Unterwegs im Internet
...
aber sicher!

**Sicher surfen,
smart schützen –
Ihr digitaler Wegweiser**

Herzlich willkommen!

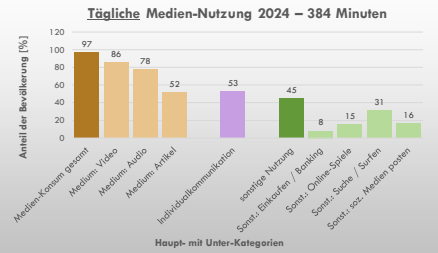
Bildquelle: KI MS-Copilot Designer 30.06.2024
Prompt: „Cybercrimes: digital, kreativ, virtuell"

1

Unterwegs im Internet … aber sicher! –
Sicher surfen, smart schützen!

2

Unterwegs im Internet … aber sicher!
1. Allgemeines – tägliche Medien-Nutzung



Quelle: ARD-ZDF-Onlinestudie 2024
Grundgesamtheit deutschsprachige Bevölkerung ab 14 Jahren: 70,08Mio., Stichprobe N=2500
Mehrfachnennungen möglich!

3

Unterwegs im Internet … aber sicher!
1. Allgemeines

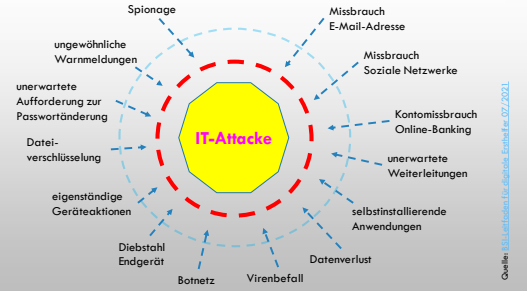
Nur 57% informieren sich präventiv zu Schutzempfehlungen!

Betroffenheit von Cyberkriminalität:
- Insgesamt: 24%
- allein 2024: 10%

Quelle: Cybersicherheitsmonitor 2024 - Bürgerbefragung zur Cyber-Sicherheit Mai 2024

4

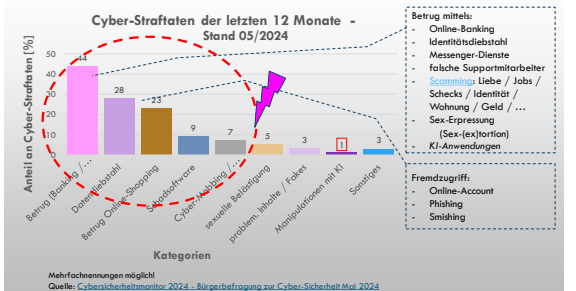
Unterwegs im Internet … aber sicher!
1. Allgemeines - typische IT-Sicherheitsvorfälle



Quelle: BSI-Lagebild zur digitalen Kriminalität 2021

5

Unterwegs im Internet … aber sicher!
1. Allgemeines – Anteile typischer Cyber-Straftaten

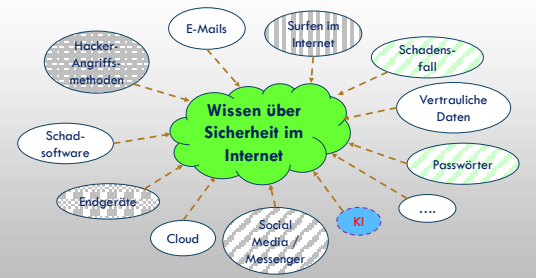


Mehrfachnennungen möglich!
Quelle: Cybersicherheitsmonitor 2024 - Bürgerbefragung zur Cyber-Sicherheit Mai 2024

6

Unterwegs im Internet … aber sicher!

1. Allgemeines – sinnvolle Wissensmodule



Quelle: Cybersicherheitsmonitor 2024 - Bürgerbefragung zur Cyber-Sicherheit April 2024

7

Unterwegs im Internet … aber sicher! –

Sicher surfen, smart schützen!

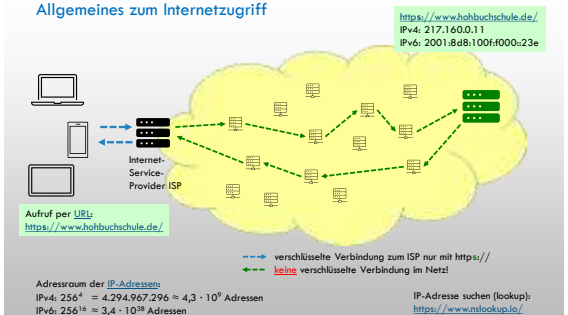
2. Internetzugang … der lange Weg durchs Internet

- Allgemeines zum Internetzugriff
- Der Browser – Pflege eines wichtigen Tools!
- Öffentliche WLAN-Netze – riskant?
- VPN – Was ist das? Wozu?

8

Unterwegs im Internet … aber sicher! 2.

Allgemeines zum Internetzugriff



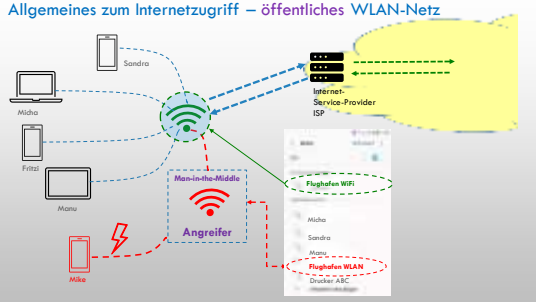
Adressraum der IP-Adressen:
IPv4: 256^4 = 4.294.967.296 ≈ $4{,}3 \cdot 10^9$ Adressen
IPv6: 256^{16} ≈ $3{,}4 \cdot 10^{38}$ Adressen

IP-Adresse suchen (lookup):
https://www.nslookup.io/

9

Unterwegs im Internet … aber sicher! 2.

Allgemeines zum Internetzugriff – öffentliches WLAN-Netz



10

Unterwegs im Internet … aber sicher! 2.

Allgemeines zum Internetzugriff – öffentliches WLAN-Netz

Achtung:
- Anmeldung im falschen WLAN-Netz
- Verteilung von Malware
- Auslesen eigener Aktivitäten und Daten / Passwörter (Man-in-the-Middel-Angriff = Snarfing)

Schutzmaßnahmen:
- Anmeldung im „richtigen" WLAN-Netz
- nur sichere Verbindung nutzen! (https://)
- keine sensiblen Daten abrufen bzw. senden (Bankverbindung, E-Mail, Social Media, …)
- Mögliche Zugriffe deaktivieren / Teilen ausschalten!
- VPN nutzen
- WLAN deaktivieren nach Gebrauch

11

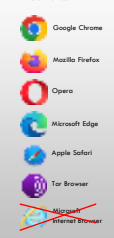
Unterwegs im Internet … aber sicher! 2.

Der Web-Browser – Pflege eines wichtigen Tools!

Der Web-Browser

- Tool für den Internetzugang mit Webanwendungen
  - Darstellung statischer und dynamischer Web-Seiten
  - Abarbeitung auch von Programmen
  - Verarbeitung und Speicherung auch sensibler Daten (Passwörter, Cookies, Chronik, Lesezeichen, …)
- verfügbar auf allen Endgeräten und Betriebssystemen
- gewünschten Browser auswählen, herunterladen, Einstellungen vornehmen und starten
- Empfehlung: Nutzung des gleichen Web-Browsers auf allen Endgeräten

Beispiele bekannter Web-Browser:



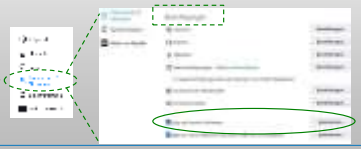
12

Unterwegs im Internet … aber sicher! 2.

