

Computerkurse



Einfach den QR-Code scannen –
und schon hast du die ganze
Präsentation auf deinem Gerät 😊

Oder klicke auf den folgenden Link:

<https://drive.google.com/file/d/1cBW14PSpSrZBZv75jLqQGQrtZk9j3Y4/view>

Seminarleiter: Metin Bulut

Vorstellungsrunde

Zu meiner Person

- Metin Bulut
- 61 Jahre alt
- Studium der Betriebswirtschaftslehre – Marketing
- Seit 34 Jahren bei der Deutschen Telekom AG als Amtsrat tätig

Kurse: VHS Neukölln

- Wordpress für Anfänger
- Computerkurs für Anfänger*innen
- Der nächste Schritt: Computeraufbaukurs für Einsteiger*innen

Kurse: VHS Mitte

- Computerclub Erste Schritte am PC
- Internet nutzen und auf Sicherheit aktiv achten
- Computerclub Mails und Internet Grundkurs
- Was kann man mit dem Computer und im Internet machen?
- Projekt: AGiL - Alphabetisierung und Grundbildung in Lernhäusern der Berliner Volkshochschulen? „Ich kann es! Schritte in den Beruf“
- ERW-IN: Was kann man mit dem Computer und im Internet machen?
- Computerkurs für Geflüchtete



Vorstellungsrunde

- Diese Themen werden wir behandeln

Einstieg in das Arbeiten mit dem Computer

- Was kann man mit dem Computer und im Internet machen?
- Bestandteile des Computers
- Steuerung des Computers
- Windows-Desktop
 - Startknopf
 - Taskleiste
 - Explorer

Internet & Sicherheit

- Welche Gefahren gibt es?
- Wie verbreiten sich Viren?
- Wie kann man sich schützen?
- Tipps beim Surfen im Internet
- Sicherer Umgang beim Surfen im Internet
- Top 10 der Regeln für Internetsicherheit
- Zahlungsmöglichkeiten im Internet
- Seriöse Online-Shops

THEORIE

Vorstellungsrunde

- Diese Themen werden wir behandeln

Erste Schritte am Computer

Windows-Desktop

- Startknopf
- Taskleiste
- Explorer
- Suche
- Ordner und Unterordner anlegen
- Dateien kopieren/verschieben

Textverarbeitung mit MS Word

- Einführung in MS Word
- Textformatierung
- Arbeiten mit Listen
- Kopf- und Fußzeilen
- Tabellen erstellen
- Bilder und Formen einfügen
- Einfache Briefe und Dokumente
- Rechtschreib- und Grammatikprüfung
- Dokumentgestaltung
- Drucken und Exportieren

Mail

- Wie lege ich eine kostenlose und seriöse E-Mail-Adresse an?
- Wie schreibe ich eine E-Mail?
- Wie formatiere ich den Text der E-Mail?
- Wie füge ich Anhänge bei?
- Tipps & Tricks

PRAXIS

Vorstellungsrunde

Hauptthemen



MS Word



MS Excel



MS PowerPoint



E-Mail




Computer- und
Internetsicherheit



Dateimanager



Künstliche
Intelligenz

A photograph of a classroom. In the foreground, a wooden desk is cluttered with books, papers, and a blue pencil case. A black backpack and a patterned bag are on chairs. In the background, a large whiteboard with a wooden frame is mounted on the wall. The text 'Was kann man mit dem Computer und im Internet machen?' is written on the whiteboard in bold black font. To the left, a window with white curtains is visible.

Was kann man mit dem Computer und im Internet machen?

Was kann man mit dem Computer und im Internet machen? Seite 1

Computer und das Internet sind aus unserem Alltag kaum noch wegzudenken. Sie bieten uns eine Vielzahl von Möglichkeiten, unsere Zeit zu verbringen, zu lernen und zu arbeiten. Hier sind einige Beispiele für Dinge, die man mit einem Computer und im Internet machen kann:

- **Informationen suchen**

Das Internet ist eine riesige Wissensdatenbank. Mit nur wenigen Klicks können wir Informationen zu jedem Thema finden.

- **In Kontakt bleiben**

Wir können mit Freunden und Familie über E-Mail, soziale Netzwerke und Instant Messaging in Kontakt bleiben.

- **Unterhaltung**

Wir können Musik hören, Filme und Videos ansehen, spielen und lesen.

- **Arbeiten**

Wir können mit dem Computer und im Internet Texte schreiben, Präsentationen erstellen, Tabellenkalkulationen erstellen und vieles mehr.

Was kann man mit dem Computer und im Internet machen?, Seite 2

Computer und das Internet sind aus unserem Alltag kaum noch wegzudenken. Sie bieten uns eine Vielzahl von Möglichkeiten, unsere Zeit zu verbringen, zu lernen und zu arbeiten. Hier sind einige Beispiele für Dinge, die man mit einem Computer und im Internet machen kann:

- **Lernen**

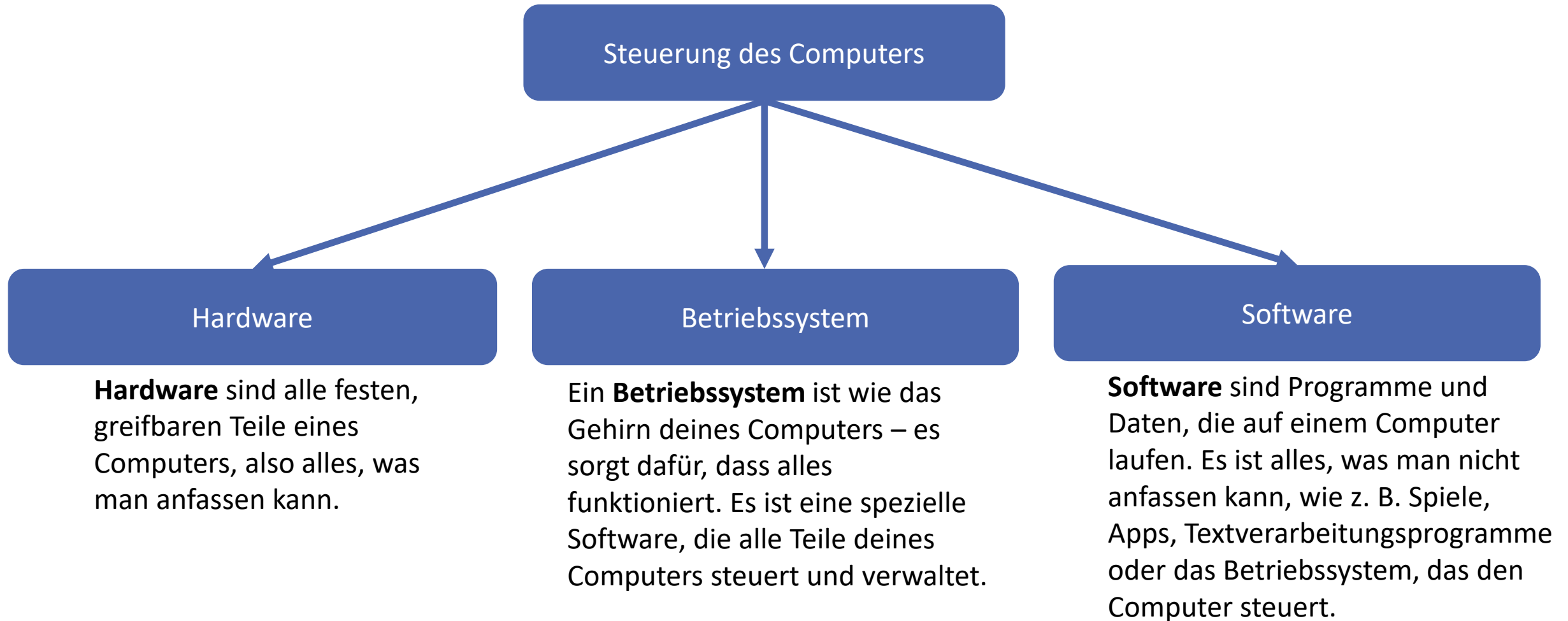
Wir können mit dem Computer und im Internet neue Sprachen lernen, an Kursen teilnehmen, Bücher lesen und vieles mehr. Die Möglichkeiten, die uns Computer und das Internet bieten, sind vielfältig. Es liegt an uns, zu entscheiden, wie wir sie nutzen wollen.

Hier sind einige zusätzliche Tipps für die Nutzung von Computern und dem Internet

- Seid kritisch gegenüber den Informationen, die Ihr im Internet findet. Nicht alles, was Ihr online liest, ist wahr.
- Schütze Deine Ihre Privatsphäre. Sei vorsichtig, welche persönlichen Informationen Du im Internet preisgibst.
- Setze Dir Grenzen. Es ist wichtig, sich auch Zeit für andere Aktivitäten zu nehmen, als nur am Computer zu sitzen.
- Computer und das Internet sind ein wertvolles Werkzeug. Mit ihnen können wir unsere Zeit produktiv nutzen, lernen und Spaß haben. Es liegt an uns, sie verantwortungsbewusst zu nutzen.

Bestandteile des Computers

Bestandteile des Computers



Bestandteile des Computers

- Hardware -



Bestandteile des Computers

- Betriebssystem -



Windows

74,96 %*

Ein weit verbreitetes Betriebssystem für PCs, das benutzerfreundlich ist und viele Programme unterstützt.



Mac OS X

16,02 %*

Das Betriebssystem von Apple, bekannt für seine einfache Bedienung und nahtlose Integration mit anderen Apple-Geräten.



Chrome OS

2,02 %*

Ein schnelles, cloudbasiertes Betriebssystem von Google, das hauptsächlich für Chromebooks entwickelt wurde.



Linux

2,18 %*

Ein kostenloses und anpassbares Betriebssystem, das oft von Technik-Enthusiasten und Servern verwendet wird.

Bestandteile des Computers

- Software -

Programme (Apps)



Word



Outlook



Excel



Teams



PowerPoint



OneNote

Software sind **Programme**, mit denen man Computer betreibt. Dank Software passiert überhaupt etwas auf dem Computer. Die Software enthält Regeln und Befehle, damit der Computer weiß, was er tun soll.

Bestandteile des Computers

- Software -



Word

Mit Word kannst du Texte schreiben, gestalten und bearbeiten, z. B. für Briefe, Berichte oder Aufsätze.



Excel

Mit Excel kannst du Tabellen erstellen, Daten berechnen, analysieren und Diagramme erstellen, z. B. für Finanzen oder Planungen.

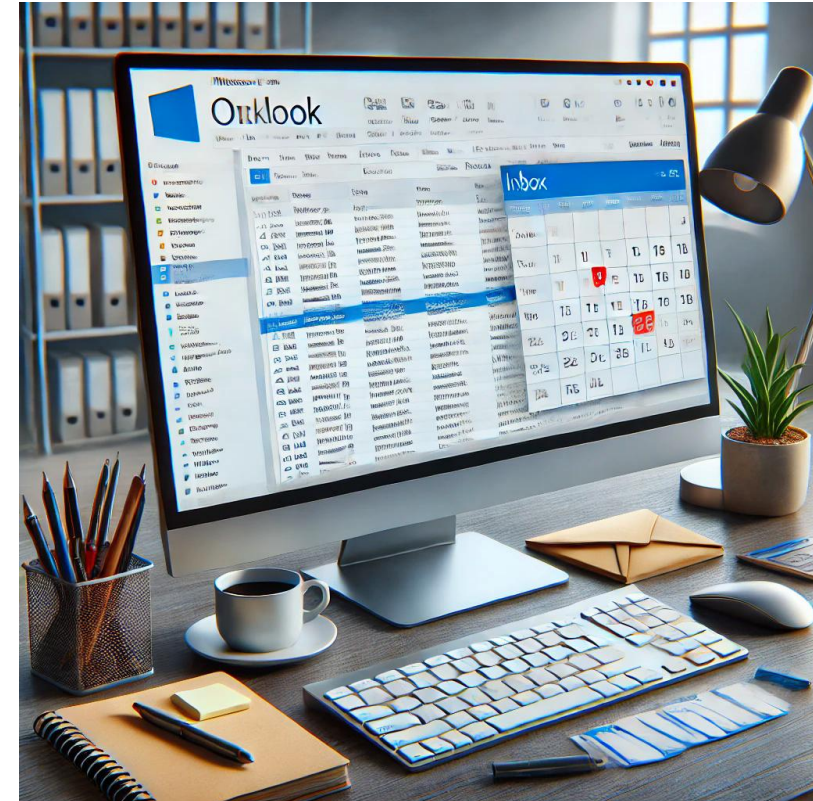
Bestandteile des Computers

- Software -



PowerPoint

Mit PowerPoint kannst du Präsentationen mit Text, Bildern und Animationen erstellen, z. B. für Vorträge oder Schulungen.



