

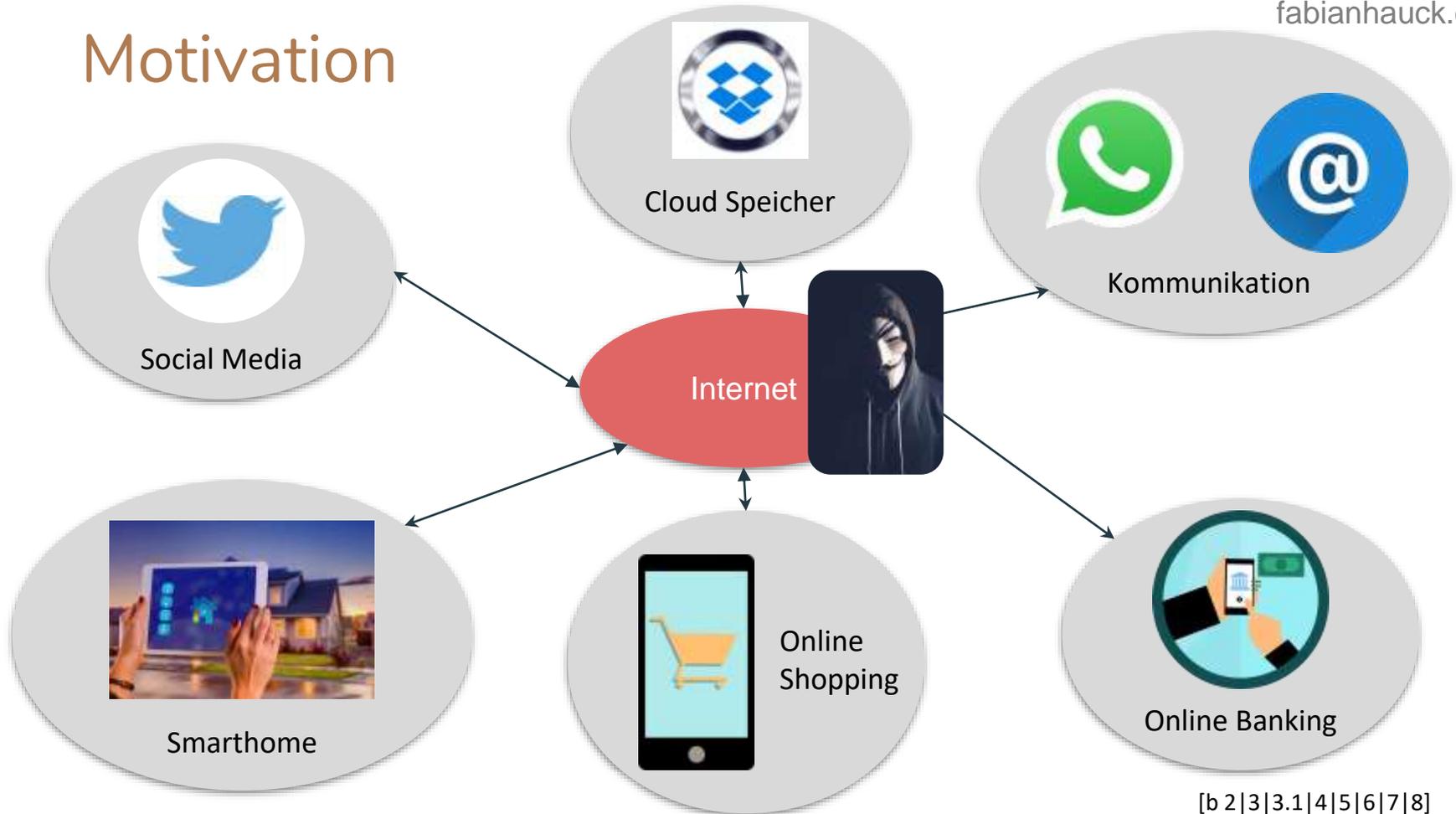


Data Security Workshop

Fabian Hauck



Motivation



Gliederung

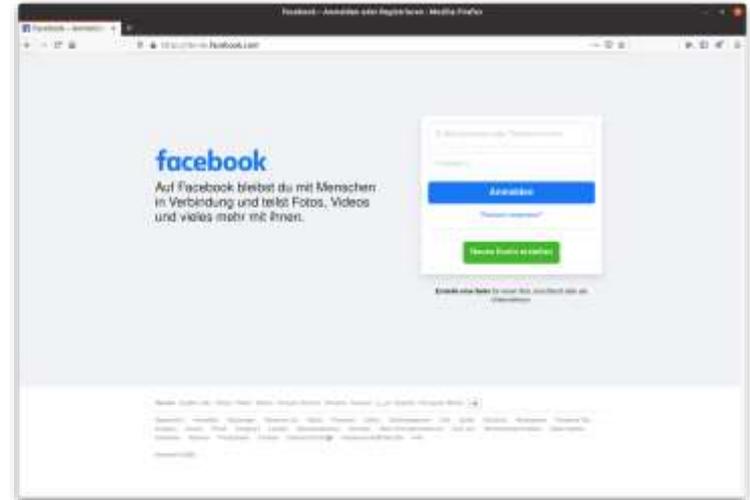
1. Passwörter
2. 2-Faktor Authentifizierung
3. Phishing
4. Sicher im Internet surfen
5. Gerätesicherheit



Passwörter

Passwörter

- Definition: “Ein **Passwort** ist eine Zeichenfolge, die zur Zugangs- oder Zugriffskontrolle eingesetzt wird.” - [Wikipedia](#)
- Web Services (E-Mail, Instagram) verwenden Passwörter oft in Kombination mit Benutzernamen, um
 - meine Daten mir zuzuordnen
 - meine Daten vor Fremden zu schützen
 - meine Daten vor fremder Veränderung zu schützen
- Passwörter werden aber auch für PC Logins, Smartphones, WLAN Netzwerke, Router usw. verwendet.



=> **Passwörter schützen Daten oder Geräte, da sie ein Geheimnis sind, das nur du kennst.**

Typische Fehler mit Passwörtern

- Wählen von Passwörtern, die einfach erratbar sind
 - Geburtsdatum, Kindernamen, Haustier
 - sehr kurze Passwörter
- Für jeden Account das gleiche Passwort verwenden

09.02.1999

Bello

Moritz

rush2112

[3]

Insbesondere das E-Mail Passwort sollte nur einmal verwendet werden, da ein Angreifer per E-Mail andere Passwörter zurücksetzen kann.

[Passwort Listen Demo](#)

Angriffe auf Passwörter

1. **Bruteforce:** Raten von sämtlichen Kombinationen
2. **Passwort-Listen:** Ausprobieren von häufig benutzten Passwörtern
3. **Recherche:** Nutzen von persönlichen Informationen, um mögliche Passwörter zu erstellen
4. **Shoulder Surfing:** An öffentlichen Orten bei der Passworteingabe beobachten
5. **Phishing:** Eingabe des Passworts auf einer bösartigen Webseite, die aussieht wie eine legitime

Improve Your Passwords!

Wie kann man sich gute Passwörter merken?

1. Satz bilden und Anfangsbuchstaben merken. Beispiel:

- Die 4 Workshops der Jugendpresse BW im September waren sehr interessant! => **Passwort:** D4WdJBWiSwsi!