Der Browser – Pflege eines wichtigen Tools! - **Einstellungen**

Thema:	Aktionen:
I. Pop-Ups / Pop-Unders	stets deaktivieren!
II. Cookies	regelmäßig (automatisch) löschen! Drittanbieter-Cookies generell deaktivieren
III. Tracking	möglichst ausschalten

Beispiel Firefox
Pop-ups: Einstellungen -> Datenschutz & Sicherheit



13

Unterwegs im Internet … aber sicher! 2.

Der Web-Browser – Pflege eines wichtigen Tools! - **Bedienung**

Thema:	Aktionen:
IV. Unsichere Verbindungen	unsichere Verbindung ***nicht*** nutzen! (**sicher**: https:// <> unsicher: http://) bei Nutzung: Risiko abschätzen!
V. gefälschte URLs	korrekter Domain-Name direkt vor der Toplevel-Domain .de, .com, .org, ... : korrekt: https://www.sparkasse.de/ falsch: http://www.DieSparkasse.de/

14

Unterwegs im Internet … aber sicher! 2.

Der Web-Browser – Pflege eines wichtigen Tools! - **Bedienung**

Thema:	Aktionen:
VI. Phishing	- stets korrekte URL prüfen - nur sichere Verbindung nutzen! (sicher: https://) - ggf. Zertifikat prüfen
VII. Veraltete Version	- Web-Browser immer aktuell halten!
VIII. Unseriöse Werbung	- nicht anklicken! - Blocker als Add-On installieren - Achtung! Möglichst separate Fenster ***nicht*** über „x" schließen

15

Unterwegs im Internet … aber sicher! 2.

Der Web-Browser – Pflege eines wichtigen Tools! - **Bedienung**

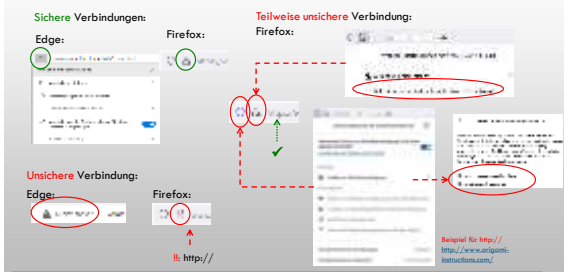
Thema:	Aktionen:
IX. Downloads von unseriösen Quellen	- grundsätzlich vermeiden!
X. Gespeicherte Passwörter / Passwortmanager	- möglichst ***nicht*** im Browser-speichern! - Nutzung eines separaten Passwort-Manager (digital / analog)

16

Unterwegs im Internet … aber sicher! 2.

Der Web-Browser – Pflege eines wichtigen Tools! - **Bedienung**

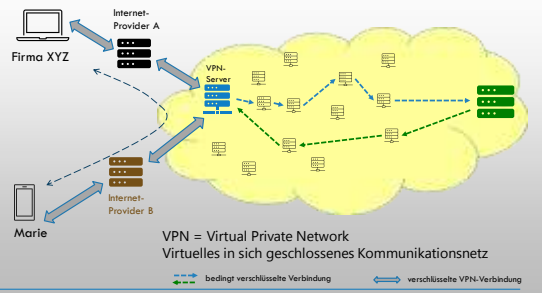
Beispiele für „Verbindungen", „Cookies" und „Tracking":



17

Unterwegs im Internet … aber sicher! 2.

VPN – Was ist das? Wozu?



18

Unterwegs im Internet … aber sicher! 2.

VPN – Was ist das? Wozu?

Wie funktioniert VPN und wozu?

- verschlüsselte Verbindung zu einem VPN-Server
- Verbindung vom VPN-Server ins offene Netz unverschlüsselt
- eigene IP-Adresse im „offenen" Netz nicht sichtbar

19

Unterwegs im Internet … aber sicher! 2.

VPN – Was ist das? Wozu?

+ Vorteile:

- Verschleierung der eigenen IP-Adresse im „offenen" Netz
- eigener Aufenthaltsorte nicht direkt feststellbar
- Zugriff auf regionale Inhalte (z.B. Netflix USA)
- sicherer Datenaustausch zu einem anderem User im gleichen VPN-Netz

- Nachteile:

- VPN-Anbieter kann Daten mitlesen -> Auswahl eines vertrauenswürdigen Anbieters erforderlich
- Anzahl VPN-Server begrenzt
- evtl. Verbindungsaufbau verlangsamt

20

Unterwegs im Internet … aber sicher! 2.

VPN – Was ist das? Wozu?

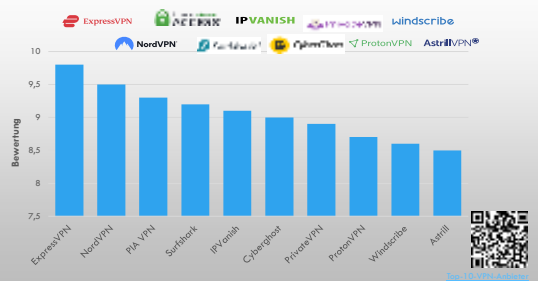
Nutzung einer VPN-Verbindung:

- sicherer Schutz in offenen unverschlüsselten WLAN-Netzen
- Bezahlung VPN-Server: u.U. mit eigenen Daten bzw. indirekt über Affiliate-Geschäft
- VPN zur Verschleierung der Identität ungeeignet
  besser: Nutzung TOR-Netzwerk mittels Tor-Browser
- Nutzung der VPN-Funktionalität des Routers (z.B. Fritzbox-VPN)

21

Unterwegs im Internet … aber sicher! 2.

VPN – Was ist das? Wozu?



22

Unterwegs im Internet … aber sicher!

Sicher surfen, smart schützen!

3. Passwörter – die Türöffner zu vielen Dingen

- Starke Passwörter – aber wie merken?
- Erhöhter Schutz durch Zwei-Faktor-Authentisierung – wozu?

23

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Regeln für sichere Passwörter: - Teil I

- mindestens 10 besser mehr Zeichen (>20)
- Nutzung von Zahlen, Sonderzeichen, großen und kleinen Buchstaben
- keine länderspezifischen Sonderzeichen (ä, ö, ü, ß)
- sensible Portale erfordern starke Passwörter
- Nutzung unterschiedlicher Passwörter je Portal
- Passwörter immer unter Verschluss halten
- keine Weitergabe von Passwörtern

Link: BSI Sichere Passwörter

24

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Regeln für sichere Passwörter: - Teil II

- Regelmäßige Änderung von Passwörtern, v.a. wenn Portal gehakt wurde
- Passwortgenerierung:
  - mittels Passwortgenerator
  - auf der Basis eines Akronyms (Passphrasen)
  - verschachtelte Wörter
- Nutzung Zwei-Faktor-Authentisierung (2FA)
- Nutzung PassKey
  (kryptografisches Verfahren ohne Passwort!)