Outlook

Mit Outlook kannst du E-Mails schreiben, Termine planen und Kontakte verwalten.

Bestandteile des Computers

- Software -



Teams

ist eine Plattform, die Kommunikation und Zusammenarbeit erleichtert, indem sie Chats, Videokonferenzen, Dateiablage und gemeinsame Bearbeitung von Dokumenten an einem Ort bündelt.



OneNote

OneNote ermöglicht es, Notizen zu erstellen, sie mit Texten, Bildern, Checklisten oder Skizzen zu erweitern und alles übersichtlich an einem Ort zu organisieren und zu speichern.

A photograph of a classroom. In the foreground, a wooden desk is cluttered with several open books, a blue pencil case, and a black bag. A chair with a patterned bag is also visible. In the background, a large whiteboard with a wooden frame is mounted on the wall. The whiteboard contains the title text. To the left, a window with white curtains is partially visible.

Computertastatur und Computermaus

Computertastatur

Haupttasten

- **Buchstabentasten (A-Z):** Zum Eingeben von Text.
- **Umlaut-Tasten (Ä, Ö, Ü):** Für deutsche Sonderzeichen.
- **ß-Taste:** Für das Eszett, ein deutsches Sonderzeichen.

Zahlentasten

- **Oben (1-0):** Für Zahlen und Sonderzeichen wie !, @, €, etc.
- **Ziffernblock (rechts):** Zum schnellen Eingeben von Zahlen und Rechenoperationen.

Funktionstasten (F1 bis F12)

- **F1:** Öffnet oft die Hilfe eines Programms.
- **F2:** Zum Umbenennen von Dateien.
- **F5:** Aktualisiert eine Seite (z. B. im Browser).
- **F11:** Vollbildmodus in Browsern und Programmen.

Sondertasten

- **Enter:** Zum Bestätigen von Eingaben oder Ausführen von Befehlen.
- **Leertaste:** Fügt ein Leerzeichen ein.
- **Backspace:** Löscht Zeichen links vom Cursor.
- **Tabulator (Tab):** Zum Wechseln zwischen Feldern oder Einfügen eines Tabs.



Steuerungstasten

- **Shift:** Umschalten auf Großbuchstaben oder Sonderzeichen.
- **Strg (Ctrl):** Für Tastenkombinationen (z. B. Strg + C für Kopieren).
- **Alt und Alt Gr:** Alt Gr für Sonderzeichen wie @ oder €.

Windows-Taste: Zum Öffnen des Startmenüs.

Navigations- und Steuerungstasten:

- **Pfeiltasten:** Zum Navigieren innerhalb von Texten oder Menüs.
- **Entf (Delete):** Löscht Zeichen rechts vom Cursor.
- **Pos1 und Ende:** Zum Springen an den Anfang oder das Ende eines Dokuments.
- **Bild↑ und Bild↓:** Zum Scrollen in Dokumenten.

Computertastatur

Bricht Vorgänge ab / schließt Menüs.

Tab: Springt zum nächsten Eingabefeld / Einzug

Backspace: Löscht Zeichen links vom Cursor

Führt Befehle aus / Absatzwechsel

Einfügen (Insert): Wechselt zwischen Einfügen und Überschreiben

Pos1 (Home): Zum Zeilenanfang / Seitenanfang.

Ende (End): Zum Zeilenende / Seitenende.

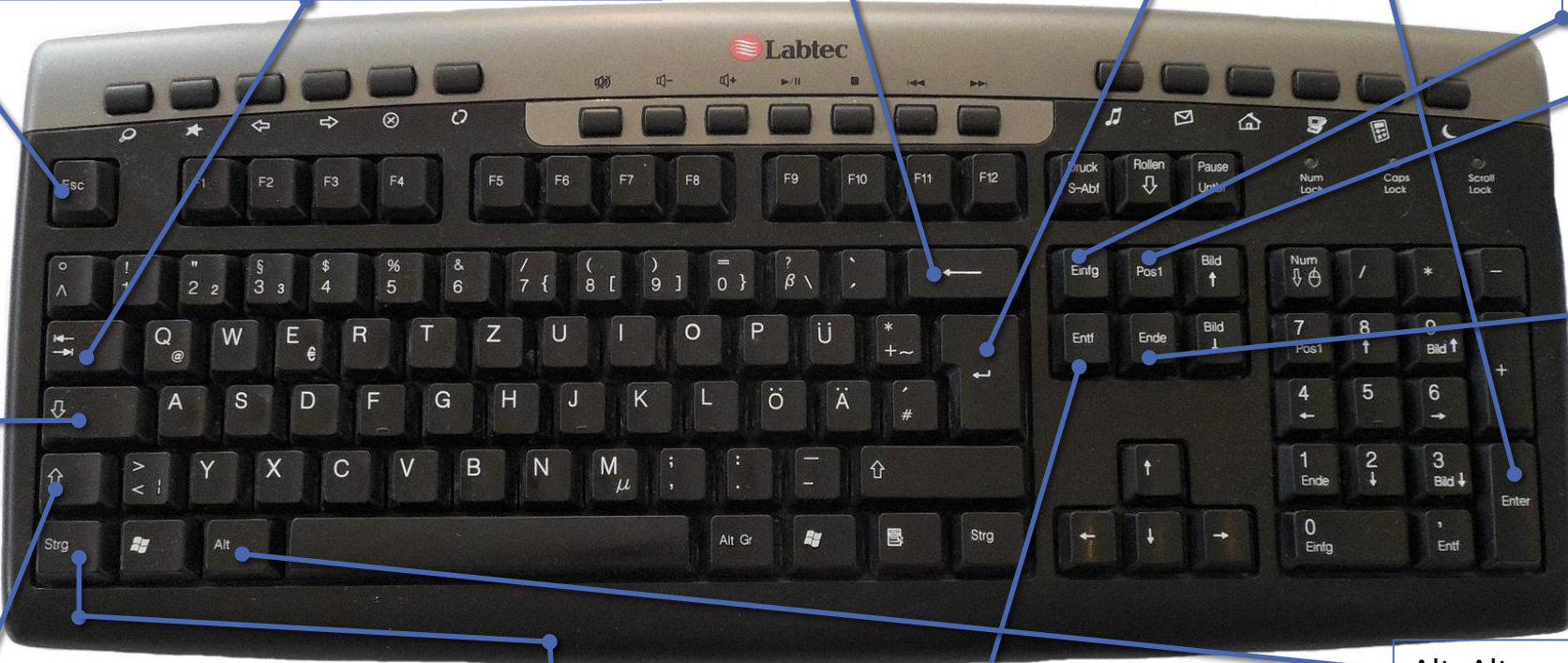
Alt: Alternative Steuerung / Menüzugriffe.

Entf (Delete): Löscht Zeichen rechts vom Cursor

Shift: Großschreibung / obere Zeichen

Strg (Ctrl): Für Tastenkombinationen (z. B. Strg+C zum Kopieren).

Caps Lock (Feststelltaste): Schaltet auf Dauergroßschreibung um



Computertastatur

- **Lupe:** Internetsuche
- **Stern (Favoriten/Lesezeichen):** öffnet die Favoritenliste im Browser
- **Pfeil nach links:** Zurück zur vorherigen Seite
- **Pfeil nach rechts:** Vorwärts (wenn du vorher zurückgegangen bist)
- **Kreuz (Stopp):** Bricht das Laden der aktuellen Webseite ab
- **Kreis mit Pfeil (Aktualisieren/Neu laden)** → Lädt die aktuelle Seite neu



Multimedia-Steuerung

Lautsprecher mit Kreuz (Mute)

1. Schaltet den Ton sofort stumm.
 2. Nochmal drücken → Ton wieder aktiv.
1. Lautsprecher mit „-“ (Volume Down)
1. Macht die Lautstärke leiser.
2. Lautsprecher mit „+“ (Volume Up)
1. Macht die Lautstärke lauter.
3. (Doppelpfeil nach links)
1. Springt zum vorherigen Titel oder Anfang des aktuellen Stücks.
4. (Play/Pause-Symbol)
1. Startet die Wiedergabe oder pausiert sie.
5. (Stopp-Symbol – Quadrat)
1. Stoppt die Wiedergabe komplett.
 2. Beim erneuten Start spielt er von Anfang.
6. (Doppelpfeil nach rechts)
1. Springt zum nächsten Titel.

Computertastatur



1. 🎵 Musiknote

1. Öffnet den **Standard-Musikplayer** auf deinem PC (z. B. Windows Media Player, iTunes, Spotify – je nachdem, was als Standard eingestellt ist).

2. ✉ Briefumschlag

1. Startet dein **Standard-E-Mail-Programm** (z. B. Outlook, Thunderbird oder die Mail-App in Windows 10/11).

3. 🏠 Haus (Home)

1. Öffnet deinen **Standard-Webbrowser** und lädt die **Startseite**.

4. 🔍 Lupe (rechts oben, nicht die links)

1. Öffnet die **Windows-Suche**
→ Dateien, Programme und Einstellungen finden.
In neueren Windows-Versionen auch Cortana oder die Startmenü-Suche.

5. 📁 Ordner

1. Öffnet den **Windows-Explorer** (Dateimanager), sodass du direkt auf deine Ordner und Dateien zugreifen kannst.

6. ☾ Mond (Standby / Sleep)

1. Versetzt den PC in den **Energiesparmodus** oder **Ruhezustand**.
2. Dadurch wird der Computer nicht ausgeschaltet, sondern pausiert, und du kannst ihn schnell wieder aufwecken.

Laptoptastatur [1]



Laptoptastatur [2]



Taste	Bedeutung / Funktion		
Esc	Bricht eine laufende Aktion ab oder schließt ein Menü/Fenster.	F9	Tastaturbeleuchtung ein-/ausschalten.
F1	Öffnet in den meisten Programmen die Hilfe.	F10 (Einfg)	Einfügen-Funktion („Insert“) – Umschalten zwischen Einfügen und Überschreiben beim Tippen.
F2	Schaltet oft zwischen externem Monitor und Laptop-Display um (Bildschirm umschalten).	F11	Flugmodus (alle Funkverbindungen – WLAN, Bluetooth – ausschalten).
F3	Helligkeit verringern (Display dunkler).	F12	Symbol mit zwei Rauten = Bildschirm duplizieren / erweitern (Display-Modus wechseln, ähnlich wie Windows-Taste + P).
F4	Helligkeit erhöhen (Display heller).	Druck	Macht einen Screenshot (Bildschirmfoto).
F5	Lautsprecher stumm schalten / Ton aus.	Ein/Aus-Taste (Power)	Computer ein-/ausschalten oder in den Energiesparmodus versetzen.
F6	Lautstärke verringern.	Entf (Delete)	Löscht markierte Elemente oder Zeichen rechts vom Cursor.
F7	Lautstärke erhöhen.	Pos1 (Home)	Springt an den Anfang einer Zeile oder Seite.
F8	Mikrofon stumm schalten / aktivieren.	Ende (End)	Springt ans Ende einer Zeile oder Seite.
		Bild ↑ (Page Up)	Eine Seite nach oben scrollen.
		Bild ↓ (Page Down)	Eine Seite nach unten scrollen.