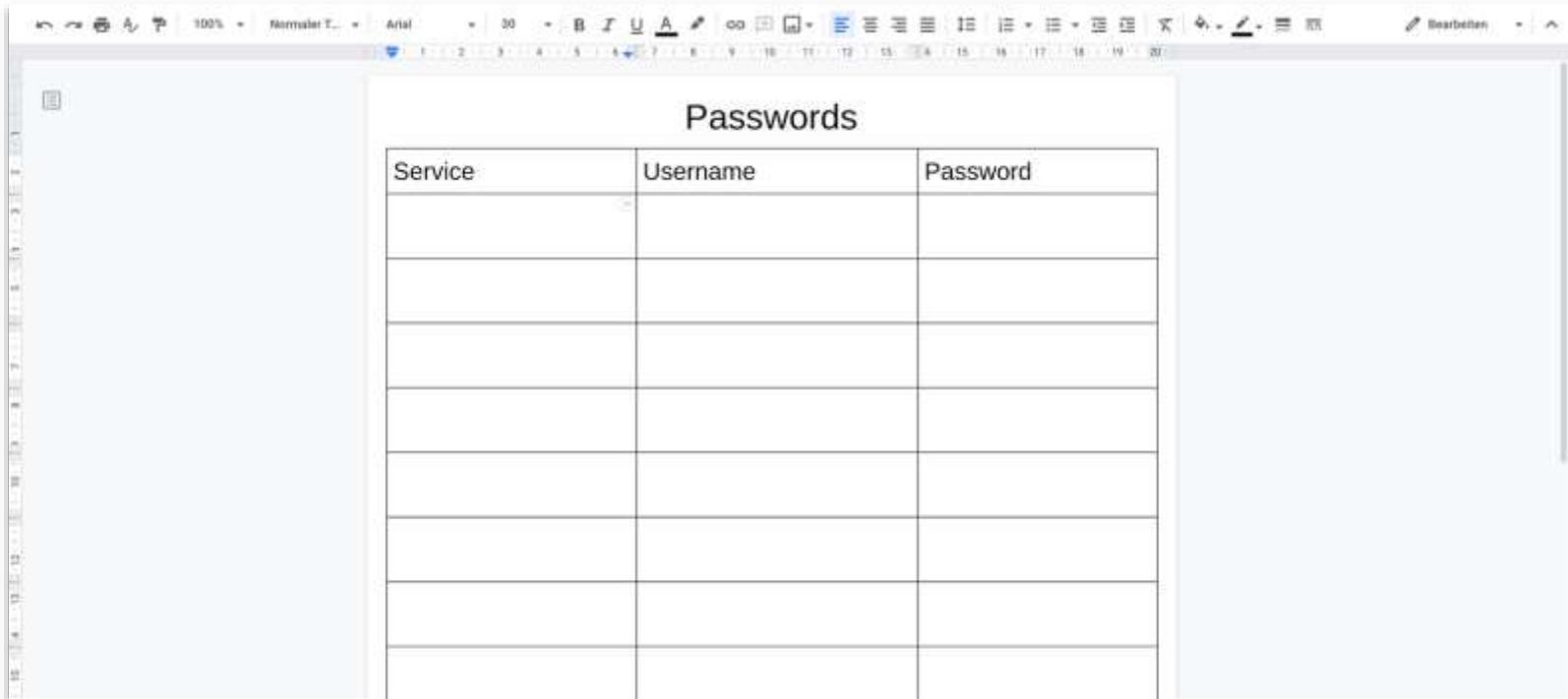
2. Länge schlägt Komplexität: Merken von verschiedenen Wörtern. Beispiel:

- **Passwort:** Sonne arbeiten Tisch Workshop

Passwörter merken



Passwörter merken



The image shows a screenshot of a spreadsheet application. The title bar at the top indicates a zoom level of 100%, a font size of 10, and a font style of Arial. The spreadsheet itself has a title "Passwords" centered above a table. The table has three columns: "Service", "Username", and "Password". There are ten rows in total, with the first row being the header and the remaining nine rows being empty.

Service	Username	Password

Passwort Manager

- Speichert alle Passwörter an einem Ort und verschlüsselt diese mit einem Masterpasswort
- Kann oftmals Passwörter mit verschiedener Länge und Komplexität erzeugen
- Es gibt verschiedene Arten von Passwort Managern:
 - im Browser integriert (z.B. Google Chrome, Mozilla Firefox)
 - als Webservice mit Browser Plugin (z.B. True Key, LastPass)
 - lokale PC Software (z.B. KeePass, Enpass)



[b1]



Keepass Passwort Manager einrichten

Software:

- Windows / macOS / Linux: [KeepassXC](#)
- Android: [Keepass2Android](#)
- iPhone / iPad: [KeePassium](#)

[Link zum YouTube Video](#)

Account-Sicherheit verbessern

- **Bisher:** Schutz des Kontos durch Passwort → ein Geheimnis
- Verbesserung der Sicherheit durch einen **2. Faktor**, den man “besitzt” → Beispiel: zum Anmelden muss man neben dem Passwort auch eine PIN eingeben, die man per SMS empfängt
- 2-Faktor-Authentifizierung ist gesetzliche Pflicht für Banken → z.B. durch TAN, generiert mit TAN Generator und Bankkarte (Bankkarte muss man “besitzen”) [1]
- 2-Faktor-Authentifizierung wird auch von vielen Web Services unterstützt (z.B. Google Konto, Apple ID, Amazon, PayPal)

