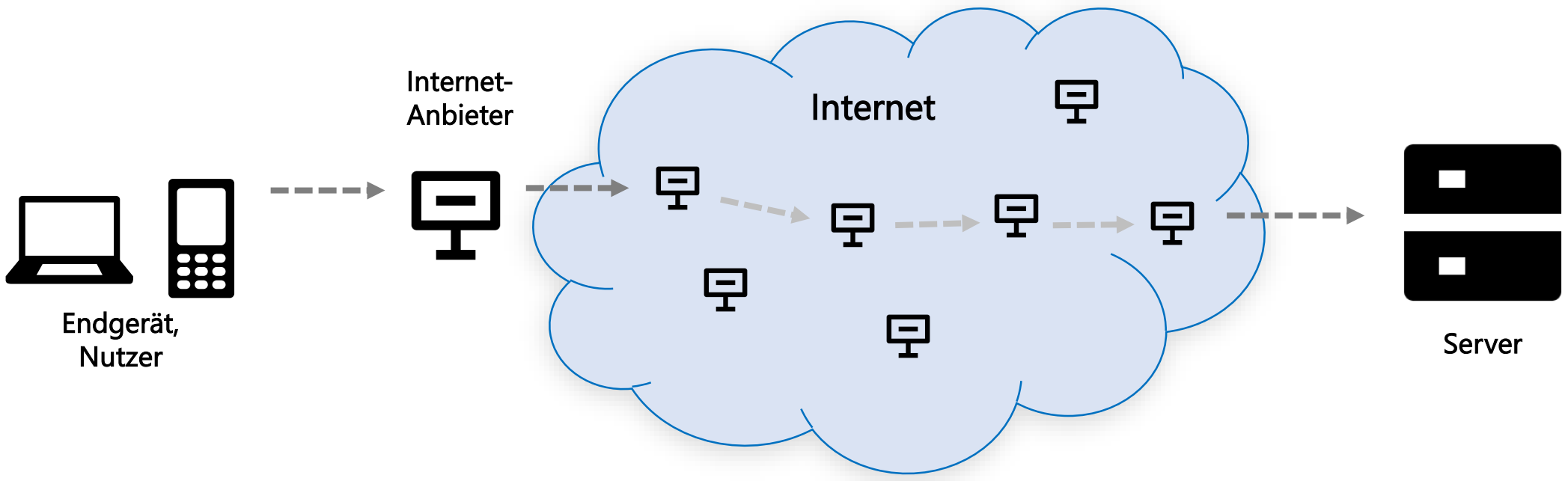
Aktueller Stand (Digitalbarometer 2021)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.html?nn=520690

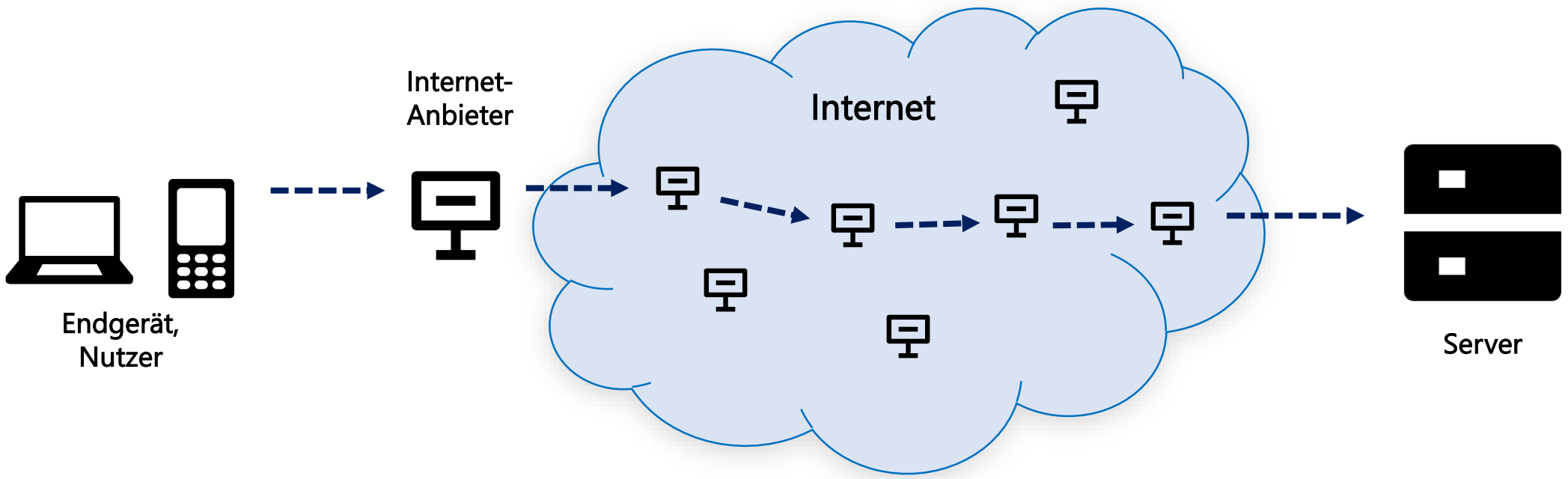
2. Gefahren und Lösungen beim Internetzugriff