Computermaus

Linke Maustaste

- **Klicken:** Um etwas auszuwählen, beispielsweise ein Programm oder eine Datei.
- **Doppelklicken:** Zum Öffnen von Dateien, Programmen oder Ordnern.
- **Ziehen und Ablegen (Drag & Drop):** Zum Verschieben oder Kopieren von Objekten, indem du die Taste gedrückt hältst und die Maus bewegst.
- **Markieren:** Zum Hervorheben von Texten oder Objekten, z. B. in einem Dokument



Rechte Maustaste

- **Kontextmenü öffnen:** Zeigt spezielle Optionen für das ausgewählte Objekt an, z. B. Kopieren, Einfügen oder Eigenschaften anzeigen.
- **Schnelle Funktionen:** Je nach Programm oder Anwendung kannst du hier zusätzliche Werkzeuge oder Einstellungen aufrufen.

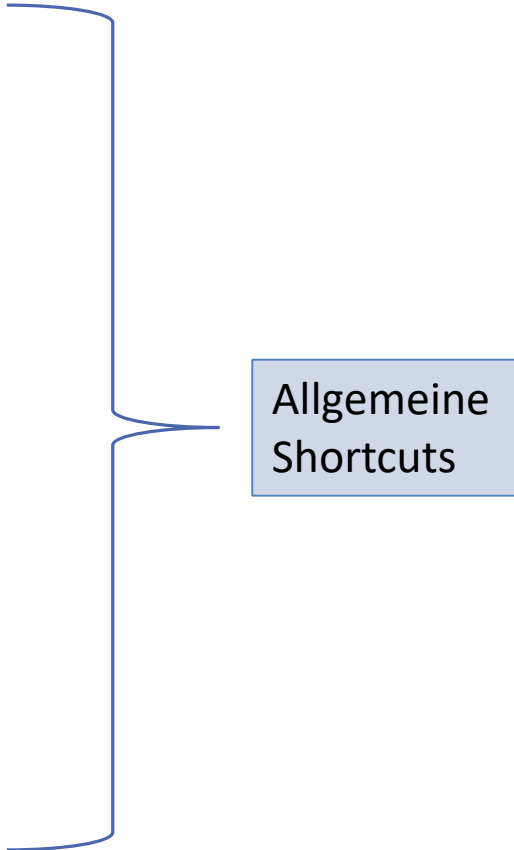
Mausrad

- **Scrollen:** Nach oben oder unten blättern, um z. B. durch Webseiten, Dokumente oder Listen zu navigieren.
- **Mittel-Taste (manchmal):** Das Mausrad kann bei manchen Mäusen auch als Taste gedrückt werden, um Funktionen wie das Öffnen eines Links in einem neuen Tab oder spezielle Scroll-Modi zu aktivieren.
- **Horizontales Scrollen (bei manchen Mäusen):** Einige Mäuse erlauben es, durch Kippen des Rads seitlich zu scrollen.

Wichtige Windows-Hotkeys

Eine Übersicht der wichtigsten Tastenkombinationen

Tastenkombination	Funktion
Strg + C	Kopieren
Strg + X	Ausschneiden
Strg + V	Einfügen
Strg + Z	Rückgängig machen
Strg + Y	Wiederholen
Strg + A	Alles markieren
Strg + S	Speichern
Alt + Tab	Zwischen offenen Fenstern wechseln
Alt + F4	Aktives Fenster schließen
Windows + D	Desktop anzeigen/verstecken
Windows + L	Computer sperren

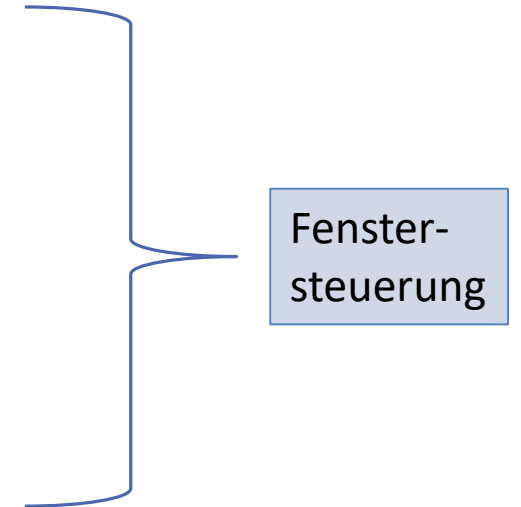


Allgemeine Shortcuts

Wichtige Windows-Hotkeys

Eine Übersicht der wichtigsten Tastenkombinationen

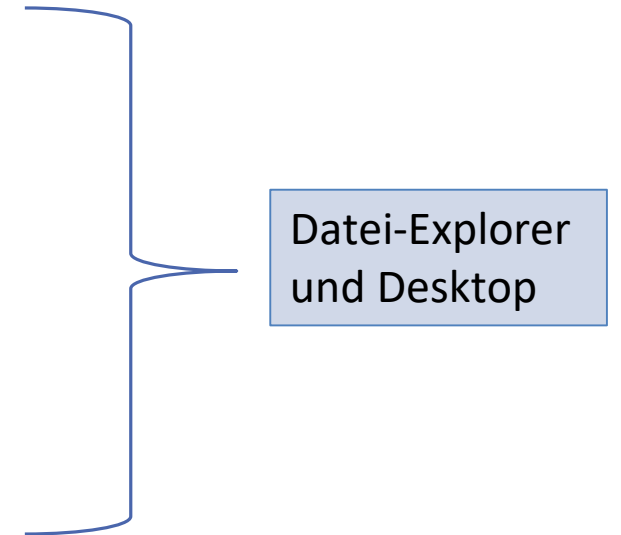
Tastenkombination	Funktion
Windows + Pfeil links/rechts	Fenster an Bildschirmseite andocken
Windows + Pfeil oben	Fenster maximieren
Windows + Pfeil unten	Fenster minimieren oder zurücksetzen
Windows + Tab	Task-Ansicht öffnen
Strg + Shift + Esc	Task-Manager öffnen



Wichtige Windows-Hotkeys

Eine Übersicht der wichtigsten Tastenkombinationen

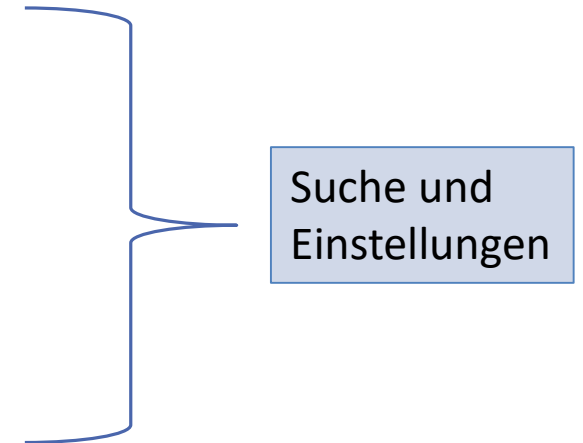
Tastenkombination	Funktion
Windows + E	Datei-Explorer öffnen
F2	Datei/Ordner umbenennen
F5	Aktualisieren
Alt + Enter	Eigenschaften anzeigen
Entf	Löschen
Shift + Entf	Endgültig löschen (ohne Papierkorb)



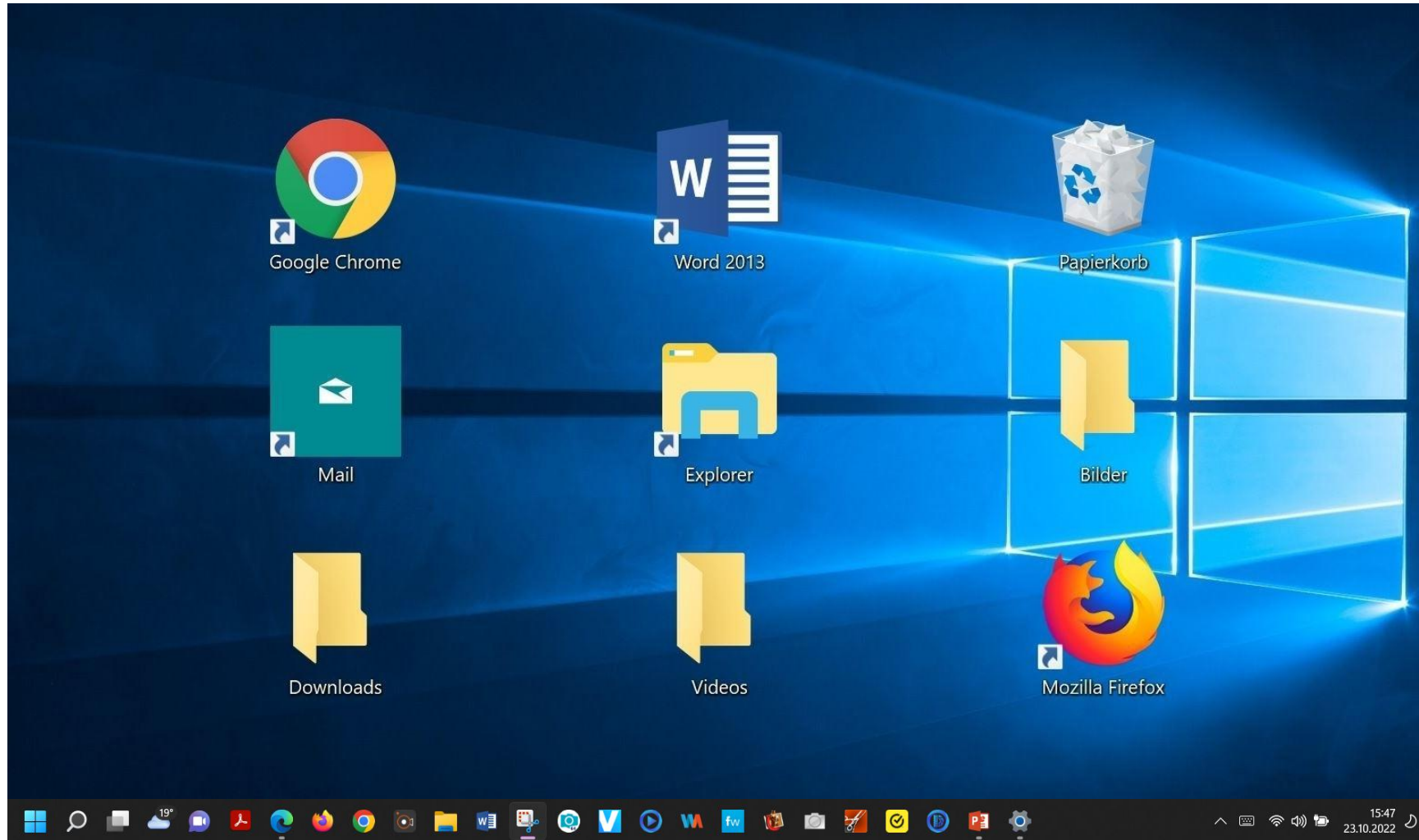
Wichtige Windows-Hotkeys

Eine Übersicht der wichtigsten Tastenkombinationen

Tastenkombination	Funktion
Windows + S	Suche öffnen
Windows + I	Einstellungen öffnen
Windows + R	Ausführen-Dialog öffnen
Windows + Pause	Systemeigenschaften anzeigen