→ **2-Faktor-Authentifizierung sollte für alle wichtigen Konten verwendet werden!**



WEB.DE E-Mail 2-Faktor-Authentifizierung einrichten

[Link zum YouTube Video](#)

Phishing

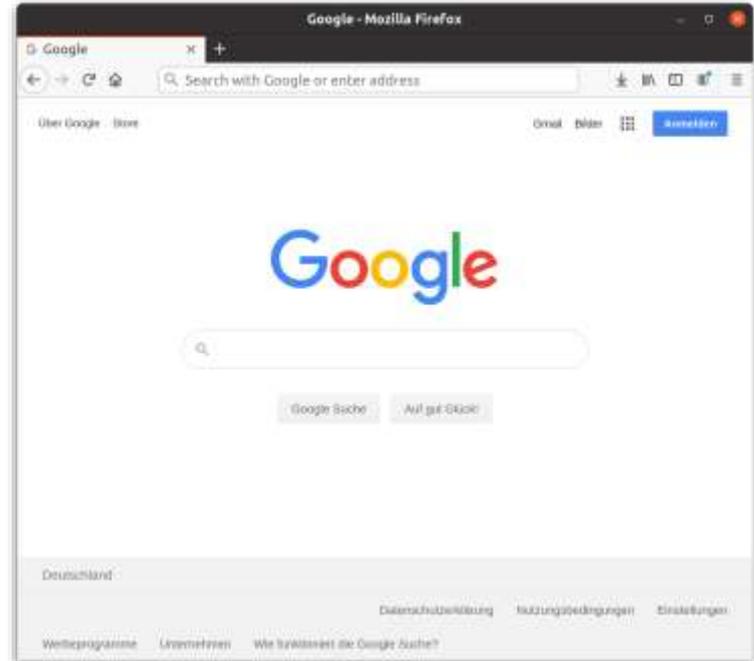
Phishing

Was ist ein Webbrowser?

- Computerprogramm zum Anzeigen von Webseiten im World Wide Web
- Es sind viele verschiedene Programme verfügbar:
 - Google Chrome
 - Apple Safari
 - Mozilla Firefox
 - Internet Explorer
 - Microsoft Edge
 - Opera



[b24]



Phishing

Was ist eine Domain?

- Eindeutiger Name einer Webseite, z.B. google.com, facebook.de, amazon.com
- Wird in die Adresszeile des Browsers eingegeben, um die Webseite aufzurufen

So wie die Adresse den Ort eines Hauses angibt, so lokalisiert die Domain eine Webseite im Internet.



Phishing

Uniform Resource Locator (URL)

- Enthält den Domainnamen einer Webseite
- Enthält zusätzliche Informationen,
 - **wie** eine Seite aufgerufen wird (**Protokoll**)
 - **welcher Teil** einer Webseite aufgerufen wird (**Pfad**)
- Beispiele:
 - <http://www.vvs.de/home/>
 - <https://google.com/>
 - <https://jpbw.de/naechste-workshops-seminare/>

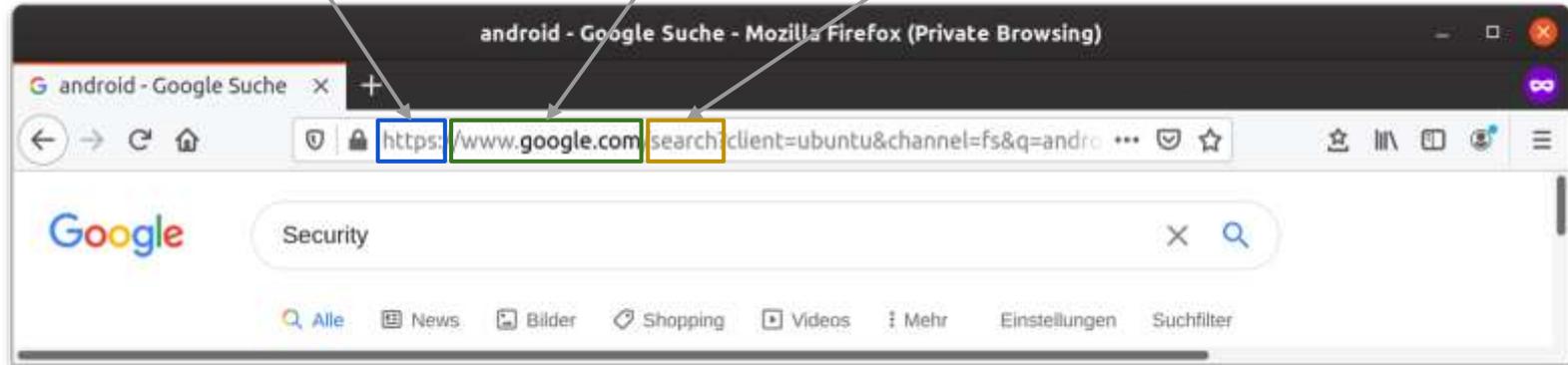
Protokoll = Wie erreicht man das Haus? Mit dem Auto (**https**) oder zu Fuß (**http**)?