Link: BSI Sichere Passwörter

25

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

NoGo´s:

- keine offensichtlichen Buchstaben- bzw. Zahlenreihen
  z.B.: „passwort“ / „1234567890“ / „qweretzuiop“ / „abcdefgh“ / „AaAaAa“
- keine Begriffe aus dem Wörterbuch
- keine Begriffe aus dem persönlichen Umfeld
  z.B. Familien- bzw. Freundesnamen, Haustiere, Arbeitgeber
- keine Weitergabe von Passwörtern bzw. PINs (TANs)
- kein offener Zugang zu Passwörtern
  (z.B. unter Schreibtischunterlage)
- sehr riskant: Nutzung eines Passwortes für viele Portale

26

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Praktische Informationen zu Passwörtern – Teil I:

- jedes Endgerät schützen (Bildschirmsperre mit Passwortschutz)
- Verwendung eines separaten Passwort-Managers (digital / analog)
- Passwörter im Web-Browser mit Masterpasswort schützen!
- Überprüfung eigener Passwörter:
  - *nicht* mit Internet-Tools (= Veröffentlichung eigener Passwörter)!
  - Nutzung eines Passwort-Managers bzgl. Passwort-Qualität

27

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Praktische Informationen zu Passwörtern – Teil II:

- Beispiel einer Passphrase:
  „Ohh, am liebsten esse ich Pizza mit vier Zutaten und viel Käse!“ :
  Passwort: „O,aleiPm4Z&vK!“ (gute Passwort-Qualität, Entropie: 69,47Bit)
- Kenntnisse über Methoden zum Passwort-Diebstahl:
  - Phishing (per E-Mail)
  - Keylogger (per Schadsoftware)
  - Sniffing (per Netzwerkanalyse)
  - Passwort aus Datenbank / Wörterbuch
  - Brute-Force-Attacke (durch Ausprobieren)

Überprüfung Ausspionierung eigener Identitätsdaten: Hasse-Plattner-Institut

28

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Digitaler Passwort-Manager:

+ Vorteile:
- Verwaltung von (allen) Passwörtern durch Verschlüsselung mittels Master-Passwort
- sehr gute Unterstützung bei Passwort-Vergabe: Anzeige Passwort-Stärke
- Synchronisation per Cloud für mehrere Endgeräte möglich
- Unterstützung bei Passwort-Eingabe im Browser mit Sicherheitsfunktionen

- Nachteile:
- Verlust Master-Passwort:
  > hoher Wiederherstellungsaufwand
- Diebstahl Master-Passwort:
  > Cyber-Angriff auf alle Portale möglich
- Vertrauen in den Cloud-Anbieter
  (Prüfen der AGBs und Datenschutzrechte)

29

Unterwegs im Internet … aber sicher! 3.

Starke Passwörter – aber wie merken?

Beispiele für Passwort-Manager:

1Password Enpass bitwarden DASHLANE AVIRA Keeper KeePassXC

Auswahlkriterien:
- Sicherheit
- Komfort und Produktivität
- Verfügbarkeit auf den gewünschten Systemen
- Funktionsumfang
- Sharing mit anderen Personen (nur bei dringendem Bedarf!)
- Kosten

Vergleich Passwort-Manager 2021/23: GIGA Chip Heise c't 05/2021

30

Unterwegs im Internet … aber sicher! 3.

Erhöhter Schutz durch Zwei-Faktor-Authentisierung – wozu?

Grundlagen I:

- Identitätsnachweis mittels einer Kombination aus 2 unterschiedlichen und unabhängigen Komponenten
- mögliche Faktoren:
  1. Wissen (z.B. Benutzername und Passwort)
  2. Besitz (z.B. Smartphone, Personalausweis)
  3. Inhärenz (Eigenschaft des Nutzers, z.B. Fingerabdruck)
- Wozu?: Erhöhung der Sicherheit v.a. bei sensiblen Daten (z.B. Banking, Zugriff Firmennetzwerk)

BSI-Information zu 2FA

31

Unterwegs im Internet … aber sicher! 3.

Erhöhter Schutz durch Zwei-Faktor-Authentisierung – wozu?

Grundlagen II:

- gängige Systeme zur Zwei-Faktor-Authentisierung:
  - Einmalkennwort (OTP): z.B. chipTAN, pushTAN, Authenticator App, smsTAN (unsicher auf gleichem Endgerät!) / veraltet: iTAN
  - kryptographische Token: Speicherung eines privaten Schlüssels / Zertifikats auf Endgerät oder in Hardware (Chipkarte / spezielle Sticks), z.B. Softwarezertifikat für ELSTER-Portal, HBCI, Personalausweis, FIDO-Stick
  - biometrische Systeme: Erfassung einzigartiger persönlicher körperlicher Merkmale (z.B. Fingerabdruck, Gesicht, Retina)

32

Unterwegs im Internet … aber sicher! 3.

Erhöhter Schutz durch Zwei-Faktor-Authentisierung – wozu?

2-Faktor-Authentisierung (2FA):

+ Vorteile / Empfehlungen:	- Nachteile:
○ bei Passwort-Diebstahl trotzdem kein Zugriff durch Cyber-Kriminelle	○ geringfügig verlängerte Anmeldevorgang
○ 2FA, wenn möglich, stets anwenden	○ Falls besitzbasierter Faktor nicht mehr verfügbar: kein oder eingeschränkter Portalzugang
○ Hinterlegung ***mehrerer*** „zweiter" Faktoren (z.B. bei Smartphone-Diebstahl)	

Zwei-Faktor-Authentisierung: BSI 2FA-Hinweise

33

Unterwegs im Internet … aber sicher!

Sicher surfen, smart schützen!

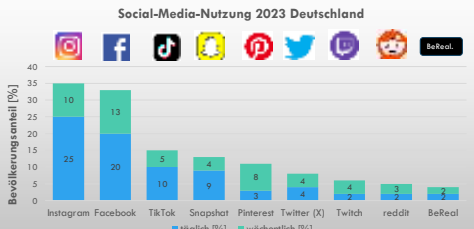
4. Unterwegs im digitalen Raum

- Umgang mit sozialen Netzwerken / Messengern
- Sicher im Internet bezahlen
- Betrug durch Phishing, Smishing bzw. Vishing
- Identitätsdiebstahl
- Opfer krimineller Aktivitäten? Was tun?

34

Unterwegs im Internet … aber sicher! 4.

Umgang mit sozialen Netzwerken – Social-Media

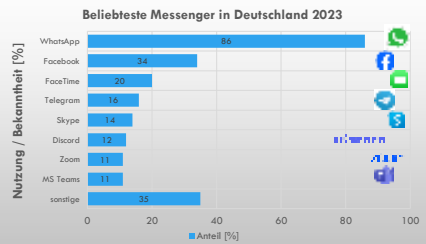


Quelle: ARD/ZDF-Onlinestudie 2023
Grundgesamtheit deutschsprachige Bevölkerung ab 14 Jahren: 70,67Mio., Stichprobe N=2000
Begriff: Social Media

35

Unterwegs im Internet … aber sicher! 4.

Umgang mit sozialen Netzwerken - Messengern



Quelle: Verbraucherzentrale "Beliebteste Messenger in Deutschland"
Doppelnutzung möglich!
Datenbasis: 2023: Abfragen: 4063, 18-64-Jährige
Begriff: Instant Messaging

36

Unterwegs im Internet … aber sicher! 4.