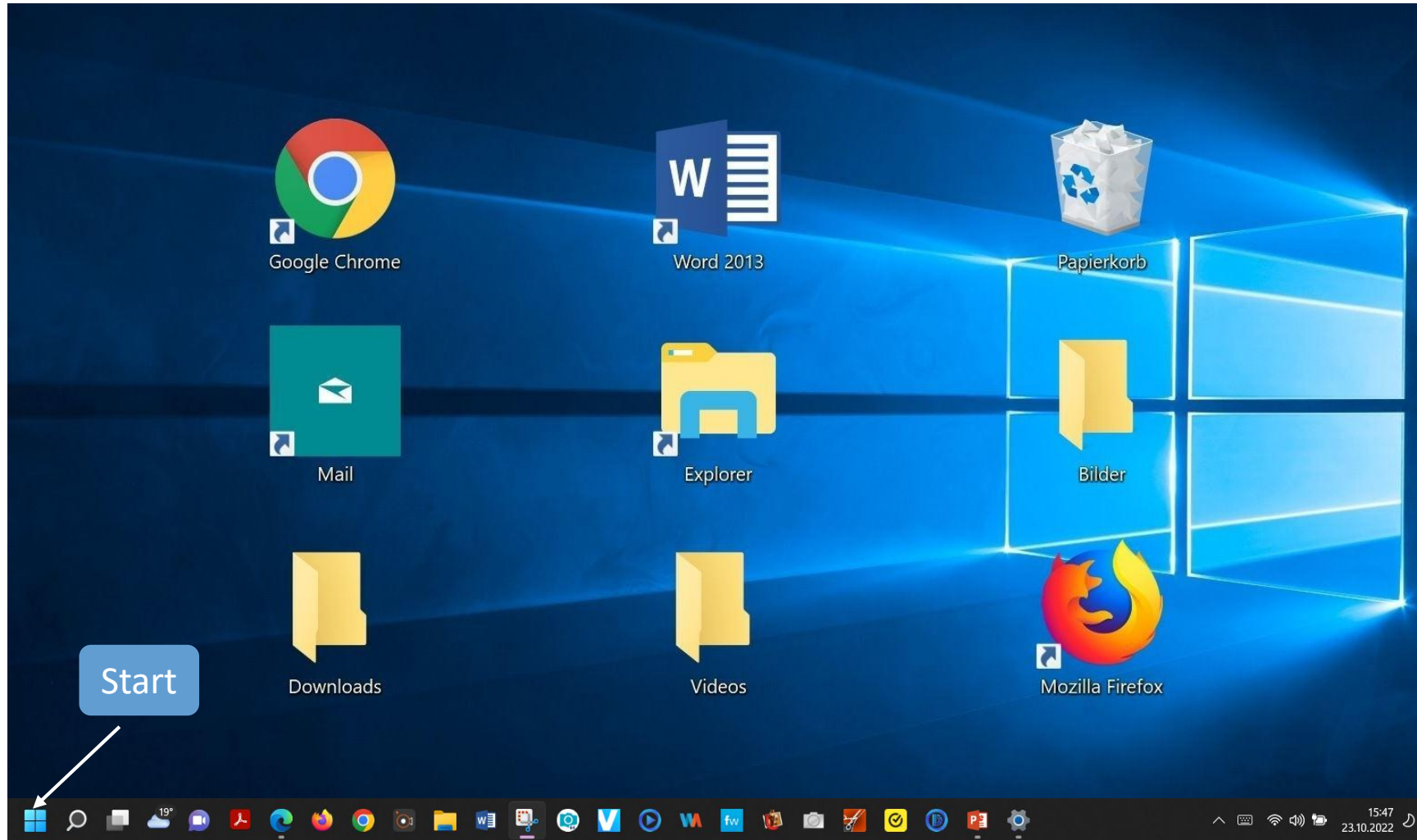


Arbeiten mit dem Computer: Der Desktop [1]



Der Desktop in Windows ist die Hauptoberfläche, die du siehst, sobald der Computer gestartet ist. Er wirkt wie ein virtueller Schreibtisch, auf dem du Programme und Dateien ablegen kannst, um schnell darauf zuzugreifen. Dabei kannst du Symbole anklicken, um Anwendungen zu öffnen oder Dateien zu organisieren.

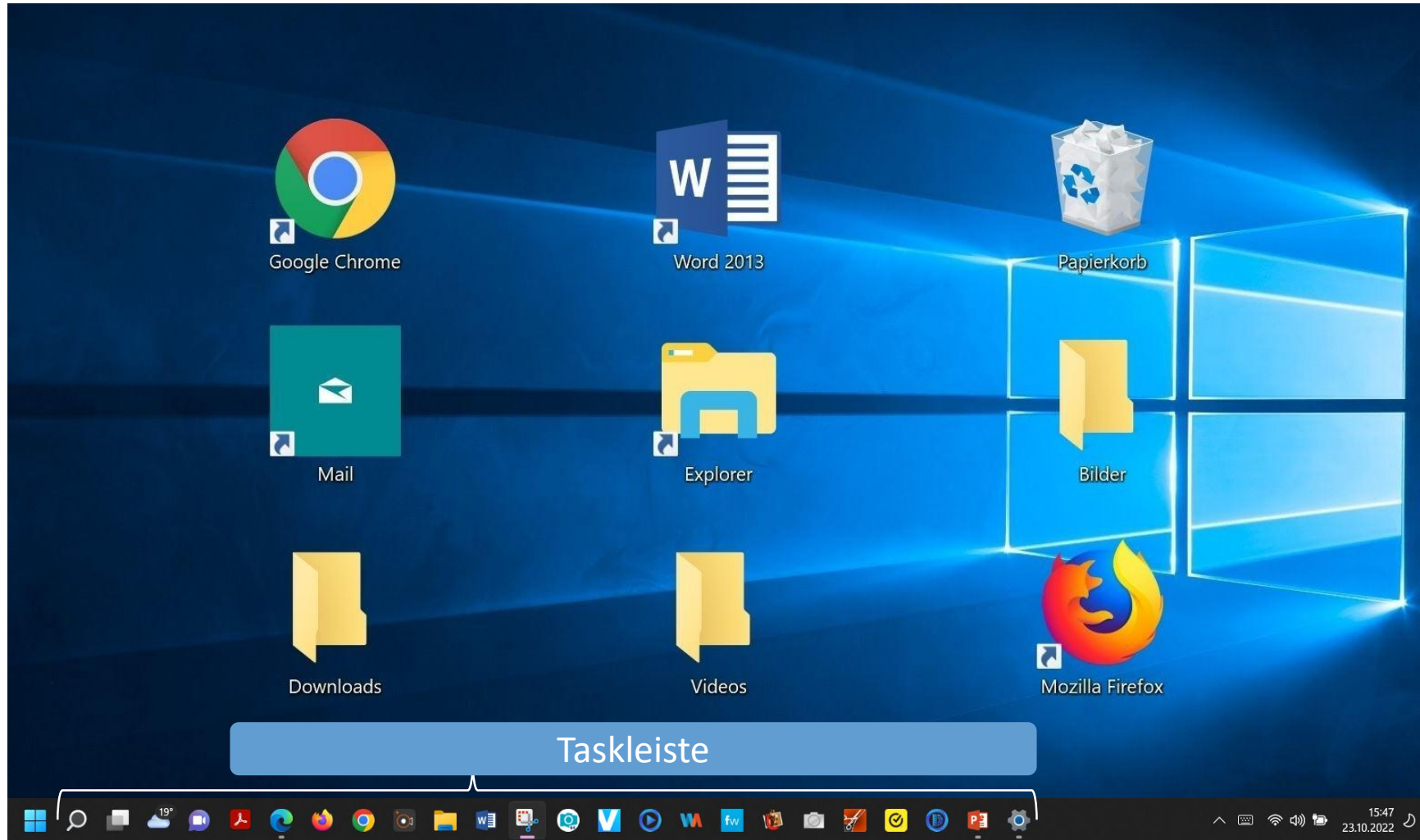
Arbeiten mit dem Computer: Der Desktop [2]



Windows-Startknopf

Der Startknopf ist ein Symbol (oft unten links auf dem Bildschirm), mit dem du das **Startmenü** öffnen kannst. Von dort aus kannst du Programme starten, Dateien suchen, Einstellungen ändern und den Computer herunterfahren oder neu starten.

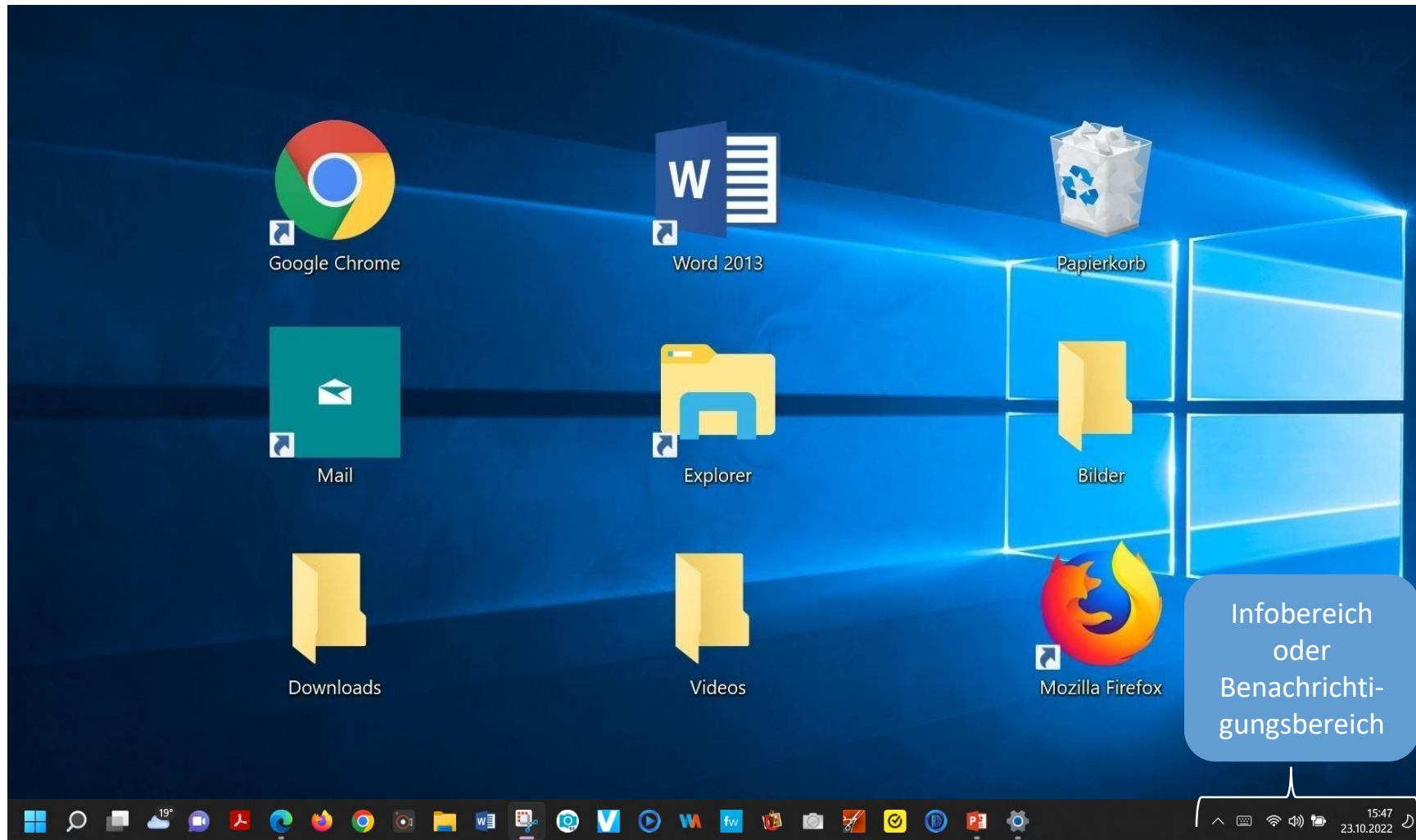
Arbeiten mit dem Computer: Der Desktop [3]