Pfad = In welchem Stockwerk des Hauses befindet sich die Wohnung?

Phishing

Uniform Resource Locator (URL)

Protokoll (http oder https) **Domain (Adresse der Webseite)** **Pfad**



Phishing

Was ist Phishing?

Definition: “Unter dem Begriff **Phishing** [...] versteht man Versuche, über gefälschte **Webseiten**, **E-Mails** oder **Kurznachrichten** an persönliche Daten eines **Internet-Benutzers** zu gelangen [...].” - [Wikipedia](#)

→ **Angreifer haben es dabei insbesondere auf Logindaten für Online Banking oder Shopping Accounts abgesehen.**



Phishing

Beispiel für Phishing

Datum: 17.07.2019

amazon

Sehr geehrte/r [REDACTED]

wir, das Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst. Aus diesem Grund ist es vorzuziehen eine routinemäßige Sicherheitskontrolle durchzuführen.

Der Datenabgleich dient dazu, dass Ihre persönlichen Daten fortwährend aktuell sind. So können wir Sie unter anderem vor Missbrauch durch Dritte schützen.

Sollte einer Abweichung der hinterlegten Daten vom System erkannt werden, werden Sie temporär gesperrt und von einem Mitarbeiter schriftlich informiert.

Wir bitten Sie Ihre Daten binnen 48 Stunden vollständig zu verifizieren.

[Weiter zur Verifizierung](#)

mit freundlichen Grüßen,
Ihr Amazon-Kundenservice

Dies ist eine automatisch generierte Nachricht. Bitte antworten Sie nicht auf diese E-Mail, da die Adresse nur zur Verifizierung von E-Mails eingerichtet ist.

Prime Day ist Montag, 15. Juli & Dienstag, 16. Juli

Ein zweitägiges Feuerwerk voller toller Angebote, Entertainment-Events und vieles mehr.
Machen Sie sich bereit

prime day

© Amazon.com Inc. oder Tochtergesellschaften. Alle Rechte vorbehalten

S Sparkasse



Sehr geehrte/r [REDACTED]

Ihre persönlichen Daten bedürfen der Aktualisierung. Sie sind verpflichtet, Ihre Daten bei Aufforderung zu aktualisieren. Sollten Sie Ihre Daten nicht innerhalb der nächsten 14 Tage fristgerecht bis zum 01.08.2019 aktualisiert haben, werden wir Sie schriftlich per Einschreiben zur Aktualisierung auffordern. Hierbei kann ein Entgeld von 2,58 Euro entstehen.

Aktuelle Versandadresse:

[REDACTED]

[Zur Aktualisierung](#)

[Weitere Informationen auf der Webseite des BSI](#)



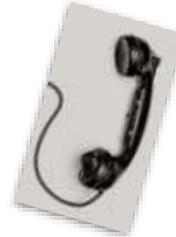
Phishing Beispiele zeigen



Phishing

Unterschiedliche Formen von Phishing

- **E-Mail** → haben wir bereits gesehen
- **Webseiten** → oft in einer E-Mail verlinkt
- **SMS / Whatsapp** → gleiches Prinzip wie bei E-Mails
- **Anrufe** → z.B. Anruf von einem falschen Microsoft Support, der behauptet, dass ein Fehler bei dem eigenen PC vorliegt
- **Post** → gleiches Prinzip wie bei E-Mails, aber eher selten [5]