Umgang mit sozialen Netzwerken / Messengern

Empfehlungen Social-Media / Messenger **Teil I:**

- Privatsphären-Einstellungen prüfen und anpassen
- Nicht zu viel Informationen veröffentlichen:
  - Bilder und Stories zeitversetzt posten
  - Abwesenheit und aktuellen Aufenthaltsort **nicht** posten
  - **keine** Aussagen posten, die evtl. der Karriere schaden könnten
- **keine** vertraulichen Informationen preisgeben (u.a. Bilder, Arbeit / Arbeitgeber, Zugangsdaten)
- Bildverwertungsrechte werden i.A. stets abgetreten! (siehe AGB's)

37

Unterwegs im Internet … aber sicher! 4.

Umgang mit sozialen Netzwerken / Messengern

Empfehlungen Social-Media / Messenger **Teil II:**

- Anfragen nur von persönlich Bekannten zulassen
- Nachdenken bei zweifelhaften Anfragen!
- Cyber-Mobbing, Cyber-Stalker und kriminelle Machenschaften melden
- alte Accounts löschen: Das Internet vergisst nie!
- AGBs und Datenschutzbestimmungen lesen (u.a. Rechte an Bildmaterial)

38

Unterwegs im Internet … aber sicher! 4.

Sicher im Internet bezahlen!

1. Hinweise zu seriösen Online-Shops:

- gutes Web-Layout mit passenden AGBs sind ***kein*** ausreichendes Kriterium!
- Überprüfung des Impressums: **vollständige** Angabe der Kontaktdaten inklusive Adresse und Telefonnummer
- Lesen der Erfahrungsberichte von anderen Usern v.a. auch auf anderen Plattformen
- Online-Shop **nur mit Verschlüsselung** (https://) nutzen!

Weitere Informationen Finanztipp

39

Unterwegs im Internet … aber sicher! 4.

Sicher im Internet bezahlen!

2. Wie kann man im Internet bezahlen?

- Rechnung – am sichersten
- Nachnahme – erhöhte Kosten / unsicher
- Bankeinzug – Rückbuchung 8 Wochen lang möglich!
- Vorkasse – *überhaupt nicht* zu empfehlen!
- Ratenkauf – evtl. erhöhte Kosten
- Kreditkarte – weltweiter Einkauf ggf. mit Zusatzkosten / Rückbuchung möglich

Weitere Informationen Finanztipp

40

Unterwegs im Internet … aber sicher! 4.

Sicher im Internet bezahlen!

3. Bezahldienste über Drittanbieter:

- Paypal – Hinweis: ***niemals*** über „Freunde und Familie" bezahlen; *besser* „Geld senden für Waren und Dienstleistungen"
- Giropay (Einstellung Ende 2024!)
- Sofortüberweisung
- Klarna
- Amazon Pay
- Gutscheinkarten – keine Bankverbindung erforderlich
- Ratenkauf über Sezzle oder Afterpay

4. weitere Hinweise:

- regelmäßige Kontrolle der Abbuchungen
- ggf. Löschen des eigenen Shop-Zugangs
- ggf. Sperrung Kreditkarte

Weitere Informationen Finanztipp

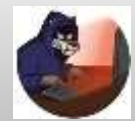
41

Unterwegs im Internet … aber sicher! 4.

Hackerangriffe – Was ist das? Wie geht das?

Was wollen Hacker erreichen? - Teil I

- Zugang zu Online-Bankkonten verschaffen und Geld entwenden
- Kontrolle über fremde Systeme erlangen (z.B. Computer, Server, Websites) und Lösegeld fordern
  - Systeme manipulieren / sperren, z.B. Kliniken
  - Websites ändern
  - Viren, Würmer und Trojaner installieren
  - Daten verschlüsseln (Ransomware)
  - Botnetz einrichten (Spyware, Keylogger)



42

Unterwegs im Internet … aber sicher! 4.

Hackerangriffe – Was ist das? Wie geht das?

Was wollen Hacker erreichen? - Teil II

- Geheimnisse von Firmen und Staaten ausspionieren
- Daten stehlen, z.B. Kontakte auf dem Smartphone
- Systeme lahmlegen durch Überlastung des Datennetzes (Distributed-Denial-of-Service-Attacken (DDoS))

43

Unterwegs im Internet … aber sicher! 4.

Hackerangriffe – Was ist das? Wie geht das?

Wie kommen Hacker an fremde Daten? – Teil I

- Angriff per Social-Engineering, z.B. Enkeltrick
- klassische Manipulationstricks per Phishing / Smishing bzw. Vishing durch gefälschte E-Mails, Websites, SMS, Anrufe
- Man-in-the-Middle-Attacke in offenen Hotspots
- Brute-Force-Attacke – Ausprobieren von Passwörtern

44

Unterwegs im Internet … aber sicher! 4.

Hackerangriffe – Was ist das? Wie geht das?

Wie kommen Hacker an fremde Daten? – Teil II

- Drive-by-Downloads – unbeabsichtigtes Laden von Schadsoftware z.B. von gefälschten Websites
- Ausführen von infizierter Software aus zweifelhafter Quelle
- Ausnutzen Systemschwachstellen
- Diebstahl eines Endgerätes

45

Unterwegs im Internet … aber sicher! 4.

Erkennung von Phishing, Smishing bzw. Vishing – Teil I

Mindestens eines der folgenden Merkmale erfüllt sehr wahrscheinlich eine **Phishing-E-Mail**:

- E-Mail-Text gibt dringenden Handlungsbedarf vor, z.B. Zugangssperre, Datenverlust
- Einsatz von Drohungen, z.B. „Falls Sie nicht …, müssen wir Ihr Konto sperren“
- Eingabeaufforderung von vertraulichen Daten, z.B. PINs für Online-Banking, Kreditkartennummer
- E-Mail enthält Links oder Formulare
- ungewöhnliches Anliegen eines vertrauten Absenders
- verdächtiger falscher Absender

BSI-Information zum Phishing

46

Unterwegs im Internet … aber sicher! 4.

Erkennung von Phishing, Smishing bzw. Vishing – Teil IIa

Handlungsempfehlungen bei **Phishing** (E-Mail):

- unbekannte bzw. unerwartete E-Mail:
  - Merkmal bzgl. Phishing-E-Mail ***zuerst*** prüfen
  - E-Mail-Absender ansehen
  - Mauszeiger über Links führen und Link-Anzeige prüfen
  - ***nicht*** antworten und ***nicht*** auf Links klicken!
  - Bei SPAM-Verdacht: E-Mail-Adresse als SPAM kennzeichnen!
- proaktive Aktionen:
  - sparsame Nutzung fremder Portale
  - ggf. Verwendung von Trash-E-Mail-Adresse

BSI-Information zum Phishing

47

Unterwegs im Internet … aber sicher! 4.

Erkennung von Phishing, Smishing bzw. Vishing – Teil IIb

Handlungsempfehlungen bei **Smishing** (SMS) :

- unbekannte oder unerwartete SMS:
  - nicht auf den darin enthaltenen Link klicken!
  - ggf. Kontaktaufnahme über anderes Kommunikationsmedium
- Telefonnummer
  - als Spam melden und
  - im Handy sperren!
- anschließend SMS löschen!

48

Unterwegs im Internet … aber sicher! 4.