Taskleiste

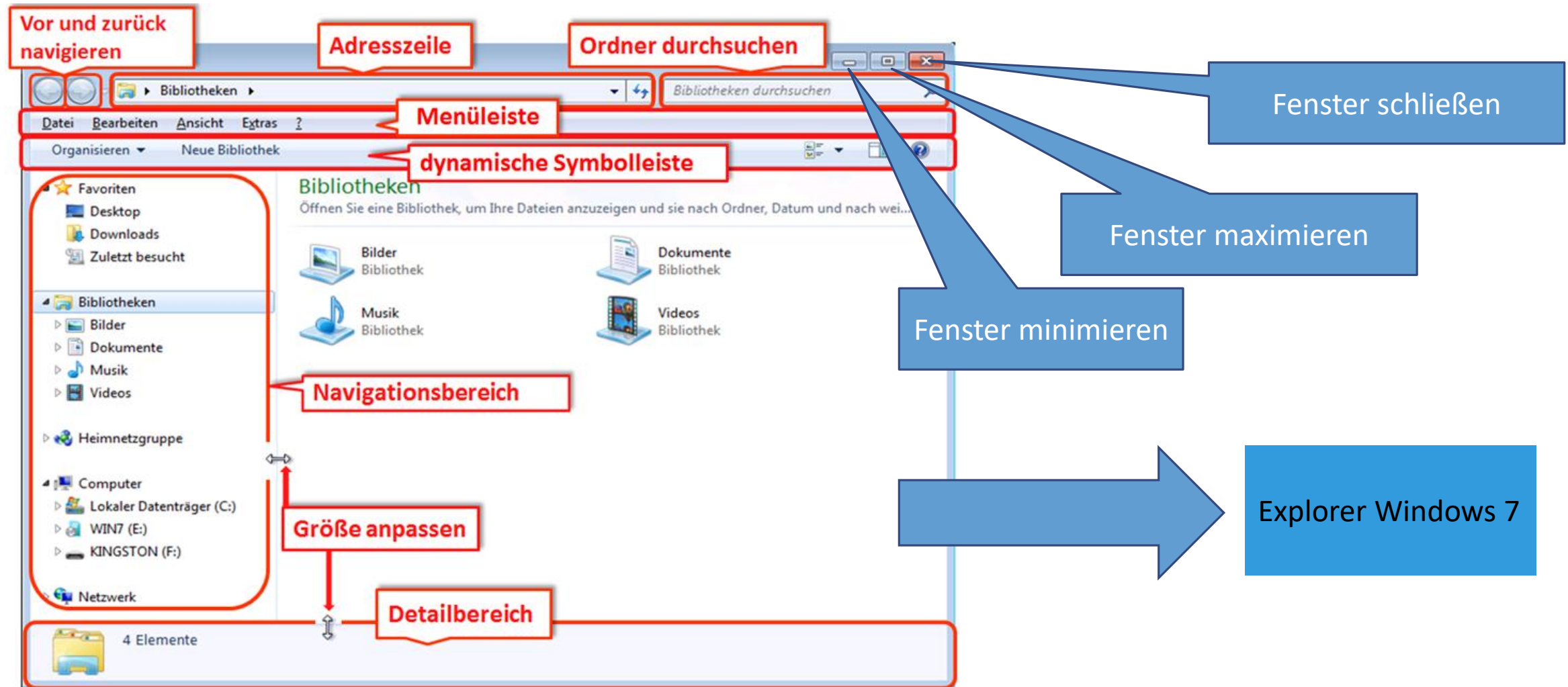
Die Taskleiste ist die Leiste unten auf dem Bildschirm, die dir schnellen Zugriff auf geöffnete Programme, wichtige Symbole (wie die Uhr oder Lautstärke) und die Suche bietet. Du kannst hier auch Programme anheften, um sie schneller zu öffnen.

Arbeiten mit dem Computer: Der Desktop [4]

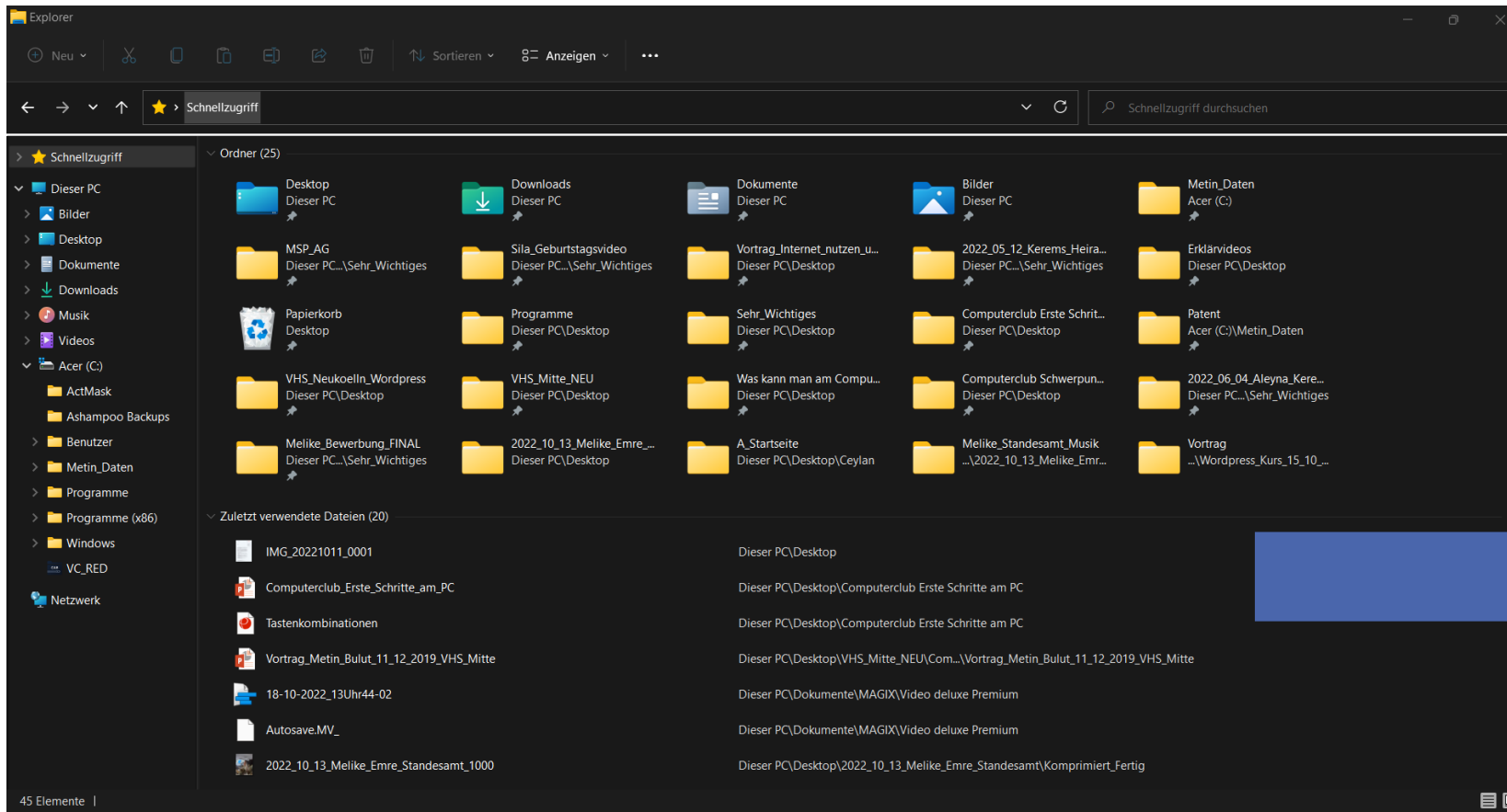


Infobereich oder Benachrichtigungsbereich
Hier findest du Symbole für Hintergrundprogramme, Systemfunktionen wie Lautstärke, Netzwerk, Akkuanzeige und Benachrichtigungen.

Arbeiten mit dem Computer: Der Explorer



Arbeiten mit dem Computer: Der Explorer



Explorer Windows 11

Geordneter Windows-Desktop

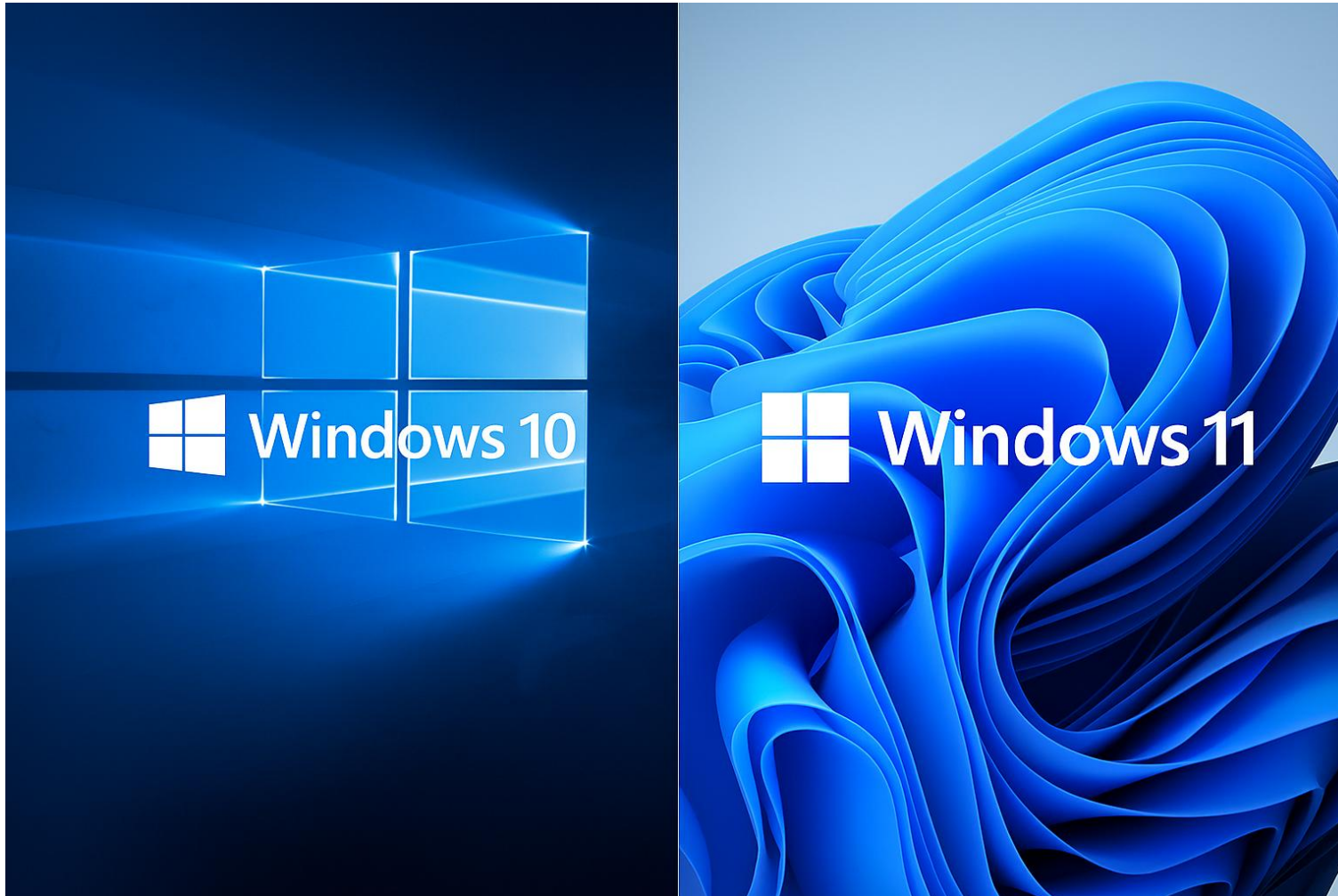


Chaotischer Windows-Desktop



Computer- und Internetsicherheit

Windows 10 nach Oktober 2025 sicher weiter nutzen



Hintergrund

- Offizieller Support von Microsoft für Windows 10 endet am 14. Oktober 2025
- Keine Sicherheitsupdates mehr → theoretisch höhere Angriffsgefahr
- Viele Geräte laufen aber weiterhin zuverlässig mit Windows 10
- Ziel: sicherer Weiterbetrieb trotz Support-Ende

Sicherheitstipps

- Antivirus & Firewall aktiv halten (Windows Defender + Firewall reicht oft schon)
- Regelmäßige Backups (externe Festplatte oder Cloud)
- Browser & Programme aktuell halten (Firefox, Chrome, LibreOffice etc.)
- Vorsicht bei Downloads & E-Mail-Anhängen

Erweiterte Schutzmaßnahmen

- Aktuellen Browser nutzen (sehr wichtig!)
- Virtualisierung oder Zweitgerät für Online-Banking & sensible Aufgaben
- Externe Sicherheitssoftware mit Updates nach 2025 verwenden
- Netzwerk- und Router-Sicherheit prüfen (WLAN-Passwort, Firmware-Update)

Alternative Optionen (nur wenn nötig)

- Extended Security Updates (ESU) von Microsoft (kostenpflichtig, v.a. für Firmen)
- Linux als Zweitsystem auf alter Hardware – parallele Nutzung mit Windows 10 möglich
- Windows 10 bleibt Hauptsystem, aber zusätzliche Flexibilität

Fazit

- Windows 10 kann auch nach 2025 sicher genutzt werden, wenn man:
 - sicheres Verhalten im Internet zeigt
 - Programme aktuell hält
 - zusätzliche Schutzmaßnahmen nutzt
- Für viele Alltagsaufgaben bleibt Windows 10 noch lange stabil

Windows 10 weiter nutzen – ESU kaufen & Sicherheits-Updates erhalten

Kurz erklärt

- Der offizielle Support für Windows 10 endete am 14. 10. 2025.
- Sicherheitspatches gibt es nur noch über Extended Security Updates (ESU), die jährlich gebucht werden können.
- ESUs sind kumulativ: Wenn du erst im 2. Jahr einsteigst, musst du auch das 1. Jahr nachzahlen.
- Anmeldung und Verwaltung erfolgen über Windows Update mit deinem Microsoft-Konto.
- Preis laut Medien: etwa 30 US-\$ pro Jahr (Jahr 1) – genaue Kosten beim Anmelden prüfen.