[b3|3.1|11
|12|13]

Phishing

Phishing erkennen

- Phishing-Angriffe täuschen oft dringenden Handlungsbedarf vor
- Abfrage vertraulicher Daten
- Anrede ist oft unpersönlich oder enthält Teile der eigenen E-Mail Adresse
- Absender-Domain in E-Mails überprüfen
- URLs im Browser überprüfen
- Niemals auf Links in verdächtigen E-Mails klicken
- Niemals Anhänge in verdächtigen E-Mails öffnen
- Rechtschreibung und Grammatik überprüfen → Phishing E-Mails/Webseiten haben oft Fehler [4]

“Noch einmal die Grundregel vorweg: Kein Kreditkarteninstitut und kein seriöser Anbieter fordert Sie per E-Mail auf, vertrauliche Zugangsdaten preiszugeben – auch nicht um der Sicherheit willen.” - [BSI](#)



[b18]

Sicher im Internet surfen

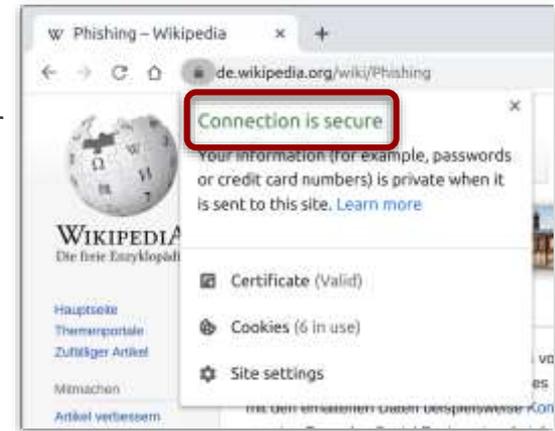
Sicher im Internet surfen

Verschlüsselte Verbindungen erkennen

- Es gibt zwei verschiedene Arten eine Webseite aufzurufen
→ über HTTP oder HTTPS
- Das **S** von HTTPS steht für **Secure** → persönliche Daten, Passwörter oder Kreditkartennummern werden dann nur verschlüsselt übertragen

→ Eine verschlüsselte Verbindung ist sehr wichtig, da sonst sensible Daten von Angreifern mitgelesen werden können.

Vorheriges Beispiel: Wie erreicht man das Haus? Sicher mit dem Auto (**https**) oder unsicher zu Fuß (**http**)

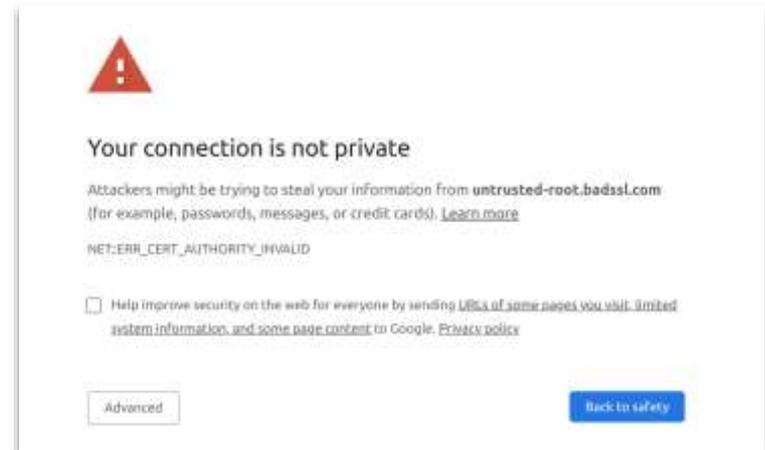


Browser Demo

Sicher im Internet surfen

Allgemeine Tipps

- Benutzung von separatem Browser oder Incognito Modus / Privates Window für Online Banking
- Vor einer Domain immer "https://" eingeben
- Immer auf den Domainnamen und das Schlosssymbol links daneben schauen
- Nicht vertrauenswürdige Webseiten sofort verlassen
- Keine Warnmeldungen ignorieren



Nicht ignorieren!!!