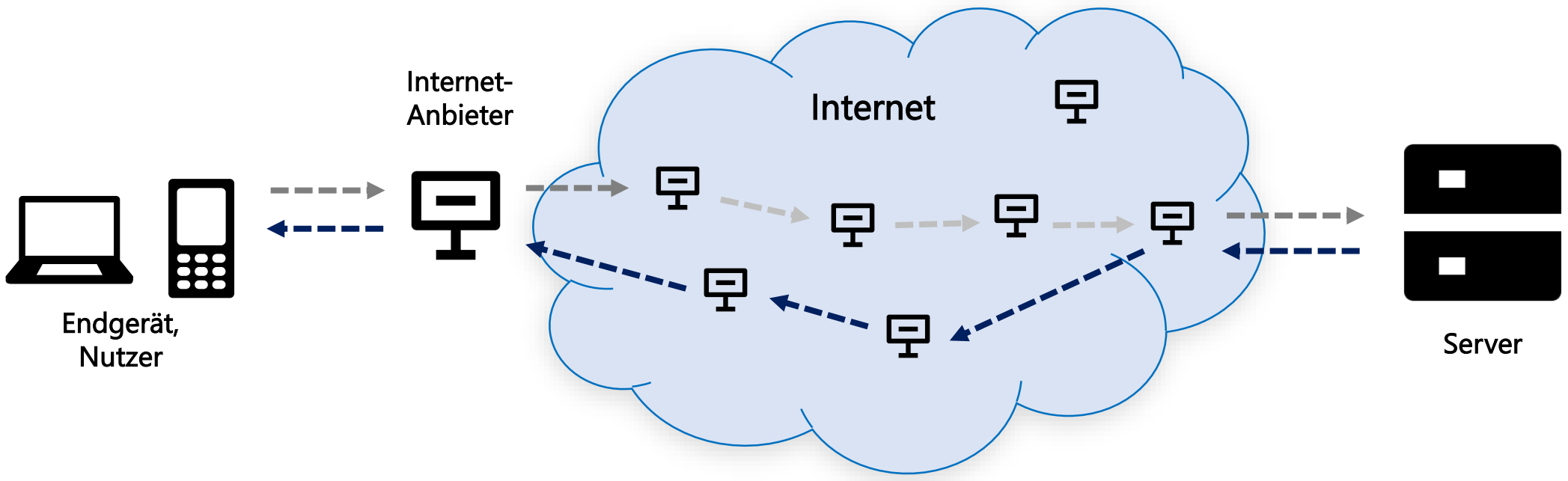
Internetzugriff allgemein



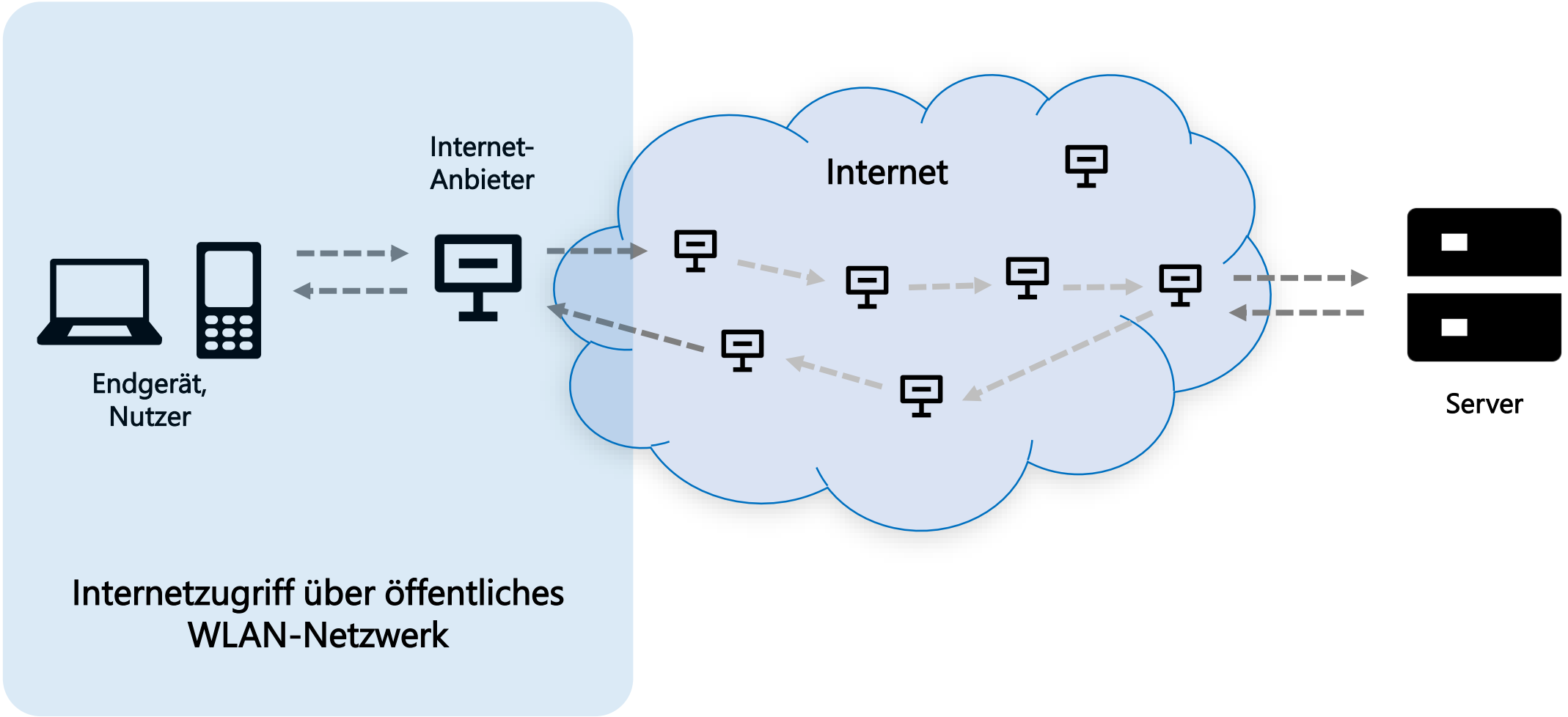
Internetzugriff allgemein



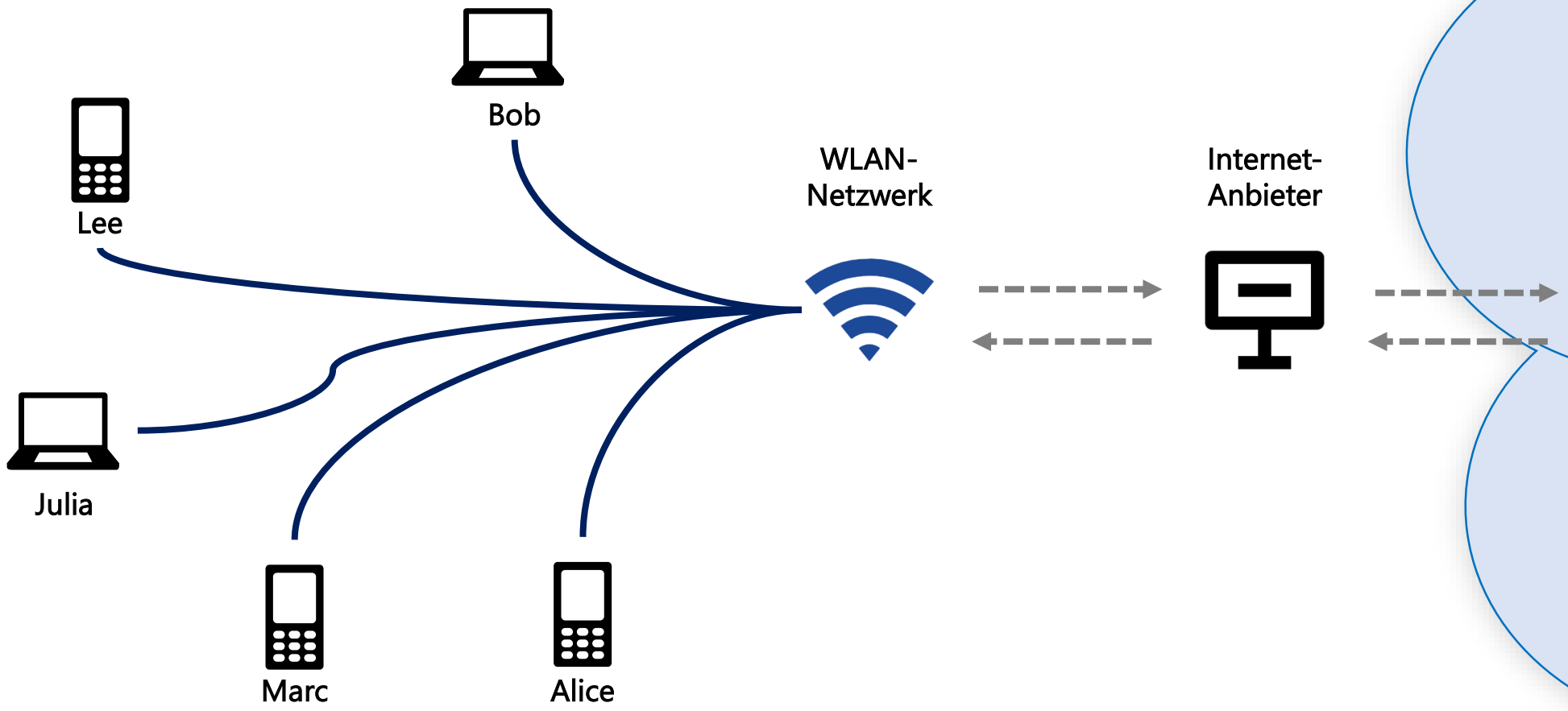
Internetzugriff allgemein



Öffentliche WLAN-Netzwerke



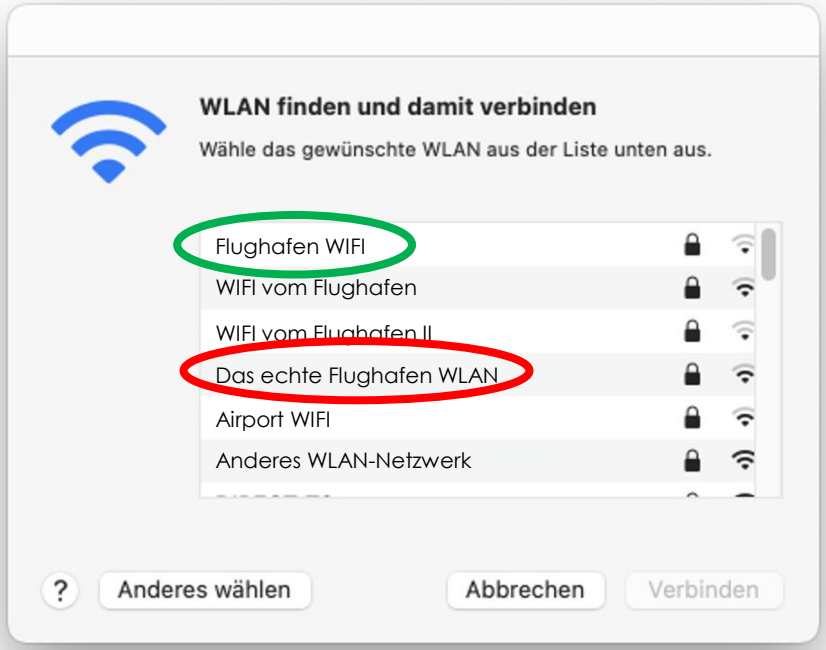
Öffentliche WLAN-Netzwerke



Öffentliche WLAN-Netzwerke

[1]