Erkennung von Phishing, Smishing bzw. Vishing – Teil IIc

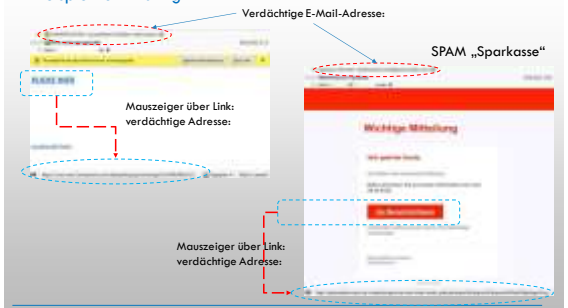
Handlungsempfehlungen bei *Vishing* (Telefon):

- unbekannte Nummer:
  - Anrufer verunsichern durch ungewohnte Meldung, z.B. „Bonjour“
  - *nicht* mit dem Namen melden!
- möglichst sofort auflegen!
- *keine* Informationen preisgeben!
- *keine* Verträge abschließen!
- Telefonnummer als Spam melden, sperren und danach löschen!

49

Unterwegs im Internet … aber sicher! 4.

Beispiel für Phishing



50

Unterwegs im Internet … aber sicher! 4.

Identitätsdiebstahl

Wie erfolgt ein Identitätsdiebstahl?

- Diebstahl / Entschlüsselung eines Passworts für E-Mail-Konto / Soziales Netzwerk / Messenger:
  - unsichere Passwörter
  - offener Zugang zu Passwörtern
    (z.B. unter Schreibtischunterlage, unverschlüsselte Speicherung)
  - Opfer einer Phishing- / Smishing- oder Vishing-Atacke
  - Befall mit Schadsoftware
  - Diebstahl ID-Card (z.B. Ausweis / EC-Karte)
  - Diebstahl eines Endgeräts

BSI-Information Identitätsdiebstahl, durch Datenfehler und Doxing

51

Unterwegs im Internet … aber sicher! 4.

Identitätsdiebstahl

Vorbeugender Schutz:

- Anwendung starker Passwörter je Portal
- sichere Erkennung, Separierung und Löschung von SPAM-E-Mails (Junk-~)
- stets aktueller Stand der Software
- Nutzung eines Viren-Scanners
- prinzipiell keine Weitergabe von persönlichen Informationen
- nur sichere Websites besuchen (https://)
- regelmäßige Kontrolle:
  - Kontobewegungen
  - Aktivitäten in sozialen Medien
  - E-Mail-Konto: u.a. den Ordner „gesendet“

52

Unterwegs im Internet … aber sicher! 4.

Opfer krimineller Aktivitäten? Was tun?

E-Mail-Postfach:

- sofortiger Viren-Scan der Endgeräte und ggf. Virenbeseitigung
- sofortige Änderung des Passwortes
- bei identischen Passwörtern auf anderen Portalen: auch diese sofort ändern und unterschiedliche Passwörter verwenden
- betroffene Kontakte informieren!
- keine Links bzw. Anhänge öffnen!
- ggf. Erstattung Anzeige bei der Online-Wache

53

Unterwegs im Internet … aber sicher! 4.

Opfer krimineller Aktivitäten? Was tun?

Soziale Medien / Messanger / Online-Shop:

- aktive Sitzung kontrollieren
- sofortiger Viren-Scan der Endgeräte und ggf. Virenbeseitigung
- Zugangsdaten sofort ändern und möglichst Zwei-Faktor-Authentifizierung anwenden
- bei gesperrtem Zugriff: neues Passwort anfordern über „*Passwort vergessen*“
- ggf. betroffene Kontakte informieren!
- ggf. an Betreiber wenden
- ggf. Anzeige bei der Online-Wache erstatten

54

Unterwegs im Internet … aber sicher! 4.

Opfer krimineller Aktivitäten? Was tun?

Missbrauch Online-Banking:

- sofortiger Viren-Scan der Endgeräte und ggf. Virenbeseitigung
- Zugangsdaten sofort ändern und möglichst Zwei-Faktor-Authentifizierung anwenden
- bei gesperrtem Zugriff: neues Passwort anfordern über *„Passwort vergessen"*
- kriminelle Transaktionen widerrufen
- Betreiber informieren
- ggf. sofort Konto sperren lassen – Sperr-Notruf: +49 116 116
- Erstattung Anzeige bei der Online-Wache

55

Unterwegs im Internet … aber sicher! 4.

Opfer krimineller Aktivitäten? Was tun?

Diebstahl Endgerät:

- Gerät möglichst schnell lokalisieren mittels Ortungsfunktion; siehe Gerätehersteller bzw. Serviceanbieter (z.B. Smartphone-Ortung)
- ggf. Sperrung SIM-Karte über Mobilfunkanbieter
- Fernaktivitäten: Gerät klingeln lassen, sperren bzw. Daten löschen (z.B. Android Google)

56

Unterwegs im Internet … aber sicher! – 5.

Sicher surfen, smart schützen!

5. Sicherheit auf meinem Endgerät

- Wichtige Einstellungen auf dem Endgerät
- Welche Tools auf meinem Endgerät?

57

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Teil I

- Betriebssystem und alle wichtigen Tools stets **aktuell** halten
- regelmäßige Kontrolle **Systemspeicher**auslastung v.a. bei Smartphones mit kleinem Speicher; evtl. sind Updates nicht möglich!
- laden von Software nur aus **sicheren** Quellen
- Viren-Scan vor Software-Installation
- Nutzlose Apps löschen bzw. deaktivieren

58

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Teil II

- Anwendung einer Verschlüsselung bei Firmendaten oder wichtigen persönlichen Daten:
  (Achtung! Schlüssel nicht verlieren!)
  - auf dem Endgerät, z.B. mit Windows-10-Tool *Bitlocker*
  - beim Transfer per E-Mail oder Stick, z.B. mit tooleigener Verschlüsselung oder mit Tool 7-zip / VeraCrypt / Volksverschlüsselung / GnuPG
- Wiederfinden des Endgerätes vorbereiten und möglichst ausprobieren v.a. für Smartphones / Tablets

59

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Teil III

- Durchführung täglicher automatischer Backups mit Verschlüsselung ggf. mit Zusatztool auf dem PC
- Sicherheitseinstellungen prüfen und ggf. anpassen:
  - Anwendung sicherer Passwörter mit automatischer Aktivierung eines Sperrbildschirms
  - Nutzung eines Passwort-Managers
  - jeder Benutzer mit separatem Account
  - Aktivierung Virenschutz am PC
  - regelmäßig vollständigen Viren-Scan
- stets datensparende Einstellungen vornehmen:
  (Daten = eine Internet-Währung!)
  - Telemetrie / Berechtigungen / Spracherkennung / Werbe-ID / Feedback

60

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Sicherheit

Windows 10:

Einstellungen -> Update & Sicherheit -> Windows-Sicherheit

Beispiel Windows 10-Sicherheit

Literatur: Heise-Heft „Sicher im Netz"

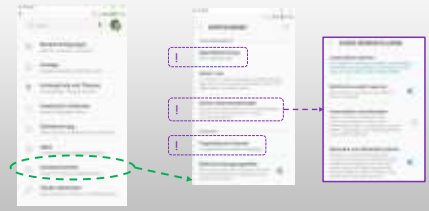
61

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Sicherheit

Android - Teil I:

Einstellungen -> Gerätesicherheit



Beispiel Android

Literatur: Heise-Heft „Sicher im Netz"

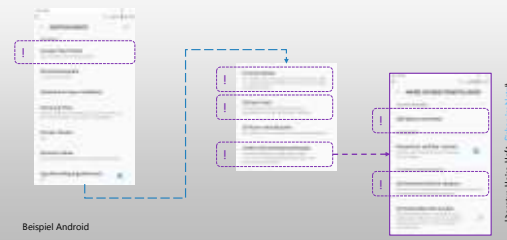
62

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Sicherheit

Android – Teil II:

Einstellungen -> Gerätesicherheit



Beispiel Android

Literatur: Heise-Heft „Sicher im Netz"

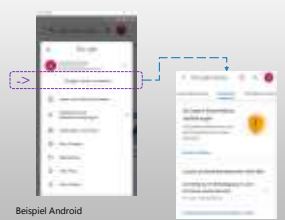
63

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Sicherheit

Android – Teil III:

Einstellungen -> Gerätesicherheit



Beispiel Android

- umfangreiche Einstellmöglichkeiten!
- Prüfung bzgl. unbedingt erforderlicher Funktionen

Literatur: Heise-Heft „Sicher im Netz"

64

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Datenschutz

Windows 10:

Einstellungen -> Datenschutz

Beispiel Windows 10-Sicherheit - Datensparsamkeit

Literatur: Heise-Heft „Sicher im Netz"

65

Unterwegs im Internet … aber sicher! 5.

Wichtige Einstellungen auf meinem Endgerät – Beispiele Datenschutz

Android – Teil II - Google-Konto:

Einstellungen -> Google

- umfangreiche Einstellmöglichkeiten!
- Prüfung bzgl. unbedingt erforderlicher Funktionen

Literatur: Heise-Heft „Sicher im Netz"

66

Unterwegs im Internet … aber sicher! 5.

Welche Tools auf meinem Endgerät? Teil I

Grundlegende Gedanken – I :

- Reduktion der App-Tracking-Informationen an den Hersteller:
  - > Verwendung eines anderen Web-Browser, z.B. Firefox, o.Ä. als Standardbrowser
  - > App unbedingt erforderlich? Bei gleicher Funktionalität Web-Browser benutzen!
  - > Verwendung weiterer anderer nicht vom Hersteller vorgegebener Tools, z.B. E-Mail- / Kalender-App
  - > Löschung / Deaktivierung nicht benötigter Apps

67

Unterwegs im Internet … aber sicher! 5.

Welche Tools auf meinem Endgerät? Teil I

Grundlegende Gedanken – II:

- bevorzugte Nutzung von bekannten und als gut bewerteten Apps
- erleichterte/r Bedienung / Austausch durch gleiche Tools auf mehreren Endgeräten, z.B. Firefox

68

Unterwegs im Internet … aber sicher! 5.

Welche Tools auf meinem Endgerät? Teil II

Windows 10 / 11 – Vorschläge für die private Nutzung:

Nr.	Bezeichnung	Tools	Bemerkungen
1	Viren-Scanner	AVAST, Avira Antivirus, (Microsoft-Defender)	- Achtung! BSI-Warnung: Kaspersky-Scanner nicht verwenden! - siehe Vergleich 06/2024
2	Web-Browser	Firefox, o.Ä., Tor-Browser	- Austausch von Lesezeichen, Chronik usw. möglich
3	Such-Maschine	DuckDuckGo, Metager, Google, Google Scholar	Suchmaschinen im Web-Browser
4	Datenträger-Verschlüsselung	Microsoft Bitlocker, Veracrypt	- kostenlose Tools - Vergleich Datenverschlüsselung 2024
5	Office	MS-Office, Open-Office / Libre-Office	- Open-Source: Open- / Libre-Office
6	Cloud	MagentaCloud, HiDrive, OneDrive, iCloud, Dropbox	Achtung! Bei nicht europäischen Anbietern! Heise-Artikel „Die besten Cloudspeicher 06/2024“

69

Unterwegs im Internet … aber sicher! 5.

Welche Tools auf meinem Endgerät? Teil II

Windows 10 / 11 – Vorschläge für die private Nutzung:

Nr.	Bezeichnung	Tools	Bemerkungen
7	Passwort-Manager	KeePassXC	- Open-Source - verschlüsselte Datenbankspeicherung auch in der Cloud
8	Backup-Tool	Duplicati	- Open-Source - verschlüsselte Daten-Backup auch in der Cloud
9	PDF-Tools	PDF24, Foxit-Pdf-Reader, Adobe-Reader	- PDF24: umfangreiche PDF-Verarbeitung (Edit, OCR, u.v.m.)
10	Bild-bearbeitung	GIMP, Paint, Foto	- GIMP: Open-Source, umfangreiche Bildbearbeitung - Windows-Tools
11	Zip-Programm	7-zip	- Open-Source - Datenkomprimierung und ggf. Verschlüsselung
12	Bild-Betrachter	Windows-Fotos, Irfan-Viewer	- kostenlose Bild-Betrachter - Irfan-Viewer: v.a. Batch-Bildverarbeitung
13	E-Mail-Client	Thunderbird	- Open-Source - umfangreiche Verwaltung von E-Mail-Konten

70

Unterwegs im Internet … aber sicher! 5.

Welche Tools auf meinem Endgerät? Teil III

Windows 10 / 11 – Vorschläge für die private Nutzung:

Nr.	Bezeichnung	Tools	Bemerkungen
14	Text-Editor	Windows: Editor, WordPad, Notepad ++	- Notepad: Open-Source-Texteditor mit umfangreichen Funktionen (u.a. Syntax-Highlighting, Makros, Vergleich)
15	Video-/Audio-Bearbeitung	VLC-Media-Player, Windows: Movie-Maker, Media-Player, Clipchamp	- VLC: einfache Formatkonvertierung - Movie-Maker: einfache Filmbearbeitung
16	Dateimanager	FreeCommander, Win-Dateimanager	- FreeComm.: Freeware mit sehr guter Suchfunktion
17	Übersetzung	DeepL, Google-Übersetzer	- DeepL: sehr gutes Übersetzungstool - Google: auch als Add-Ons für Website-Übersetzung
18	Bildverwaltung	Microsoft Foto, Google Photos	- Auswahl nach eigenen Präferenzen
19	KI-Tools	ChatGPT, MS Copilot, Perplexity, Google Gemini, MS Designer, DALL*E2, DeepL Write	- KI-Tools (Recherche, Ideensammlung) - KI-Bildtools - DeepL Write: besseren Text schreiben
20	Bild-Detektiv	Reverse Image Search	- detektivische Bildsuche im Web

71

Unterwegs im Internet … aber sicher! – 6.

Sicher surfen, smart schützen!

6. Zusammenfassung

72

Unterwegs im Internet … aber sicher! 6.

Zusammenfassung Teil I

- sinnvolle Einstellungen am Betriebssystem des Endgerätes bzgl. Virenschutz, Sicherheit, Tracking und Datenschutz vornehmen
- regelmäßige Aktualisierung des Betriebssystems und der Apps
- Anwendung sicherer Passwörter **je** Endgerät **und** Portal
- Nutzung Passwort-Manager (digital / analog)
- **starkes** Passwort für die E-Mail-Adresse
- Nutzung eines geeigneten Web-Browsers mit zusätzlichen Sicherheitseinstellungen und passender Suchmaschine
- regelmäßiges Löschen des Browser-Verlaufs und dessen Cache
- Installation sinnvoller Apps **nur** aus **sicheren** Datenquellen
- regelmäßiges der Daten

73

Unterwegs im Internet … aber sicher! 6.