Sicher im Internet surfen

VPN und Tor

VPN:

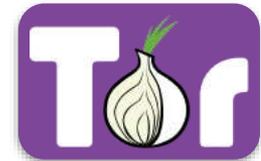
- Pro: Schutz vor Angreifern im lokalen Netzwerk
- Contra: VPN-Anbieter kann sämtlichen Datenverkehr mitlesen

Tor:

- Pro: anonymisiert die eigene Internetadresse, Identität kann aber trotzdem anderweitig preisgegeben werden
- Contra: Tor-Endpunkt bekommt sämtlichen Datenverkehr mit



[b23]



Gerätesicherheit

Gerätesicherheit

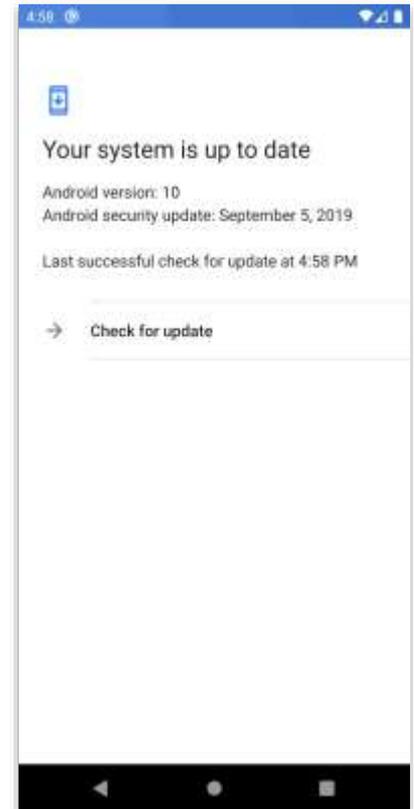
Updates, updates, updates!!!

- Die meisten modernen IT Geräte bekommen regelmäßig Updates
→ insbesondere Sicherheitsupdates werden meist alle ein bis zwei Monate verteilt

→ **Vor allem die Sicherheitsupdates sollten regelmäßig installiert werden, um sich vor aktuellen Sicherheitslücken zu schützen!**

- Geräte, die regelmäßig upgedatet werden müssen:
 - Windows PC / Mac
 - Android Smartphone / iPhone / iPad / Smartwatch
 - WLAN Router / NAS / Smarthome Geräte
 - Smart TV / AV Receiver / Streaming Stick

Update Demo



Gerätesicherheit

Virens Scanner

- Windows 10: integrierter Windows Defender bietet ausreichende Sicherheit
- Android: Virens Scanner nicht nötig, solange man nur Apps aus dem Play Store installiert
- iPhone / iPad: Virens Scanner nicht nötig
- macOS: hat schon einen integrierten Virens Scanner wie Windows (XProtect) [6]

[Siehe auch die Empfehlungen des BSI](#)

Windows Defender Demo



[b19]

Gerätesicherheit

Allgemeine Tipps

- IT Geräte an öffentlichen Orten niemals unbeaufsichtigt lassen
- Nur vertrauenswürdige Programme installieren
- Nicht benötigte Programme deinstallieren
- E-Mail Anhänge nur öffnen, wenn der Absender vertrauenswürdig ist
- Keine offensichtlichen Warnmeldungen übergehen
- Festplatte verschlüsseln → unter Windows mit [BitLocker](#) (bei Problemen kann [dieses Tutorial](#) helfen), unter macOS mit [FileVault](#)



[b20]

Device Demo

Backup

Regelmäßige Backups für Datensicherheit

- Daten von IT Geräten sollten regelmäßig gesichert werden, um Datenverlust zu vermeiden
- Backups sind aber auch notwendig, um nach einem Virenbefall das Gerät wiederherzustellen
→ insbesondere wenn eine Ransomware die eigenen Daten verschlüsselt hat und Lösegeld verlangt

→ Lösegeld sollte niemals bezahlt werden, da dadurch die Angreifer nur motiviert werden weitere Angriffe zu starten!