- Falsche öffentliche WLAN-Netzwerk Namen



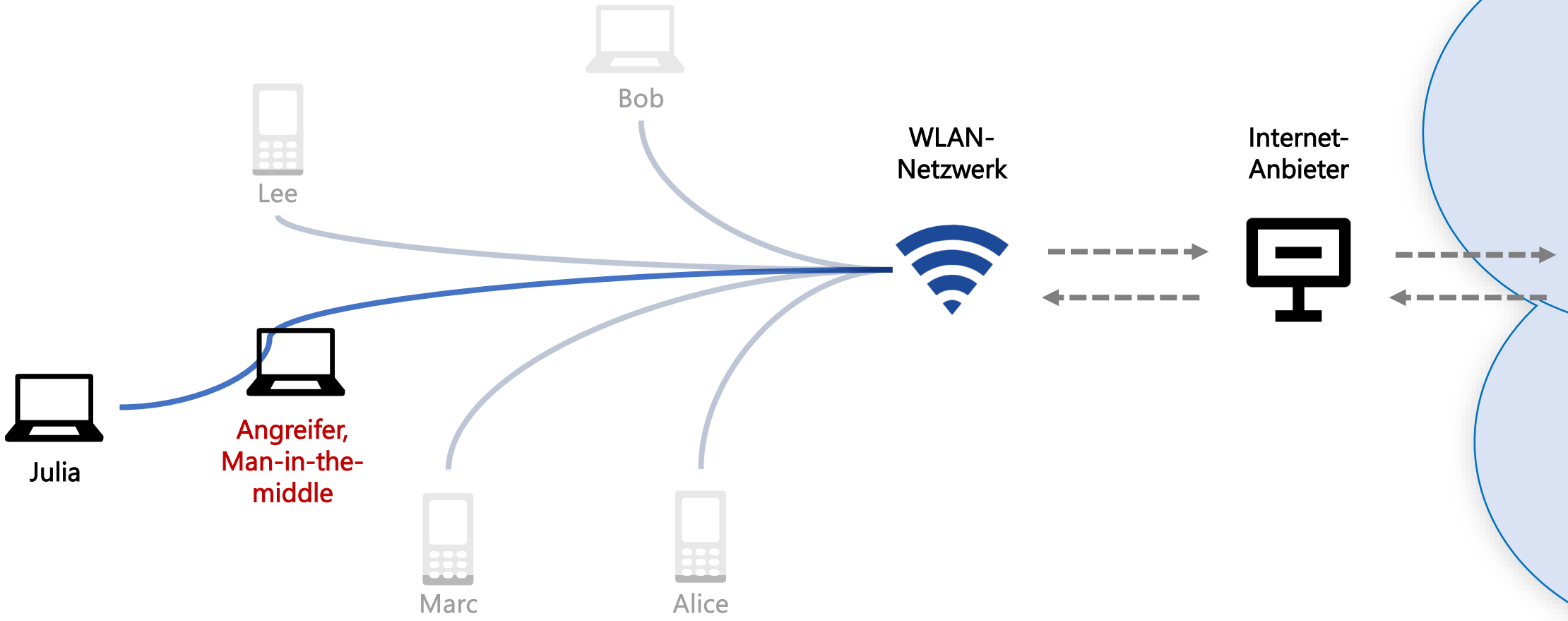
https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Öffentliche WLAN-Netzwerke

- Falsche öffentliche WLAN-Netzwerk Namen
- Malware verteilen über öffentliche WLAN-Netzwerke
- Aktivität und persönliche Daten auslesen (bspw. über sog. Man-in-the-middle Angriffe)

https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Öffentliche WLAN-Netzwerke



https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Öffentliche WLAN-Netzwerke

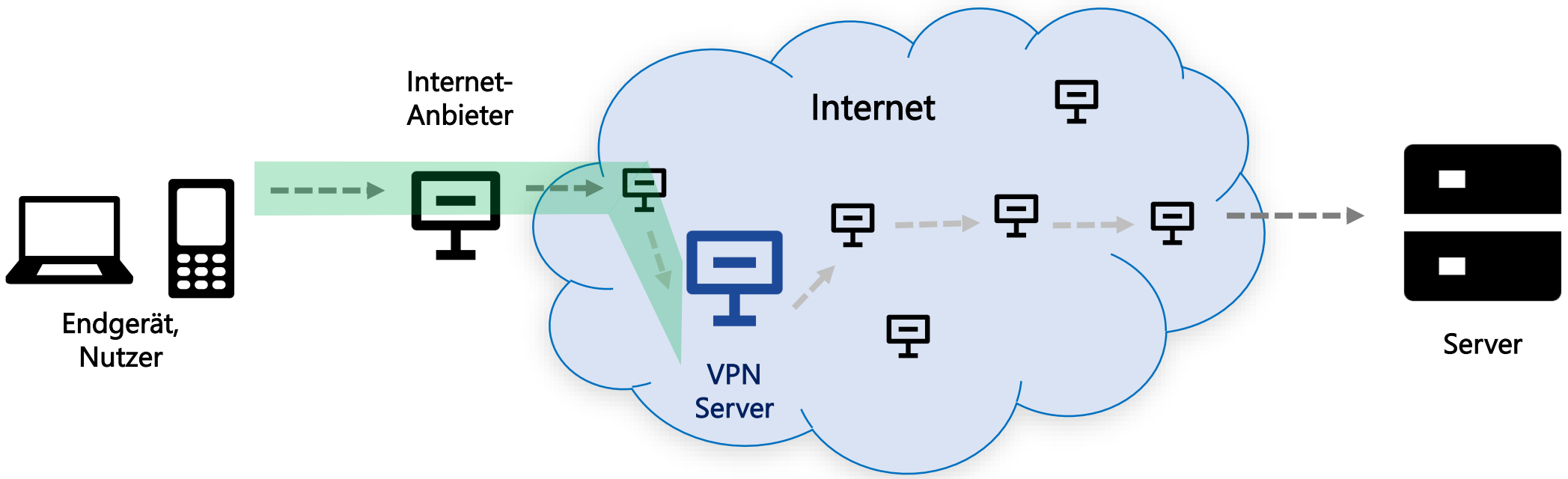
- Sicher sein, über die Verwendung des richtigen WLAN-Netzwerks
  (meistens im Gebäude ausgeschrieben)
- Keine sensiblen Daten abrufen oder senden (Bankverbindung, Social Media, Email, usw.)
- Mögliche Zugriffe deaktivieren, Teilen ausschalten
- Auf sichere Verbindung achten (SSL: dazu später mehr)
- VPN benutzen
- WLAN wieder ausschalten, nach Benutzung → Potentieller Hacker verliert die Verbindung

https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

VPNs – Was bringen sie und Vergleich

- VPN = Virtual Private Network
- Software, die einen sicheren, privaten *Tunnel* durch das Internet bereitstellt

VPNs – Was bringen sie und Vergleich



VPNs – Was bringen sie und Vergleich

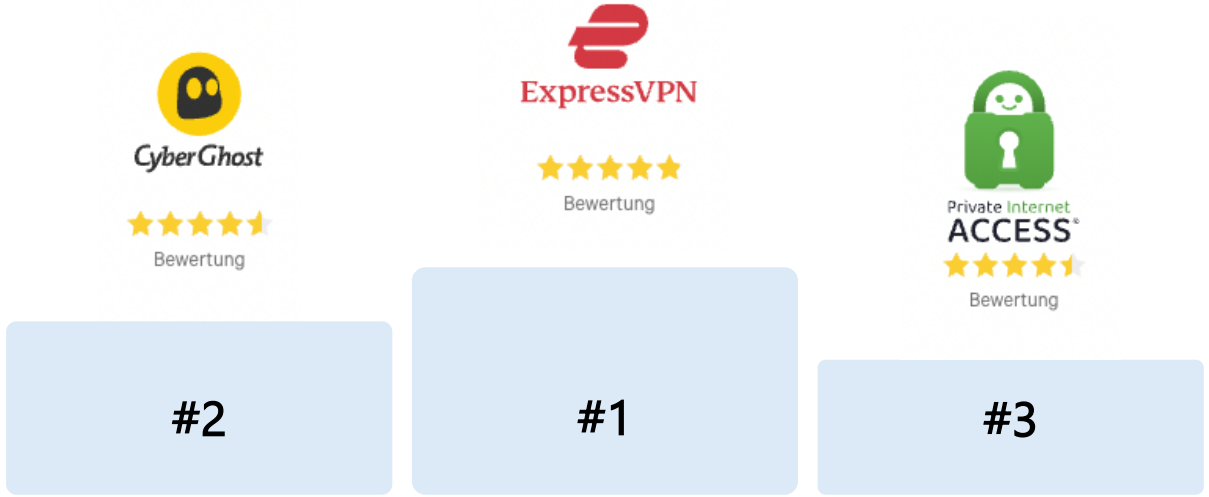
- Aber Vorsicht:
  VPN-Verbindung immer nur so sicher und vertrauenswürdig, wie VPN-Anbieter selbst
- Aktivität und Anfragen bleiben zwar bis zum VPN-Server verschlüsselt, dieser hat (um sie weiterleiten zu können) aber unverschlüsselt Einsicht darauf