Zusammenfassung Teil II

- Nutzung nur **sicherer** Internetseiten: https://
- Reduzierung der Nutzung von WLAN-Hotspots
- Übermittlung sensibler Daten nur über sichere Verbindung **und** verschlüsselt
- gesundes Misstrauen und zusätzliche Überprüfung:
  - bei auffälligem Verhalten des Endgerätes
  - bei unerwarteter Kontaktaufnahme (Phishing, Smishing, Vishing)
  - bei Weiterleitung auf Fake-Websites
- Nutzung Social-Media / Messenger mit **datensparsamen** Einstellungen sowie mit Augenmaß
- Opfer krimineller Aktivitäten: **sofort** handeln!

74

Unterwegs im Internet … aber sicher! – 7.

Sicher surfen, smart schützen!

7. Daten und Fakten zum Nachlesen

- Basisinformationen des BSI
- Interessante Links und Literatur
- Begriffe

75

Unterwegs im Internet … aber sicher! 7.

Basisinformationen des BSI

BSI-Homepage

BSI-Cyber-Sicherheitsmonitor

BSI-Digitaler Verbraucherschutz

Digitale ERST-Helfer – Broschüre

BSI-Newsletter

BSI-Angebote für Verbraucher*innen: #einfachaBSIchern!

BSI: Bundesamt für Sicherheit in der Informationsverarbeitung

76

Unterwegs im Internet … aber sicher! 7.

Interessante Links:

Bin ich fit in Sachen Sicherheit im Internet?

Schulung, Tipps und Quiz:

- kleiner Selbsttest zu wichtigen Sicherheitsfragen: Quiz der Studenten Herr Engler und Herr Kraft der Hochschule Reutlingen, Fakultät Informatik
- Selbsttest Behörden-IT-Sicherheitstraining (BITS) (gutes Schulungsprogramm mit mehreren Quiz nicht nur für Behördenmitarbeiter)
- Deutschland sicher im Netz (DsiN)
- Die Cyberfibel von DsiN / BMI

77

Unterwegs im Internet … aber sicher! 7.

Interessante Links und Literatur:

Internet-ABC für Kinder, Lehrkräfte und Eltern:
https://www.internet-abc.de/
Sehr viele und kindgerecht aufbereitete Informationen!

Hier geht's zum Internet-Surfschein für Kinder bei Internet-ABC:
https://www.internet-abc.de/kinder/surfschein/

Weitere Informationen:

- https://www.netzdurchblick.de/
- Heise-Heft „Sicher ins Netz - 2022"
- Heise-Artikel c't 24/2022: „So wird Windows angegriffen"
- empfehlenswerte c't-Security-Checklisten ct.de/check2025 (frei verfügbar!)

78

Unterwegs im Internet … aber sicher! 7.

Begriffe / Abkürzungen

Begriff / Abkürzung	Erklärung
Brute-Force-Attacke	Angriff zum Ausspähen von Passwörtern durch wiederholtes Ausprobieren
DDoS	**D**istributed-**D**enial-**o**f-**S**ervice: Überlastung eines Datennetzes durch viele Datenabfragen
DNS	**D**omain **N**ame **S**erver: Server für die Namensauflösung von Web-Sites, z.B. www.heise.de -> IPv4: 193.99.144.85
http:// und https://	http: **H**yper-**T**ext-**T**ransfer-**P**rotokoll / https: …. **S**ecure: sicheres Hypertext-Übertragungsprotokoll im Internet
IP-Adresse	Adresse im Internet basierend auf dem Internet-Protokoll
ISP	Internet Service Provider: Internetdienstleister
Keylogger	„Tasten-Protokollierer": Erfassung aller Eingaben über die Tastatur
Man-in-the-Middel-Angriff = Snarfing	Angriffsform im Internet; Angreifer steht logisch zwischen User und dem Internetprovider (v.a. im offenen WLAN-Netzen (Hotspots)
Phishing, Smishing, Vishing	„Abfischen" von Daten über E-Mails, Web-Sites, SMS bzw. per Telefon
Proxy-Server	Kommunikationsschnittstelle in einem Netzwerk aus Rechnern in Form eines physischen Computers
Sniffing	Software zur Analyse des Datenverkehrs in einem Netzwerk
URL	**U**niform **R**esource **L**ocator: einheitlicher Ressourcenzeiger: Zeiger auf den Ort einer Ressource im Netzwerk, z.B. Website
VPN	**V**irtual **P**rivate **N**etwork: ins sich geschlossenes privates Kommunikationsnetz
WLAN	**W**ireless **L**ocal **A**rea **N**etwork: drahtloses lokales Netzwerk

79

Unterwegs im Internet … aber sicher!

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Fragen sind gern willkommen!

80

Unterwegs im Internet … aber sicher! – 8.

Sicher surfen, smart schützen!

8. Anhang: Web-Browser - Hinweise zur Nutzung sowie zu wichtigen Einstellungen

- Allgemeine Nutzungshinweise
- Auswahl Suchmaschine
- Browser-Datenschutz / Berechtigungen / Sicherheit
- Zusatztools – Add-Ons / Erweiterungen

Google Chrome
Mozilla Firefox
Opera
Microsoft Edge
Apple Safari
Tor Browser

81

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Nutzungshinweise / Einstellungen

Allgemeine Nutzungshinweise - Empfehlungen

Google Chrome
Mozilla Firefox
Opera
Microsoft Edge
Apple Safari
Tor Browser

Installationen / erste Einstellungen:
- Nutzung des gleichen Standard-Web-Browsers auf allen Endgeräten (Vereinfachung der Bedienung und des Datenaustausches)
- Auswahl und Aktivierung der gewünschten Suchmaschine(n)
- Anpassung der Sicherheitseinstellungen (Datenschutz / Cookies / Pop-up's / Passwörter / HTTPS-Mode)
- Installation sinnvoller Zusatz-Tools (Erweiterungen / Add-Ons)
- Aktivierung der automatischen Installation von Updates

Anwendung:
- Nutzung „Private Mode" sinnvoll (i.A. mit standardmäßig verschärften Sicherheitseinstellungen)

82

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Allgemeine Einstellungen**

- Standard-Web-Browser festlegen:
  - Windows: suche nach „Standard-Apps" > Webbrowser oder
  - Firefox: Einstellungen > Allgemein … Start
  - Edge: Einstellungen > Standardbrowser
- Download-Verzeichnis definieren:
  - Firefox: Einstellungen > Allgemein … „Dateien und Anwendungen" … Downloads
  - Edge: Einstellungen > Downloads
- Automatische Updates aktivieren:
  - Firefox: Einstellungen > Allgemein … „Firefox-Updates"
  - Edge: Einstellungen > Infos zu Microsoft Edge (Auto-Updates i.A. bereits aktiv!)