Voraussetzungen

- Windows 10 Version 22H2 mit allen Updates installiert
- Echt aktiviertes Windows
- Microsoft-Konto für die ESU-Verknüpfung

Schritt-für-Schritt (für Präsentationsfolie)

1. Start → Einstellungen → Update & Sicherheit → Windows Update öffnen
2. Auf den Hinweis „Erweiterte Sicherheitsupdates (ESU) – Jetzt anmelden“ klicken
3. Mit Microsoft-Konto anmelden (oder hinzufügen)
4. ESU-Lizenz für Jahr 1 auswählen und Kauf abschließen
5. Nach Buchung:
 - Windows Update erneut öffnen
 - Nach Updates suchen
 - Sicherheitsupdates installieren

Merke

- ESU liefert nur Sicherheitsfixes, keine neuen Funktionen oder Support.
- Laufzeit: jährlich verlängerbar, maximal 3 Jahre (bis 2028).



Windows 11: Eignung prüfen & Upgrade durchführen

Kurz erklärt

- Der offizielle Support für Windows 10 endete am 14. 10. 2025.
- Sicherheitspatches gibt es nur noch über Extended Security Updates (ESU), die jährlich gebucht werden können.
- ESUs sind kumulativ: Wenn du erst im 2. Jahr einsteigst, musst du auch das 1. Jahr nachzahlen.
- Anmeldung und Verwaltung erfolgen über Windows Update mit deinem Microsoft-Konto.
- Preis laut Medien: etwa 30 US-\$ pro Jahr (Jahr 1) – genaue Kosten beim Anmelden prüfen.

Voraussetzungen

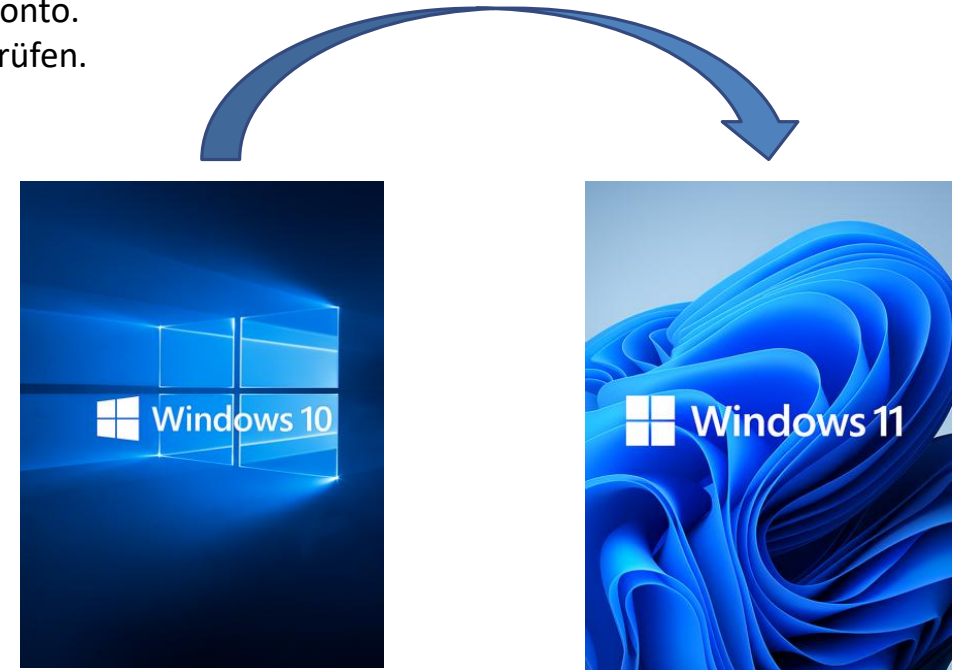
- Windows 10 Version 22H2 mit allen Updates installiert
- Echt aktiviertes Windows
- Microsoft-Konto für die ESU-Verknüpfung

Schritt-für-Schritt (für Präsentationsfolie)

1. Start → Einstellungen → Update & Sicherheit → Windows Update öffnen
2. Auf den Hinweis „Erweiterte Sicherheitsupdates (ESU) – Jetzt anmelden“ klicken
3. Mit Microsoft-Konto anmelden (oder hinzufügen)
4. ESU-Lizenz für Jahr 1 auswählen und Kauf abschließen
5. Nach Buchung:
 - Windows Update erneut öffnen
 - Nach Updates suchen
 - Sicherheitsupdates installieren

Merke

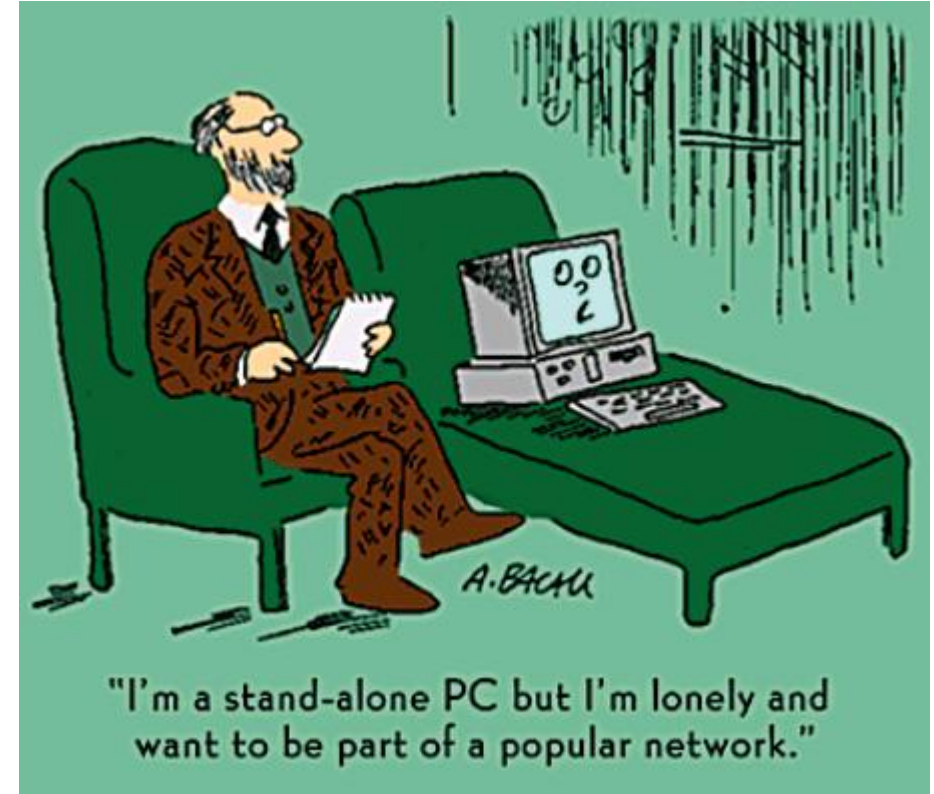
- ESU liefert nur Sicherheitsfixes, keine neuen Funktionen oder Support.
- Laufzeit: jährlich verlängerbar, maximal 3 Jahre (bis 2028).



Welchen Gefahren ist ein PC-Nutzer ausgesetzt?

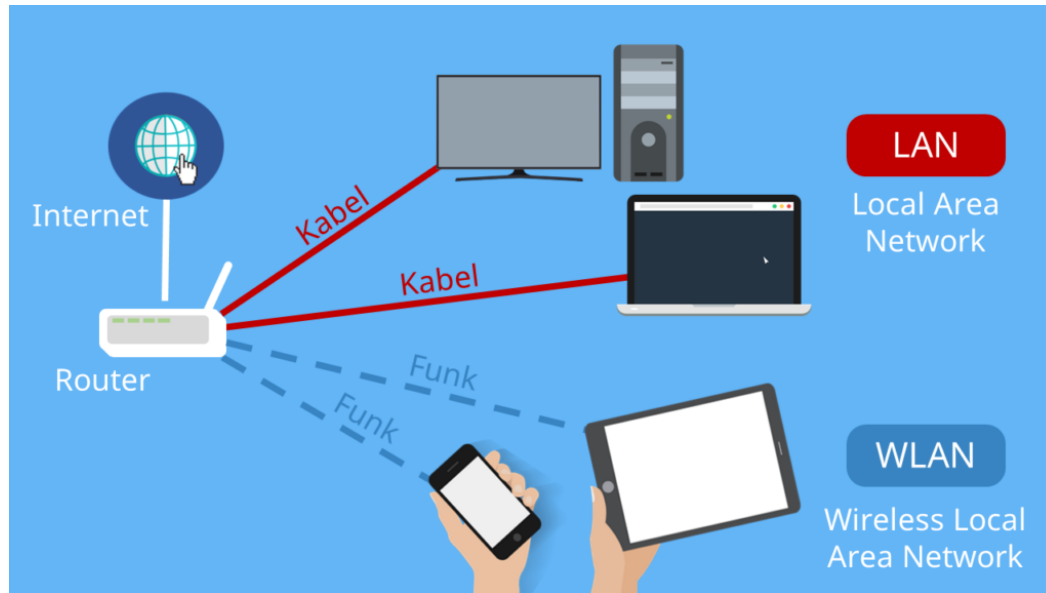
Gefahren OHNE eigenen Internetzugang:

- Externe Datenquellen, wie Disketten, Festplatten, CD, DVD, USB-Sticks
- Vermeintliche „saubere“ Datenträger von Originalherstellern (z.B. Heft-CD)
- Gebrauchte PC mit vorinstallierter Software
- Vernetzte Computer in Büros oder Heimnetzwerk - Datenübertragung
- WLAN-Sicherheit – unsichere Passwörter /Sicherheitseinstellungen

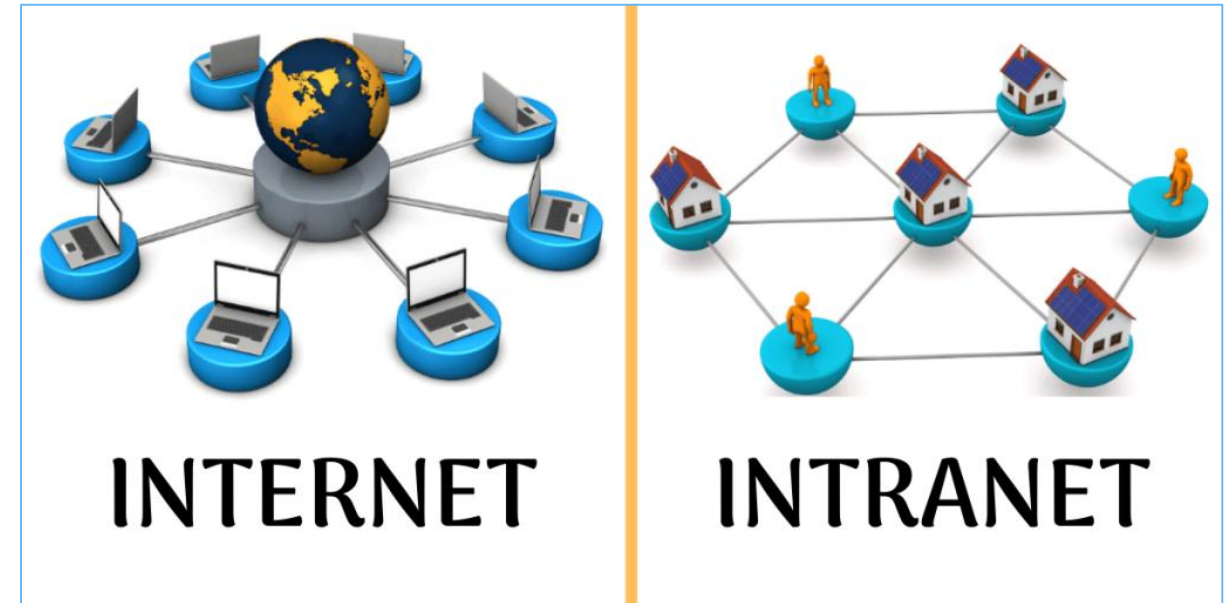


Ich bin ein allein stehender PC, aber ich bin einsam und möchte ein Teil eines beliebten Netzwerkes sein.