VPNs – Was bringen sie und Vergleich

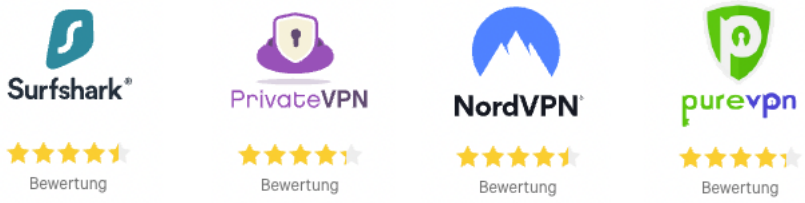
- Lösung: Seriösen und sicheren Anbieter wählen

VPNs – Was bringen sie und Vergleich

Laut **top10vpn.com**:



Weitere:



https://www.top10vpn.com/vergleich/?v=a&bsid=c11se1kw204&gclid=Cj0KCQiA2sqOBhCGARIsAPuPK0hJpVx3LHn6zfm_16BuLfjmRVkpYrnk7xXffT4IS9leRMd578s4FwYaArTnEALw_wcB

VPNs – Was bringen sie und Vergleich

Mehr Infos zu kostenlosen VPN auf **top10vpn.com**:

https://www.top10vpn.com/vergleich/?v=a&bsid=c11se1kw204&gclid=Cj0KCQiA2sqOBhCGARIsAPuPK0hJpVx3LHn6zfm_16BuLfjmRVkpYrnk7xXffT4IS9IeRMd578s4FwYaArTnEALw_wcB

Umgang mit dem Browser

Mozilla Firefox

Google Chrome

Safari

Opera

Microsoft Edge

Microsoft Internet Explorer

Tor Browser

- Zugang zu Internetseiten & Webanwendungen
- Auf allen Geräten verfügbar
- Favorisierten Browser herunterladen und loslegen

https://de.wikipedia.org/wiki/Datei:Tor_Browser_icon.svg
https://de.wikipedia.org/wiki/Datei:Microsoft_Edge_logo_(2019).svg
https://de.wikipedia.org/wiki/Mozilla_Firefox#/media/Datei:Firefox_logo,_2019.svg
https://de.wikipedia.org/wiki/Datei:Safari_browser_logo.svg
https://de.wikipedia.org/wiki/Datei:Opera_2015_icon.svg
https://de.wikipedia.org/wiki/Datei:Google_Chrome_icon_(September_2014).svg
https://de.wikipedia.org/wiki/Datei:Windows_Internet_Explorer_Logo.png

Umgang mit dem Browser

- Browser sind Programme, die das direkte Agieren im Internet ermöglichen und gleichzeitig weitreichende Zugriffsrechte auf den Geräten besitzen (bspw. Kamera- und Mikrofonzugriff; so weit erteilt)
- Rufen nicht mehr nur statische Seiten auf, sondern sind in der Lage Programme auszuführen
- Gleichzeitig Zugang zum Umgang mit sensiblen Daten (Online-Banking, Social Media, Cloud Speicher, Zahlungen, Shopping usw.)

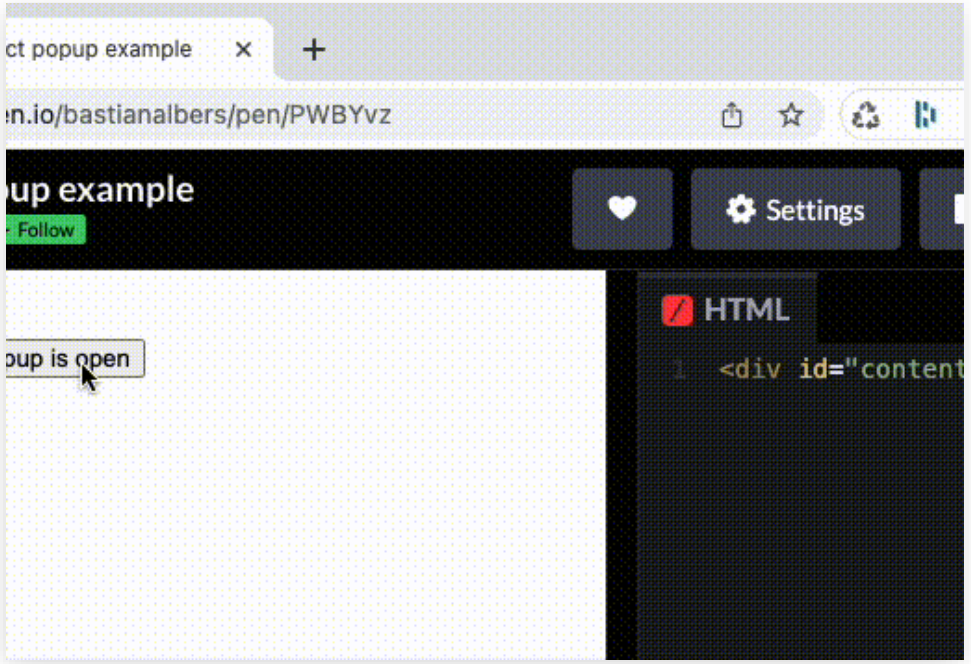
Umgang mit dem Browser

- Pop-Ups
- Cookies
- Tracking
- Unsichere Verbindungen
- Undeutliche URLs
- Phishing
- Veraltete Version
- Unseriöse Werbung
- Downloads von unseriösen Quellen
- Gespeicherte Passwörter