Legende ab dieser Folie:
>: Übergang zu dem ausgewiesenen Menüpunkt
…: Unterpunkt innerhalb des Menüpunktes

Hinweis: Setup-Details nur für die beiden Web-Browser Mozilla Firefox und Microsoft Edge

83

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Allgemeine Einstellungen**

- Suchmaschine anpassen:
  - Firefox: Einstellungen > Suche … Standardsuchmaschine: Auswahl vornehmen; ggf. „Weitere Suchmaschinen hinzufügen" (z.B. DuckDuckGo)

  - Edge: Einstellungen > „Datenschutz, …" - Dienste … „Adressleiste und Suche" >

84

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen - Datenschutz

- Verbesserter Schutz vor Aktivitätenverfolgung und „Do not track“-Sendung:
  - Firefox: Einstellungen > „Datenschutz, …“ … „Browser-Datenschutz“: Standard (1) für flüssiges Arbeiten und „Do not track“-Meldung einschalten (2)

85

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen - Datenschutz

- Verbesserter Schutz vor Aktivitätenverfolgung und „Do not track“-Sendung:
  - Edge: Einstellungen > „Datenschutz, …“ … „Verhindern der Nachverfolgung“: Ausgewogen (1) für flüssiges Arbeiten und „Do not track“-Meldung einschalten (2)

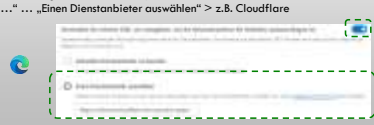
86

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen – sichere DNS-Anfragen

- Aktivierung DNS-Anfragen nur über HTTPS (verschlüsselte Anfragen an Domain Name System DNS v.a. wichtig bei Hotspot-Nutzung):
  - Firefox: Einstellungen > Allgemein … Verbindungs-Einstellungen … „DNS über HTTPS aktivieren“
  - Edge: Einstellungen > „Datenschutz, …“ … Sicherheit … „Verwenden Sie sicheres DNS, …“ … „Einen Dienstanbieter auswählen“ > z.B. Cloudflare



87

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen – Cookies / Passwörter

- Automatisches Löschen von Cookies und Website-Daten am Sitzungsende (1):
  - Firefox: Einstellungen > „Datenschutz, …“ … „Browserdaten löschen“: > „Aktion beim Schließen des Browsers“
- Passwort-Nutzung (2):
  - Firefox: Einstellungen > „Datenschutz, …“ … „Browserdaten löschen“: > „Aktion beim Schließen des Browsers“ … Kennwörter

Separate Passwort-Verwaltung mittels Passwort-Manager!

88

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen – Cookies / Passwörter

- Automatisches Löschen von Cookies und Website-Daten am Sitzungsende (1):
  - Edge: Einstellungen > „Datenschutz, …“ … „Browserdaten löschen“: > „Aktion beim Schließen des Browsers“
- Passwort-Nutzung (2):
  - Edge: Einstellungen > „Datenschutz, …“ … „Browserdaten löschen“: > „Aktion beim Schließen des Browsers“ … Kennwörter

Separate Passwort-Verwaltung mittels Passwort-Manager!

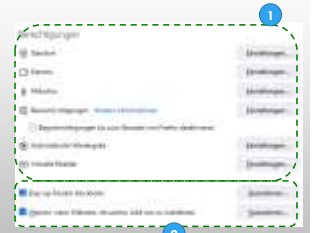
89

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – Sicherheitseinstellungen – Berechtigungen / Pop-Ups

- Sinnvolle Berechtigungen setzen (v.a. auf Smartphone) (1):
  - Firefox: Einstellungen > „Datenschutz, …“ … „Berechtigungen“: … „Standort / Kamera / …“
- Pop-Up-Fenster blockieren (2):
  - Firefox: Einstellungen > „Datenschutz, …“ … „ Berechtigungen“: … „Pop-Up-Fenster blockieren ….“



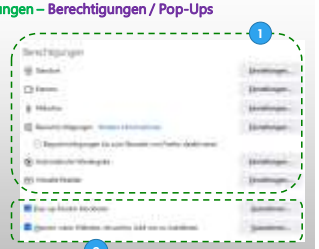
90

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Sicherheitseinstellungen – Berechtigungen / Pop-Ups**

- Sinnvolle Berechtigungen setzen (v.a. auf Smartphone) (1):
  - Firefox: Einstellungen > „Datenschutz, …" … „Berechtigungen": … „Standort / Kamera / …"
- Pop-Up-Fenster blockieren (2):
  - Firefox: Einstellungen > „Datenschutz, …" … „ Berechtigungen": … „Pop-Up-Fenster blockieren …."



91

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Zusatztools Add-Ons / Erweiterungen - Allgemeines**

Extrem hohe Anzahl an Add-Ons verfügbar!
Sinnvolle Erweiterungen installieren:

- Hinweise zur Nutzung von Erweiterungen:
  - Erfüllung der geforderten Funktionen
  - sehr guter Bewertung
  - sehr vielen Benutzern
  - Installation nur von geprüften und möglichst empfohlenen Add-Ons
  - möglichst keine parallele Nutzung gleichartiger Add-Ons
  - Nicht jedes Add-On ist für verschiedene Web-Browser verfügbar
- Basisempfehlungen:
  - Werbe-Blocker: AdBlocker Ultimate oder uBlock Origin
  - HTTPS erzwingen: HTTPS Everywhere oder
  - Allround-Privacy-Tool: DuckDuckGo Privacy Essentials
  - Optional: Website-Übersetzer: S3.Translator (vom Web-Browser unabhängiges sehr gutes Übersetzungsprogramm: DeepL)

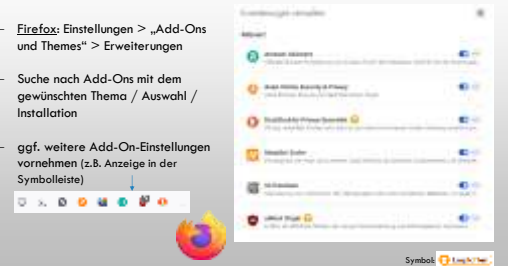
92

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Zusatztools Add-Ons / Erweiterungen - Einstellungen**

- Firefox: Einstellungen > „Add-Ons und Themes" > Erweiterungen
- Suche nach Add-Ons mit dem gewünschten Thema / Auswahl / Installation
- ggf. weitere Add-On-Einstellungen vornehmen (z.B. Anzeige in der Symbolleiste)



Symbol

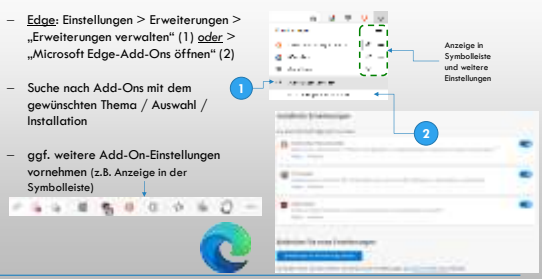
93

Unterwegs im Internet … aber sicher! 8.

Der Web-Browser – Pflege eines wichtigen Tools!

Web-Browser – **Zusatztools Add-Ons / Erweiterungen - Einstellungen**

- Edge: Einstellungen > Erweiterungen > „Erweiterungen verwalten" (1) oder > „Microsoft Edge-Add-Ons öffnen" (2)
- Suche nach Add-Ons mit dem gewünschten Thema / Auswahl / Installation
- ggf. weitere Add-On-Einstellungen vornehmen (z.B. Anzeige in der Symbolleiste)



94