[b15]

Backup

Cloud-Speicher und externe Festplatten

- **Externe Festplatte:** manuelles Backup der eigenen Daten in regelmäßigen Abständen
 - Vorteil: Speicherplatz ist sehr billig
 - Nachteil: Backups müssen manuell gemacht werden
- **Cloud-Speicher:** Dateien werden automatisch in die Cloud geladen
 - Vorteil: Dateien werden in der Regel versioniert → alte Dateien können wiederhergestellt werden
 - Nachteil: Die meisten Anbieter bieten nur wenig Speicherplatz kostenlos an

→ Ideal ist eine Backup-Strategie mit Cloud-Speicher und externer Festplatte



[b16]



[b21]

Dateisynchronisierung



[b22]

Weiterführende Themen

- Sichere Kommunikation:
 - Verschlüsselte E-Mails versenden
 - Verschlüsselte Messenger-Dienste
- Nutzung von Hardware-Security-Keys
- Anonym im Internet surfen → Tor Browser
- Schutz in öffentlichen Netzwerken oder Ländergrenzen umgehen → VPN
- Private Cloud zum sicheren und komfortablen Speichern von Dateien → Synology, QNAP



[b14]



[b23]

Fragerunde

[Hier klicken, um Feedback zu geben](#)

Quellen

- [1]: <https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/payment-services-directive-2-psd2-richtlinie.html#:~:text=Service-,Zwei%2DFaktor%2DAuthentisierung%20wird%20Pflicht%20beim%20Online%2DBanking,September%20angewandt%20werden.>
- [2]: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html
- [3]: <https://github.com/danielmiessler/SecLists>
- [4]: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/Schutzmassnahmen/schutzmassnahmen_node.html
- [5]: <https://www.computerbetrug.de/2012/08/neue-phishing-masche-datendiebe-versuchen-es-jetzt-per-post-6650>
- [6]: <https://www.macworld.co.uk/feature/mac-software/can-macs-get-viruses-3454926/#:~:text=As%20we've%20explained%20above,over%20auto%2Dupdate%20very%20quickly.>
- [7]: <https://www.datensicherheit.de/top-5-phishing-angriffe-deutschland>

Bilderquellen

- [b1] <https://pixabay.com/illustrations/box-lock-safe-metal-security-2864329/>
- [b2] <https://pixabay.com/vectors/twitter-tweet-twitter-bird-312464/>
- [b3] <https://pixabay.com/illustrations/soon-vector-whatsapp-soon-whatsapp-873316/>
- [b3.1] <https://pixabay.com/vectors/at-sign-email-news-e-mail-at-icon-1083508/>
- [b4] <https://pixabay.com/vectors/smartphone-shopping-shopping-cart-2995676/>
- [b5] <https://pixabay.com/vectors/money-transfer-banking-icon-buy-3630935/>
- [b6] <https://pixabay.com/photos/smart-home-house-technology-3920905/>
- [b7] <https://pixabay.com/photos/dropbox-storage-download-2815926/>
- [b8] <https://pixabay.com/photos/anonymous-hacker-network-mask-2821433/>
- [b9] <https://unsplash.com/photos/RLw-UC03Gwc>
- [b10] https://unsplash.com/photos/QR_vT8_hBZM
- [b11] <https://unsplash.com/photos/744oGeqpxPQ>
- [b12] <https://unsplash.com/photos/JYGnB9gTClS>
- [b13] <https://unsplash.com/photos/fb7yNPbT0I8>

Bilderquellen

- [b14] <https://unsplash.com/photos/4hfpVsi-gSg>
- [b15] https://unsplash.com/photos/JJPqavJBy_k
- [b16] <https://unsplash.com/photos/W4GR5u0M2JQ>
- [b17] <https://pixabay.com/photos/anonymous-collective-secret-hacker-4165613/>
- [b18] <https://pixabay.com/illustrations/phishing-fraud-cyber-security-3390518/>
- [b19] <https://pixabay.com/illustrations/security-professional-hand-keep-5213398/>
- [b20] <https://unsplash.com/photos/iIJrUoeRoCQ>
- [b21] https://www.flaticon.com/free-icon/cloud-storage_3014270?term=cloud&page=1&position=25 Author: Freepik
- [b22] https://www.flaticon.com/free-icon/laptop_718861?term=laptop&page=1&position=32
Author: DinosoftLabs
- [b23] https://unsplash.com/photos/VH_L_H4w7U8
- [b24] <https://pixabay.com/illustrations/browser-web-www-computer-773215/>