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

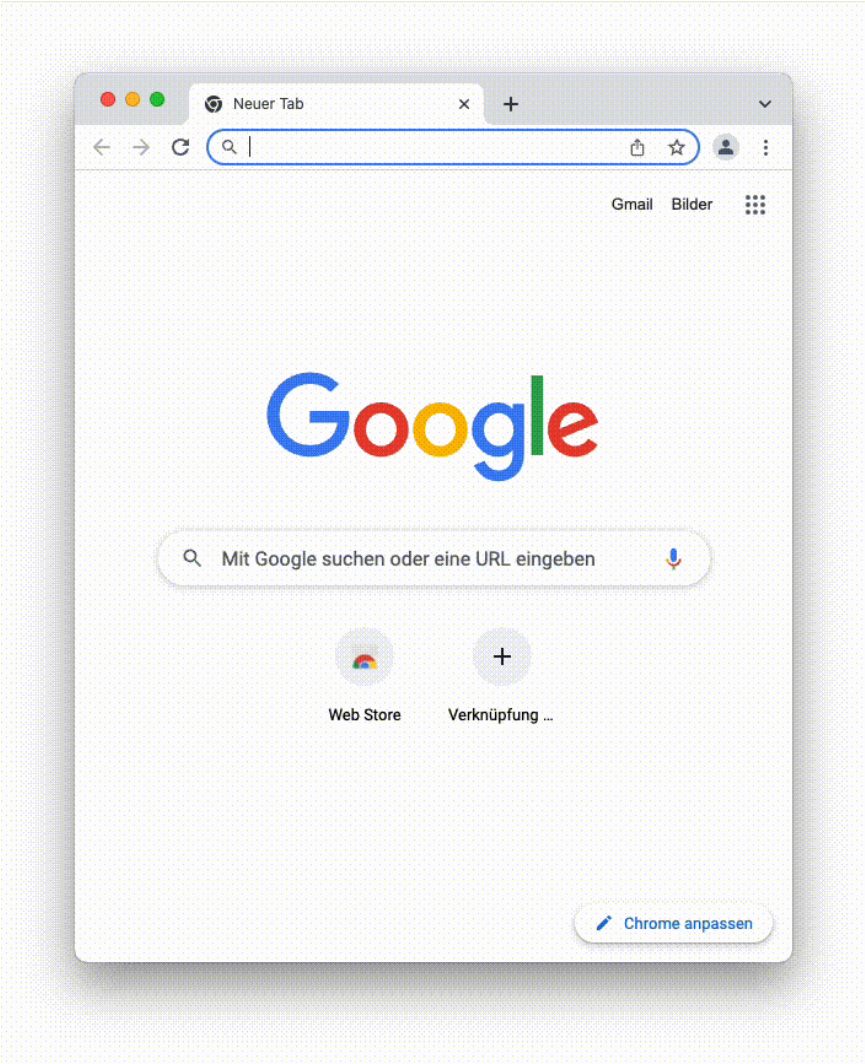
- Pop-Ups
- Grundsätzlich deaktivieren



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

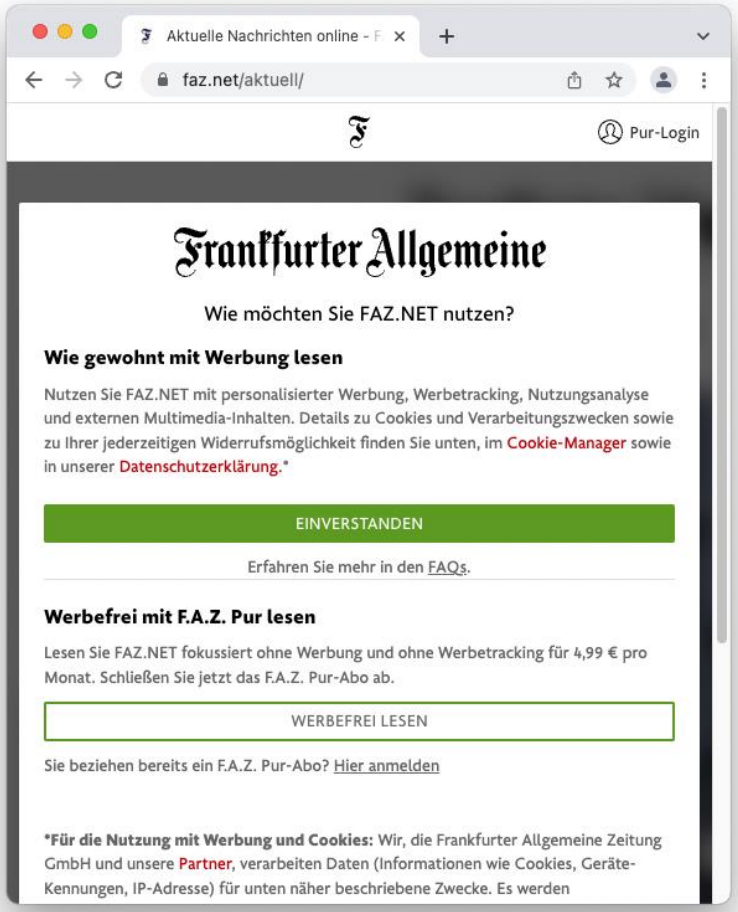
- Pop-Ups
- Grundsätzlich deaktivieren



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- Cookies
- Regelmäßig löschen

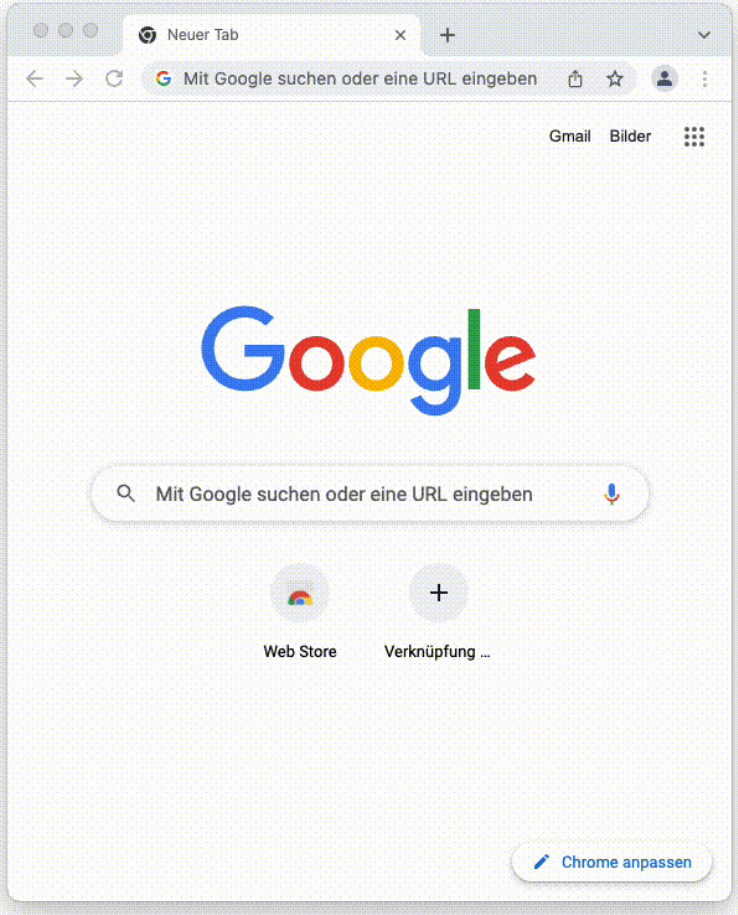


https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- Cookies

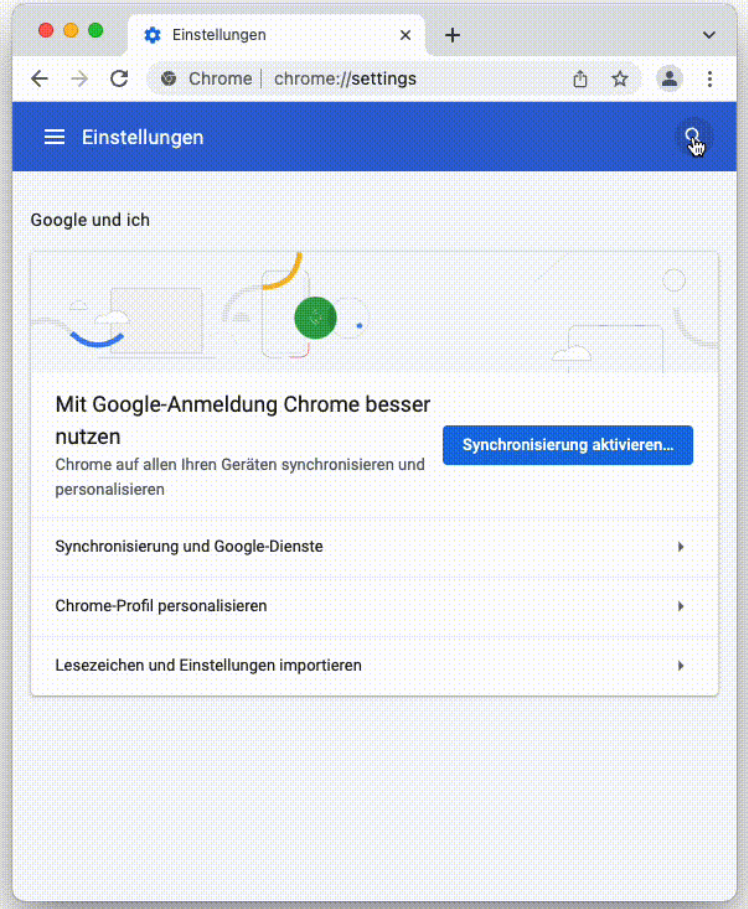
- Regelmäßig löschen
- Drittanbieter Cookies generell deaktivieren



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- Tracking
- Wenn möglich ausschalten

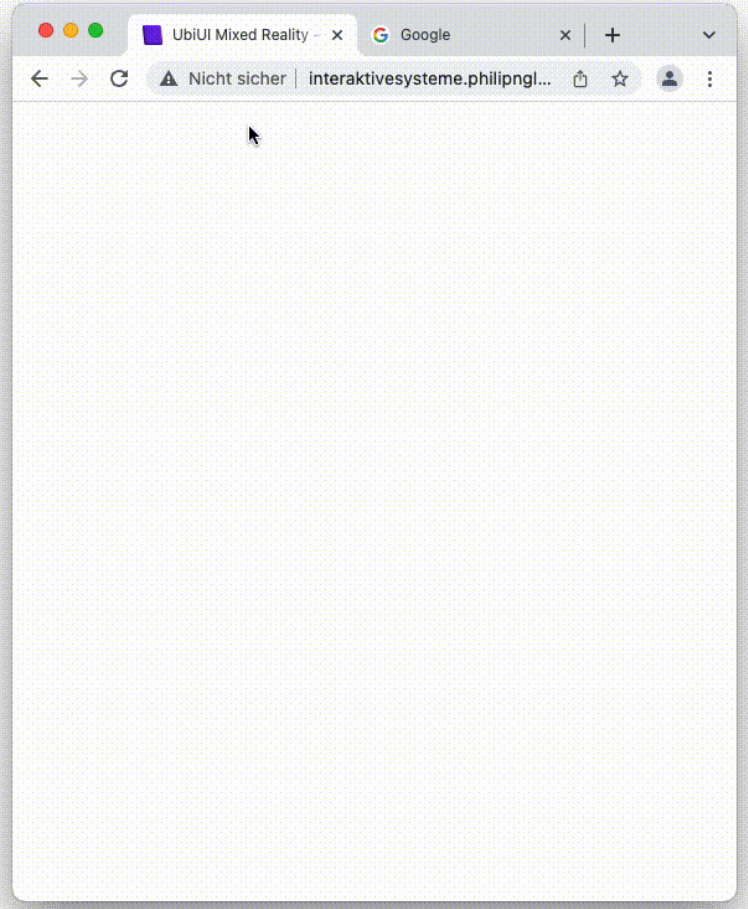


https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Unsichere Verbindungen**