Wie funktioniert das Internet?



Das **Internet**, kurz für "**interconnected networks**" (zu Deutsch: "vernetzte Netzwerke"), ist ein weltweites Netzwerk von Computern und anderen elektronischen Geräten, das es ermöglicht, Informationen und Daten zwischen diesen Geräten auszutauschen. Es ist ein riesiges Netzwerk, das Millionen von Computern und Servern weltweit miteinander verbindet.



Ein **Intranet** ist ein privates, internes Netzwerk, das in Unternehmen, Bildungseinrichtungen oder anderen Organisationen verwendet wird, um Informationen, Ressourcen und Kommunikation innerhalb der Organisation bereitzustellen und zu erleichtern. Im Gegensatz zum öffentlichen Internet, das weltweit zugänglich ist, ist ein Intranet auf autorisierte Benutzer innerhalb der Organisation beschränkt.

Antiviren- und Antimalware-Software

Windows Defender vs. andere Anbieter



Die Wahl zwischen Windows Defender, der von Microsoft bereitgestellten integrierten Antivirensoftware, und einer Drittanbieter-Antivirensoftware hängt von verschiedenen Faktoren ab, einschließlich Ihrer individuellen Anforderungen und Vorlieben. Hier sind einige Überlegungen:

- **Integriert:** Windows Defender ist bereits in Windows 10 und Windows 11 integriert, was bedeutet, dass Du keine separate Installation durchführen musst.
- **Kostenlos:** Es ist kostenlos und erfordert keine zusätzlichen Kosten oder Abonnements.
- **Geringe Systembelastung:** Windows Defender ist ressourcenschonend und wirkt sich normalerweise nicht negativ auf die Systemleistung aus.
- **Automatische Updates:** Es wird regelmäßig von Microsoft aktualisiert, um sicherzustellen, dass es gegen die neuesten Bedrohungen gewappnet ist.
- **Grundlegender Schutz:** Es bietet grundlegenden Schutz vor Viren, Malware und Spyware, kann jedoch weniger erweiterte Funktionen haben als einige Drittanbieter-Antivirenprogramme.

Die Wahl der Antiviren-Software hängt also von Deinen speziellen Anforderungen ab.

- Wenn Du nur grundlegenden Schutz wünschst und die Ressourcen Deines Systems schonen möchtest, kann Windows Defender ausreichend sein.
- Wenn Du jedoch erweiterte Sicherheitsfunktionen wünschst oder spezifische Anforderungen hast, kann es sinnvoll sein, eine Drittanbieter-Antivirensoftware zu verwenden.



- **Erweiterte Funktionen:** Viele Drittanbieter-Antivirenprogramme bieten erweiterte Funktionen wie erweiterte Firewall-Einstellungen, Schutz vor Ransomware, Schutz vor Phishing und mehr.
- **Zusätzliche Sicherheitsschichten:** Einige bieten zusätzliche Schutzschichten und Tools zur Systemoptimierung.
- **Kundensupport:** Einige Drittanbieter-Antivirensoftwareanbieter bieten Kundenbetreuung und Supportleistungen an.
- **Kosten:** Die meisten Drittanbieter-Antivirenprogramme erfordern kostenpflichtige Abonnements oder Lizenzen..

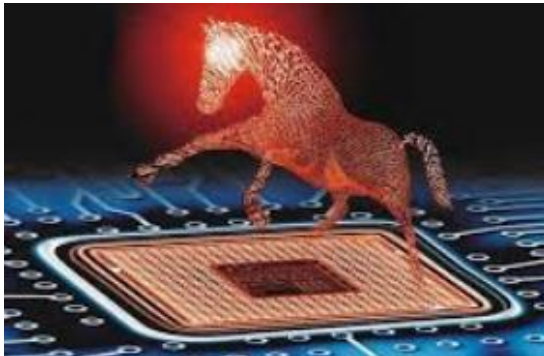
Welche Gefahren gibt es? (Teil 1)



VIREN

Computerviren sind schädliche Softwareprogramme oder Codefragmente, die dazu entwickelt wurden, sich auf einem Computer oder einem anderen digitalen Gerät ohne die Zustimmung des Benutzers zu replizieren und sich auszubreiten. Diese Viren können erhebliche Schäden verursachen, indem sie Daten löschen, Systeme beschädigen, Informationen stehlen oder die Leistung eines Computers beeinträchtigen.

- Trojanische Pferde
- Würmer
- Ransomware
- Spyware
- Adware
- Keylogger
- Rootkits
- Botnets



TROJANER (Ableitung vom trojanischen Pferd)

Software zur Fernsteuerung Deines Computers. Es wird eine Software auf Deinem PC installiert, um ihn fernzusteuern. Trojaner beschädigen nicht Dein PC, sondern missbrauchen ihn, um z.B. andere Computer zu attackieren.

Das Trojanische Pferd ist ein legendäres Ereignis aus der griechischen Mythologie, das im Kontext des Trojanischen Krieges stattfand. Die Griechen belagerten die Stadt Troja, konnten sie jedoch nicht erobern. Um die Belagerung zu beenden, entwickelten sie eine listige Taktik: Sie bauten ein riesiges hölzernes Pferd und versteckten darin heimlich griechische Krieger. Die Griechen gaben vor, sich zurückzuziehen, ließen das Pferd vor den Stadtoren zurück, und als die Trojaner es in die Stadt brachten, öffneten die versteckten Krieger in der Nacht die Tore für das griechische Heer, wodurch Troja erobert wurde. Diese Geschichte steht für List und Täuschung im Krieg und dient oft als Metapher für heimtückische Taktiken.

Welche Gefahren gibt es? (Hackerangriff auf das Pentagon)



Quelle: <https://www.faz.net/aktuell/politik/hackerangriff-auf-pentagon-11338917.html>



Quelle: <https://www.spiegel.de/politik/ausland/cyberangriff-hacker-erbeuten-tausende-pentagon-geheimdaten-a-774553.html>

Worauf muss geachtet werden, damit die Risiken minimiert werden?

- Die Sensibilisierung der Menschen für Sicherheitspraktiken
- Regelmäßige Updates
- Bedrohungsinformationen teilen, siehe www.mimikama.at
- Antiviren- und Sicherheitssoftware
- Zugangsbeschränkungen
- Sicherheitsüberwachung
- Etc.

Welche Gefahren gibt es? (Hackerangriff auf das Pentagon)

Der Hackerangriff auf das Pentagon im Jahr 2013 war ein bedeutendes Ereignis in der Geschichte der Cybersicherheit. Es handelte sich um eine groß angelegte Attacke, die gezielt auf das US-Verteidigungsministerium abzielte. Der Angriff offenbarte die zunehmende Bedrohung durch ausländische Akteure und zeigte die Verwundbarkeit selbst hoch gesicherter Netzwerke.

Hintergrund und Ablauf des Angriffs

Im Jahr 2013 griffen unbekannte Hacker das Netzwerk des Pentagon an, wobei es sich vermutlich um staatlich unterstützte Akteure handelte. Berichten zufolge war das Ziel des Angriffs, sensible militärische Informationen und strategische Daten zu erlangen. Der Angriff nutzte fortschrittliche Malware und gezielte Phishing-Methoden, um Zugang zu den Netzwerken zu erlangen.

Ein besonders betroffener Bereich war das System des US Joint Chiefs of Staff, das unter anderem für militärische Planungen und Kommunikation genutzt wird. Innerhalb kurzer Zeit wurden Zehntausende E-Mails und sensible Dokumente kompromittiert.

Reaktion des Pentagons

Das Pentagon reagierte schnell auf den Angriff und schaltete betroffene Systeme vorübergehend ab, um die Bedrohung einzudämmen. Teams für Cybersicherheit analysierten den Angriff und identifizierten Schwachstellen im System. Der Vorfall führte dazu, dass umfangreiche Sicherheitsmaßnahmen implementiert wurden, um zukünftige Angriffe abzuwehren.

Vermutete Akteure

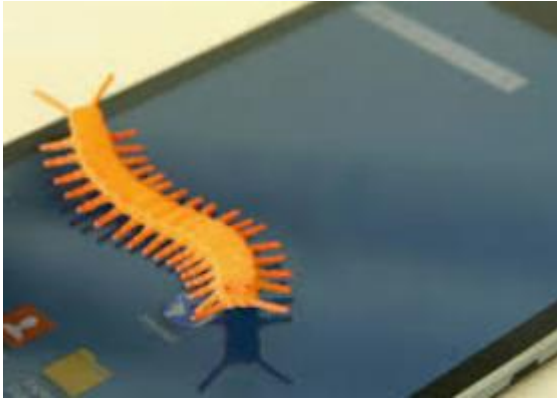
Obwohl die genauen Urheber des Angriffs nie offiziell bestätigt wurden, deuteten viele Hinweise auf ausländische staatliche Akteure, insbesondere aus Russland oder China. Diese Länder wurden in der Vergangenheit häufig mit ähnlichen Cyberangriffen in Verbindung gebracht.

Folgen des Angriffs

Der Angriff führte zu einem Umdenken in der Cybersicherheitsstrategie der USA. Es wurden Milliardeninvestitionen in die Verteidigung gegen Cyberbedrohungen getätigt, und das Cyber Command des US-Militärs wurde weiter ausgebaut. Der Vorfall unterstrich, dass Cyberkriege zunehmend eine zentrale Rolle in internationalen Konflikten spielen.

Dieser Angriff von 2013 war ein Weckruf für viele Regierungen weltweit, die Sicherheit ihrer digitalen Infrastruktur ernsthaft zu verbessern.

Welche Gefahren gibt es? (Teil 2)



WÜRMER

verbreiten sich selbstständig über Netzwerke und das Netzwerk, z.B. über offenes WLAN. Sie können oftmals Deine Sicherheitsmaßnahmen umgehen und können andere Schadsoftware wie z.B. Viren, Trojaner etc. mit sich bringen, um Deinen PC zu infizieren.



BACKDOOR

durchlöchert oder umgeht Deinen Schutz, oft für Spam oder Denial-of-Service. Kurz: Dein PC wird für Spam verwendet oder zum Attackieren von anderen PCs, um z.B. diese lahm zu legen.

Welche Gefahren gibt es? (Teil 3)



SPYWARE/ADWARE (SPY = SPION)

spioniert Benutzer und dessen Verhalten.