- Nur betreten, wenn man sich sicher ist, dass keine Gefahr besteht
- Ansonsten Verbindung ablehnen
- Darauf achten, dass **https://** vor der URL steht, nicht **http://**



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Undeutliche URLs**

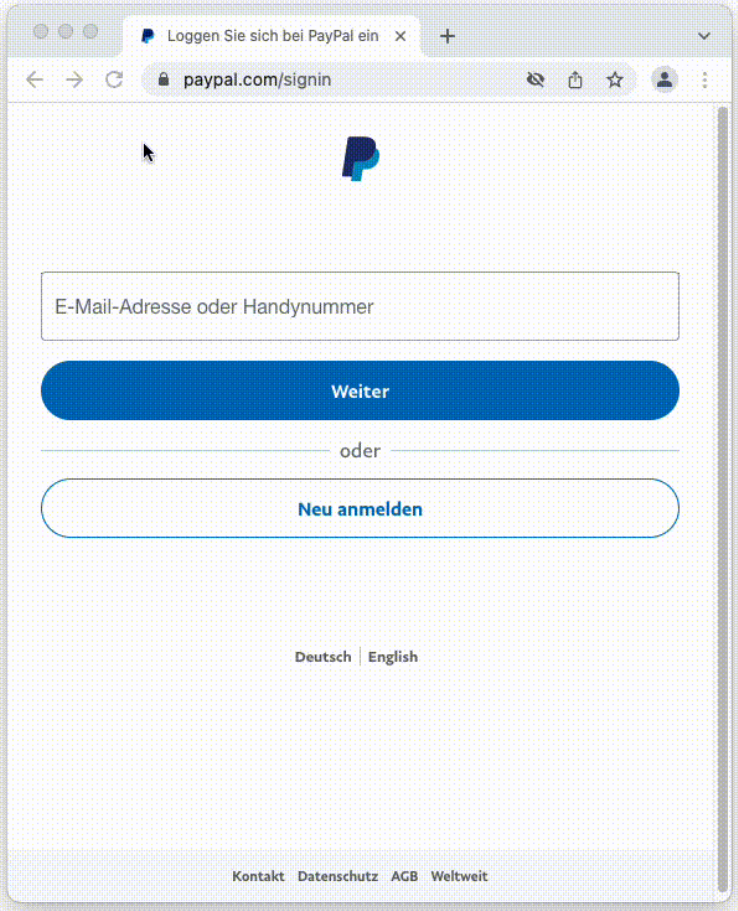
- Richtige Adresse MUSS direkt vor .com, .de, .co.uk oder Ähnlichem stehen
- Nicht: **paypal.irgendwas.com** sondern **paypal.com**

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Phishing**

- Sicher gehen, dass man sich auf der richtigen Seite befindet (undeutliche URLs vermeiden)
- Darauf achten, dass **https://** vor der URL steht, nicht **http://**
- Zertifikat prüfen



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

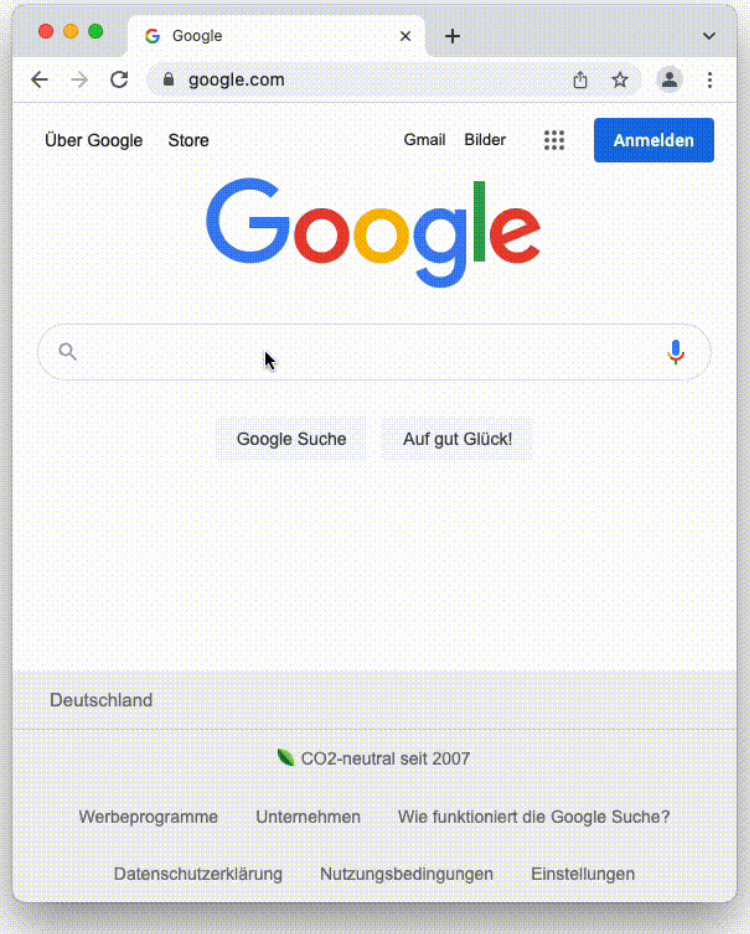
- **Veraltete Version**

- Unbedingt den Browser aktualisieren, wenn ein neues Update ansteht
  (Meistens wird man darauf hingewiesen)

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Unseriöse Werbung**
- Nicht anklicken
- Falls umgehbar auch nicht schließen (manchmal verbirgt sich ein Link hinter dem X zum Schließen)
- Ad-Blocker installieren



https://getadblock.com/de/

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Downloads von unseriösen Quellen**
- Grundsätzlich ausnahmslos vermeiden

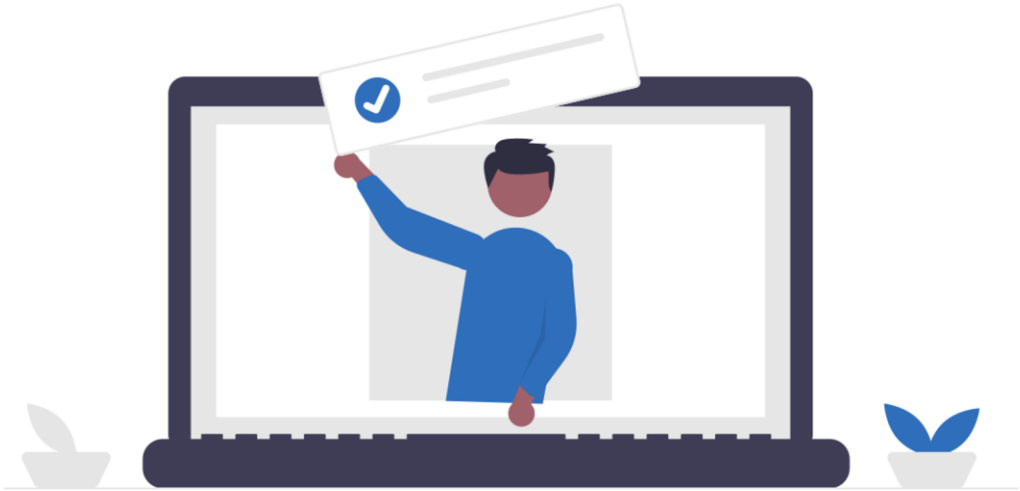
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

Umgang mit dem Browser

- **Gespeicherte Passwörter**
- Passwörter nicht im Browsereigenen Passwort Manager speichern

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/der-browser_node.html

3. Gefahren und Lösungen beim Zugriff auf Konten & Social Media



Passwortsicherheit

Passwörter dürfen nicht:

- Zu kurz sein
- Mit Ihnen oder Ihrer Familie in Verbindung gebracht werden
- Zahlen oder Buchstabenfolgen sein
- Benutzername = Passwort

Passwortsicherheit

Regeln für Passwörter:

- Mindestens 10 Zeichen
- Groß und Kleinbuchstaben
- Zahlen und Sonderzeichen
- Keine Familien/Freundesnamen
- Sensible Zugänge benötigen extra starke Passwörter
- Unterschiedliche Passwörter für unterschiedliche Portale
- Niemandem die Passwörter sagen
- Ändern wenn bekannt wird, das Portal gehackt wurde

Sichere Passwörter – so geht's | Verbraucherzentrale.de

Passwortsicherheit

Passwortcheck:

https://www.stmd.bayern.de/service/passwort-check/online-anwendung-passwort-check/

Passwortsicherheit

Ist deine Mail in einem Daten-Leak?

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

Passwortsicherheit

Ist deine Mail in einem Daten-Leak? (international)

https://haveibeenpwned.com/

Passwort-Manager

Eigenständige Passwort-Manager-Programme:

- Pop-up Fenster kann auftauchen wenn Eingabefeld angeklickt wird
- Zentrales Masterpasswort wird benötigt

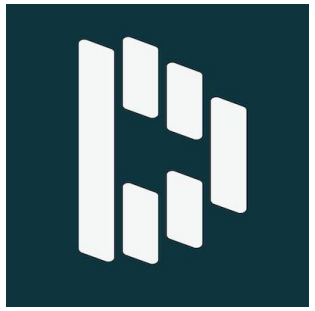
Im Browser integrierte Passwortmanager:

- Im Browser integriert
- Fügen eigenständig Passwort und Username ein
- Mögliche Sicherheitslücken, da es nicht Priorität hat bei den Browsern
- Extension

Passwort-Manager (Vergleich)

+ Vorteile	- Nachteile
Verwahren von Passwörtern und Benutzernamen mittels Verschlüsselung	Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
Unterstützung bei der Passwortvergabe: z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.	Alle Passwörter können auf einmal gestohlen werden, sollte ein Cyber-Angriff auf einen Passwort-Manager erfolgreich sein.
Warnung vor gefährdeten Websites und möglichen Phishing-Attacken, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.	Bei cloudbasierten Diensten vertrauen Sie den Zugang zu all Ihren sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind.
Synchronisieren möglich: Wer Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen nutzen möchte, kann ein Programm verwenden, das diese synchronisiert.	

Passwort-Manager



Dashlane

Keeper

1Password

KeePass

https://www.dashlane.com/de/business/try

https://www.keepersecurity.com/blog/2019/06/25/a-brand-new-look-for-keeper/

https://1password.com/img/redesign/logo-light-bg.svg

https://de.wikipedia.org/wiki/KeePass#/media/Datei:KeePass_icon.svg

Passwort-Manager

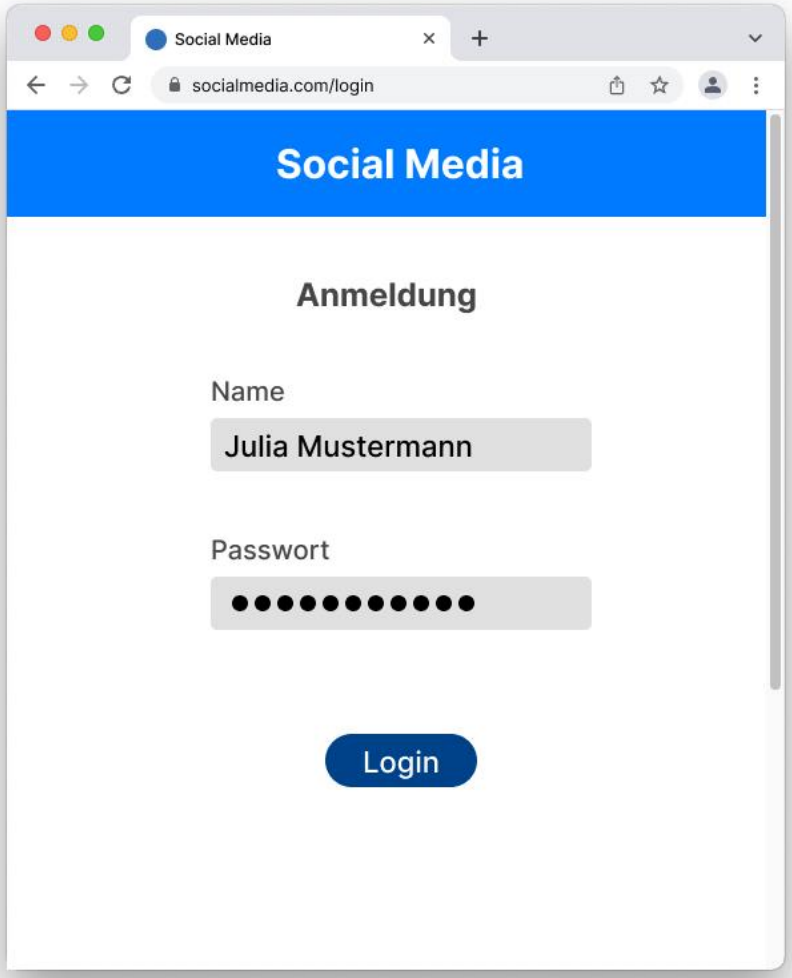
KeePass:

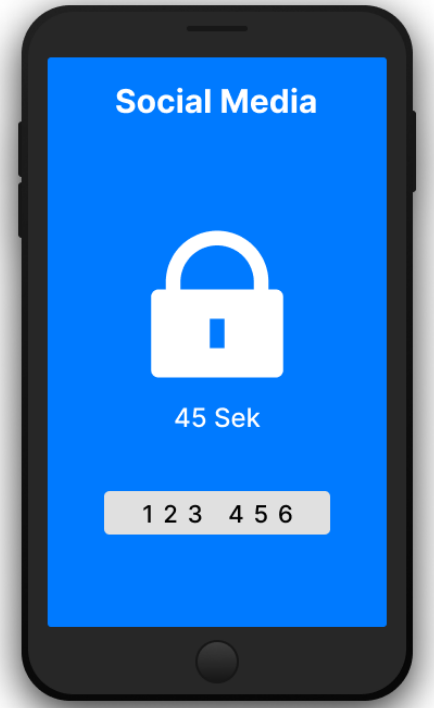
- Kostenlos & open source
- Durch open source höhere Gefahr für Sicherheitslücken
- Selbstverwaltung von Datenbank – lokale Verfügbarkeit
- Keine Automatische Log-in Funktion
- Veraltetes design

Dashlane:

- Zusatzdienste & Gerätesynchronisierung nicht kostenlos
- Ausgezeichnete Automatische Log-in Funktion
- AGB‘s

Zwei-Faktor-Authentifizierung





Zwei-Faktor-Authentifizierung

- Authentifizierungs-Apps
- E-Mail
- SMS
- Tan-App

Vor allem verwenden bei:

- Plattformen mit sensiblen Daten (Banking)
- Zugriffe auf Wichtige Plattformen

Zwei-Faktor-Authentifizierung

+ **Vorteile der Zwei-Faktor-Authentifizierung:**
- Wird das Passwort gehackt, hat man trotzdem keinen Zugriff.
- Hinweis wenn das Passwort gehackt ist.

- **Nachteile:**
- Verlängert den Anmeldevorgang
- Verlust, des Gerätes/Mail/App kann dazu führen, das der Zugriff verloren geht

BSI - Zwei-Faktor-Authentisierung – mehr Sicherheit für Geräte und Daten (bund.de)

Umgang mit sozialen Medien

- Keine Sensiblen Daten herausgeben (Passwörter/Benutzernamen/Pins)
- Privatsphäreneinstellungen anpassen
- Nicht zu viel Informationen Preis geben
  - Bilder und Stories Zeitversetzt posten
  - Keinen Urlaubszeitraum verraten
- Nur Anfragen von bekannten annehmen.
- Zweifelhafte Anfragen prüfen
- Alte Accounts löschen: Das Internet vergisst nie

Umgang mit sozialen Medien

Zahlungen: (z. B. Ebay-Kleinanzeigen)

- Zahlungen über PayPal niemals über „Freunde und Familie“
- Wenn möglich PayPal nutzen – Bei nicht erhalt der Dienstleistung Geld zurück

Identitätsdiebstahl

- Kriminelle nutzen ihre Informationen um sich als Sie auszugeben
- Name, Adresse und Geburtsdatum können schon ausreichen (Bestellungen auf falschen Namen)
- Bankdaten für Käufe auf falschen Namen
- Fake-Accounts um Informationen von anderen Leuten zu erhalten & Mobbing

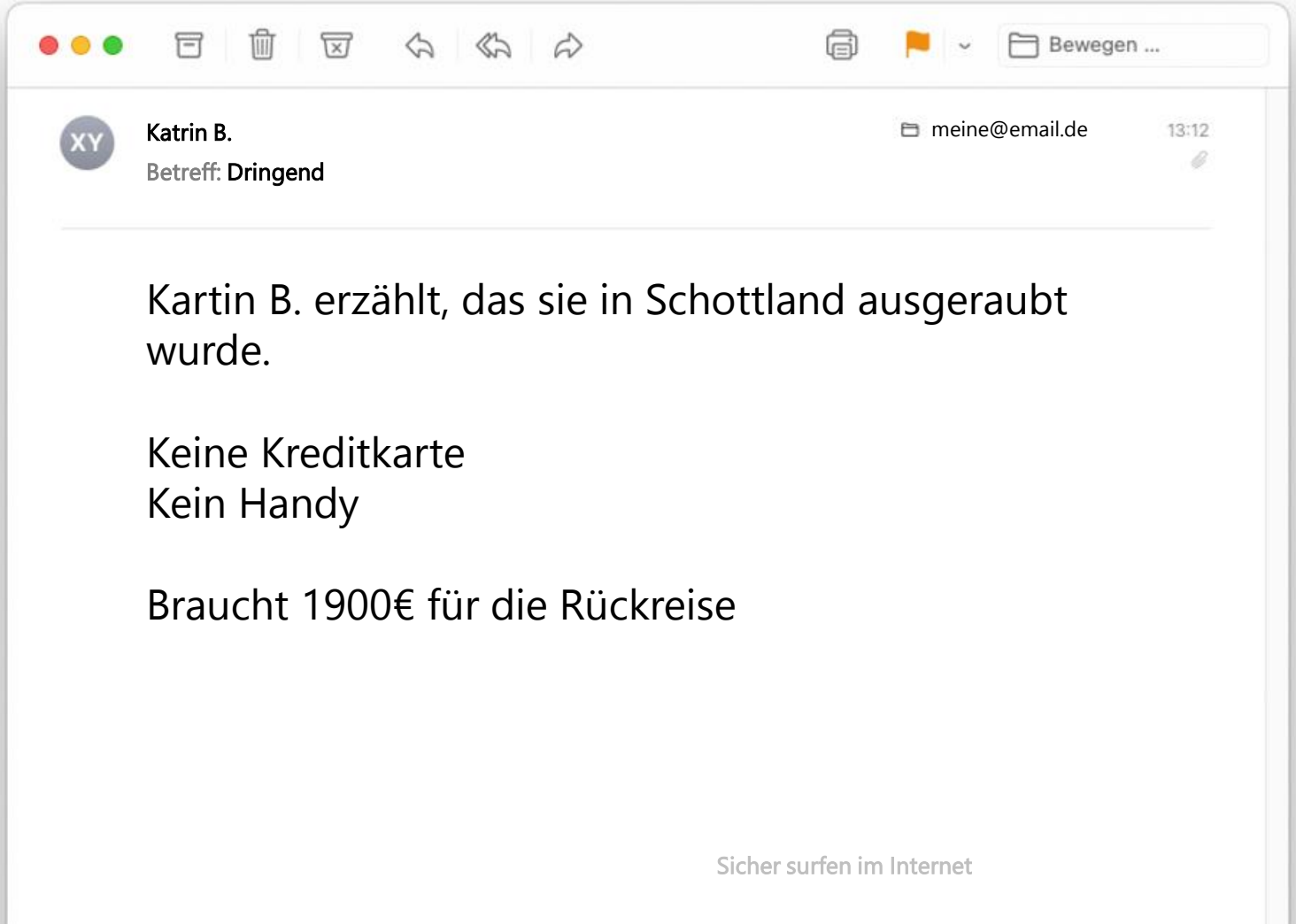
Identitätsdiebstahl

Folgen von Identitätsdiebstahl:

- Wiederkehrende Abbuchungen
- Falsche Bestellungen
- Cybermobbing
- Begehen von Cyber Straftaten
- Geld weg - Bei Fahrlässigem Umgang mit den Daten haftet man selbst

Identitätsdiebstahl im Internet: Wie er funktioniert und wie man sich schützen kann - iRights.info - Kreativität und Urheberrecht in der digitalen Welt – iRights.info

Phishing (auch SMS-Phishing)



Aber:
Katrin B. war noch nie in Schottland!

Phishing (auch SMS-Phishing)

Mail von anderem Absender als als der offiziellen Seite:

- z.B. sadjhsa@paypal.com
- Oder <beliebige Zeichenfolge>@kreisparkasse.de

noreply@paypal.com → ok, da offizielle Mail

- Bei Unsicherheit keinen Mail Inhalt anklicken und googeln ob Mail offiziell ist
- Unternehmen fragen niemals nach Login Daten

Sparkasse

Wichtige Kundeninformation Datum: 07.06.2020

Sehr geehrte/r [redacted]

jüngste hat die Regierung der Bundesrepublik Deutschland ihr 130 Milliarden schweres Konjunkturpaket verabschiedet.

Dieses bringt für Sie als Endverbraucher unzählige Vorteile mit sich, wie z.B. der Erhöhung von Freibeträgen, Erstattungen und vieles mehr.

Der wohl größte Vorteil ist die Herabsetzung der Mehrwertsteuer von derzeit 19% auf zukünftig 16%.

Für eine Bank wie uns, bedeutet dies zweifelsohne auch gewissen Anpassungen in unseren Systemabläufen.

So werden beispielsweise die monatlichen Kontoführungsgebühren vorübergehend abgeschafft.

Wenn Sie von der Abschaffung profitieren möchten, folgen Sie bitte der unten angezeigten Schaltfläche und führen Sie die entsprechenden Schritte durch. Nach Abschluss des Vorgangs werden Ihnen automatisch die oben genannten Gebühren erlassen.

Weiter

Bitte beachten Sie, dass diese positiven Anpassungen befristet sind. Wir empfehlen Ihnen daher eine zeitnahe Durchführung.

Mit freundlichen Grüßen

Ihr Service-Team

Dies ist eine automatisch versendete Nachricht.
Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zu Versendung von E-Mails eingerichtet ist.

© sparkasse.de 2020 Alle Rechte vorbehalten. | Handlungsregisternr. HRB 91513B | U St-ID DE 214205098

Phishing Sicherheits-Empfehlungen vom BSI

Was kann ich tun, wenn ich Opfer von Phishing geworden bin?

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-Checkliste-Phishing.pdf?__blob=publicationFile&v=1

Phishing Sicherheits-Empfehlungen vom BSI

Basistipps zur IT-Sicherheit

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

4. Wichtiges

Sicherheit von mobilen Betriebssystemen

Apple (iOS)	Android
Jede neue App wird genausten untersucht → weniger Apps → Weniger Apps mit Maleware	Leichtere Veröffentlichung → größere Auswahl an Apps → Größeres Risiko für Maleware
Zugriffsrecht kann eingestellt werden	Zugriffsrecht kann eingestellt werden
Weniger Nutzer → weniger Attraktivität für Hacker	Viele Nutzer → Höhere Attraktivität
Jede App läuft in einer Sandbox → kann nicht auf das Betriebssystem zugreifen	Maximale Transparenz & Flexibilität → Offener für Hacker
Updates für ein Smartphone bis zu 5 Jahre	Updates meistens nur 2 -3 Jahre für ein Smartphone

Was ist sicherer? Android oder iOS? - Avira Blog

iOS vs. Android Sicherheit 2021: Faktoren, die wichtig sind (coolsten.de)

Sicherheit von mobilen Betriebssystemen

Fazit:

- iPhone ist sicherer aber man ist eingeschränkter.
- Android hat mehr Angriffsfläche jedoch kann man so gut wie alles selbst konfigurieren.

- Auf Datenzugriffe achten und Minimal-Einstellungen wählen.
- Keine Apps von unbekannten Quellen herunterladen und nur Apps die schon mehrere Millionen male heruntergeladen wurden herunterladen.
- Kommentare im App Store durchlesen und auf Bewertungen achten

Antivirenprogramme

- Virenschutzprogramme sind angreifbar
- Virenschutzprogramme öffnen „neue Türen“ für Hacker
- z.B. Avast hat ein Browser Sicherheitsfeature deaktiviert sodass eine Sicherheitslücke entstanden ist
- Verlangsamt den Rechner

- Ausnahme: Windows Defender
- Durchsucht keine Windows Spezifischen Dateien → Keine neuen Sicherheitslücken
- Integriert in das System dadurch besser als externe Programme

→ Köpfchen einsetzten beim Surfen

Warum ich keine Internet Security Suite verwende: Ein Kommentar von Diplom-Informatiker Jörg Geiger - CHIP

Vielen Dank!
Noch Fragen?

in Zusammenarbeit mit dem Jugendhaus Hohbuch

organisiert von Philip Engler & Rodion Kraft

Internetführerschein

Abschließend: **Quiz**