Ziel:

Daten und Surfverhalten über Dich zu bekommen, um Dir damit zielgerichtet Spam zu schicken oder Deine Daten zu verkaufen.



SCAREWARE (SCARE = ANGST)

verleitet Schadstoffe zu installieren, oftmals kostenpflichtig.

Es ist ein Schadprogramm, das Dich verängstigen und so zu bestimmten Handlungen bewegen soll.

Welche Gefahren gibt es? (Teil 4)



SPAM

unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und häufig Werbeinhalte enthalten. Dieser Vorgang wird *Spamming* oder *Spammen* genannt, der Verursacher *Spammer*.



COOKIE (zu Deutsch *Keks* oder *Plätzchen*)

ist eine kleine Datei, die auf dem Computer eines Webseitenbesuchers gespeichert wird. Mithilfe der Informationen aus der Datei lassen sich beispielsweise Benutzer wiedererkennen, Aktivitäten auf Webseiten verfolgen, Einstellungen eines Benutzers wiederherstellen oder Websessions fortführen.

Welche Gefahren gibt es? (Teil 5)



PHISHING (= Angeln)

beschreibt den Versuch des Diebstahls von Kennungen und Passwörtern per Internet durch den Versand von gefälschten E-Mails oder SMS. Internet-Anwender werden von Cyberkriminellen mittels täuschend echt nachgemachter E-Mails auf gefälschte Internetseiten von Banken, Onlineshops oder anderen Onlinediensten gelockt um dort deren Benutzerkennungen und Passwörter zu ergattern. Die ergaunerten Daten werden beispielsweise für Kontoplünderungen oder Hackerangriffe auf Unternehmen verwendet.

Welche Gefahren gibt es? (Teil 5)

! Ihr Guthaben kann heute noch Großes bewirken (B4F73DBEA2)

Telekom Punkte

An: bulut-m@t-online.de



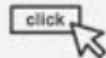
Ihre Punkte sind bereit,
um in ein Geschenk eingelöst zu werden.
Ihr Guthaben: 487 Treuepunkte

Guten Tag ,

wir möchten Sie darüber informieren, dass Ihr Treuepunktekonto 400 Punkte überschritten hat, was Ihnen nun das Recht gibt, diese Punkte gemäß den Nutzungsbedingungen für Treuepunkte (Ref. DE63200/2017) in ein Geschenk umzuwandeln.

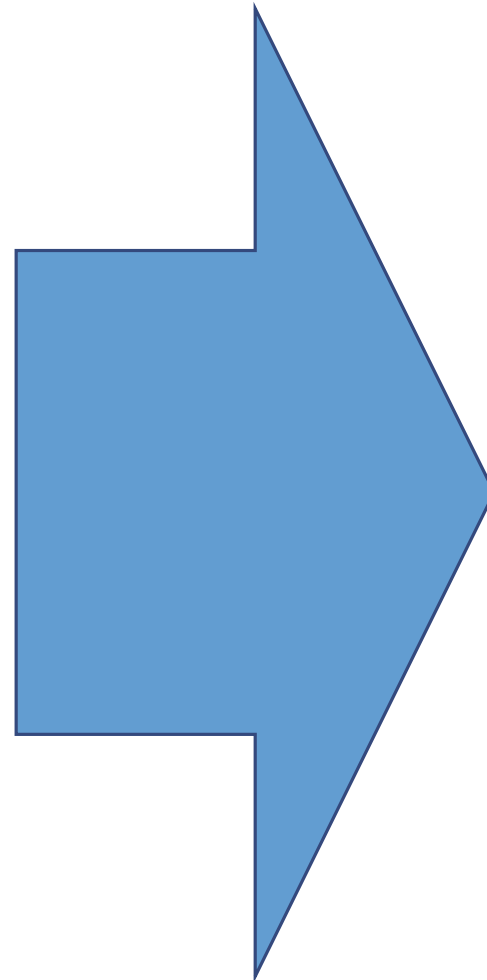
Ihr aktueller Punktestand ist bis zum **31. Januar** gültig. Nach diesem Datum wird Ihr Punktestand automatisch auf null zurückgesetzt, auch wenn die Punkte nicht eingelöst wurden. Um von Ihren gesammelten Punkten zu profitieren, laden wir Sie ein, diese rechtzeitig gegen ein Geschenk aus unserer Belohnungsliste einzutauschen.

WANDLE MEINE PUNKTE JETZT UM



Ihr Guthaben bis Dezember 2024 :

Gesammelte Punkte:	437 Punkte
Bonus:	50 Punkte
Gesamt zum Einlösen:	487 Punkte



https://treueprogramm-privatkunden.com/INSIGHT2/1.html

Privat | Business

Mobilfunk | Internettarife | TV | Magenta Family | Service & Kontakt

Produkt	Preis mit Treuepunkten	Verfügbare Punkte	Verbleibende Punkte	Gesamtkosten	Kaufpreis
Xiaomi 14T Pro 5G	550 Punkte	487 Punkte	0 Punkte	9,99 €	9,99 €
Samsung Galaxy Z Flip6 5G	620 Punkte	487 Punkte	0 Punkte	15,99 €	15,99 €
Apple iPhone 16 Plus	550 Punkte	487 Punkte	0 Punkte	9,99 €	9,99 €

Partnerprodukte

- Qualitätsprodukte von unseren Partnern.
- Exzellenz mit Partnerprodukten.
- Exklusive Angebote unserer Partner.
- Die besten Produkte unserer Partner.
- Zusätzliche Liefergebühren können anfallen

Welche Gefahren gibt es? (Teil 5)

Phishing Beispiele, Seite 1



Sehr geehrte Kundin, sehr geehrter Kunde,

aufgrund geänderter Nutzungsbedingungen steht eine Aktualisierung Ihrer Daten an. Diese Maßnahme ist aus Sicherheitsgründen zwingend erforderlich.

Klicken Sie dafür auf den unten stehenden Button und befolgen Sie die notwendigen Schritte. Geben Sie dabei Ihre Daten vollständig und korrekt an.

[Weiter zu PayPal](#)

Mit freundlichen Grüßen,
Ihr PayPal Kundenservice



Sehr geehrter Sparkasse Kunde,

Um diesen Dienst weiterhin nutzen zu koennen, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren.

[zur Aktualisierung](#)

Online Banking ist mit einem umfassenden Sicherheitssystem ausgestattet, das gewaehrleistet, dass Ihre persoelichen Daten von Unbefugten nicht entschluesselt oder veraendert werden koennen.

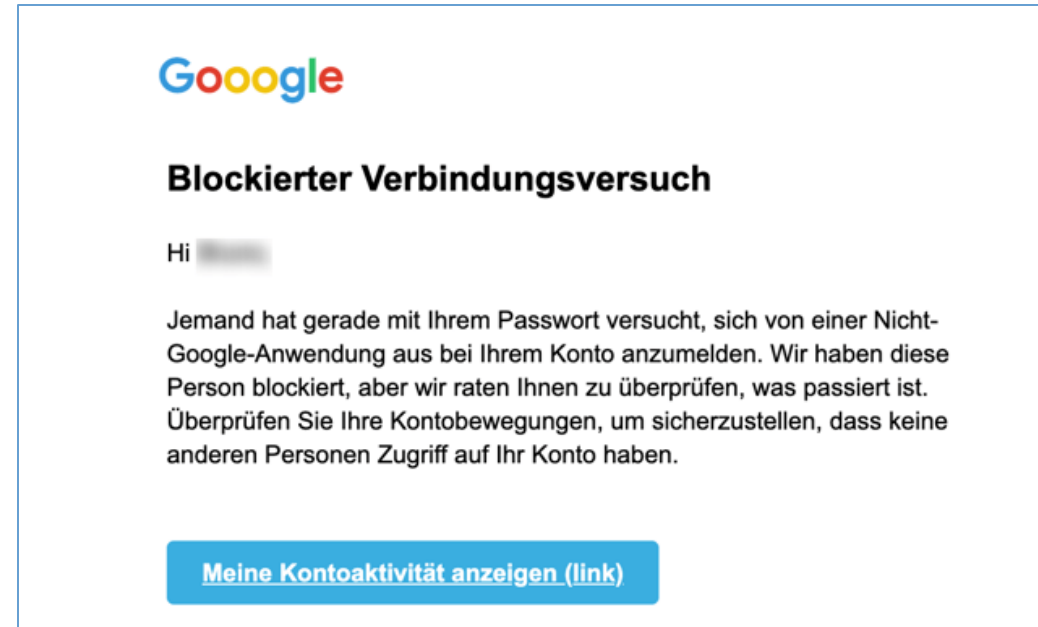
Nach Vervollstaendigung dieser Schritte werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos telefonisch kontaktiert um den Updatevorgang abzuschliessen.

Bankgeschäfte immer dort, wo Sie sind!

Verwalten Sie Ihre Konten/Depots online und erledigen Sie Ihre Bankgeschäfte einfach, schnell und sicher vom Buero oder von Zuhause aus. Unabhaengig von Öffnungszeiten - 24 Stungen am Tag, an 365 Tagen im Jahr. Alles, was Sie benoetigen, ist ein Internetzugang und die Freischaltung Ihres Kontos oder Wertpapierdepots für Ihr Online Banking der Sparkasse.

Welche Gefahren gibt es? (Teil 5)

Phishing Beispiele, Seite 2



Welche Gefahren gibt es? (Teil 5)

Phishing Beispiele, Seite 3

The Netflix logo is displayed in red, bold, sans-serif capital letters on a black rectangular background.

Hi [REDACTED]

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

Deine Freunde bei Netflix

Microsoft-Konto

Passwort abgelaufen

Ihr Host-Administrator hat Ihr Passwort für Ihre E-Mail so festgelegt, dass es jeden Monat abläuft.

Dies ist eine Funktion zum Schutz Ihres Profils. Daher ist es zwingend erforderlich, dass Sie Ihr Passwort erneuern, um Probleme mit Ihrer E-Mail zu vermeiden.

Erneuern

Vielen Dank,

Microsoft-Sicherheitsabteilung

Phishing-Mails: Stand heute

- **Keine Rechtschreibfehler mehr**
Die Texte werden automatisch überprüft, damit keine Tipp- oder Schreibfehler mehr vorkommen.
- **SSL-Zertifikat so gut wie immer vorhanden**
Die Verbindung zur Webseite ist sicher und verschlüsselt (erkennbar am Schloss-Symbol).
- **Man-in-the-Middle vorhanden**
Es wurde erkannt, dass jemand die Verbindung mitlesen könnte – die Verbindung ist nicht sicher.
- **Prüfung auf Validität der Daten**
Der Computer kontrolliert, ob die eingegebenen Daten richtig und vollständig sind.
- **Automatisches Versenden oder Speichern der Daten**
Korrekte Daten werden automatisch gespeichert oder verschickt.
- **Kontrollcenter**
Eine Übersicht, in der man alle wichtigen Funktionen und Einstellungen findet.



Phishing-SMS: Stand heute

- **Absender ist oft einfach eine Rufnummer**
Viele Betrugs-SMS oder Nachrichten zeigen nur eine Telefonnummer an. Man sieht nicht, wer wirklich dahintersteckt.
- **Kann aber auch gefälscht sein**
Betrüger können die Nummer oder den Namen fälschen, sodass es so aussieht, als komme die Nachricht von der Bank, der Post oder sogar von Freunden.
- **Druck wird aufgebaut**
Die Nachricht macht oft **Angst oder Stress**, zum Beispiel:
„Ihr Konto wird gesperrt!“ oder „Sie müssen sofort handeln!“.
Damit will der Betrüger erreichen, dass man schnell klickt.
- **Keine persönliche Anrede**
Oft steht dort nicht dein Name, sondern nur etwas wie „Sehr geehrter Kunde“ oder gar keine Anrede. Das ist ein Zeichen für eine Massen-Nachricht.
- **Wird auch oft mit „Shortnern“ gearbeitet**
Betrüger benutzen kurze, verkürzte Links (z. B. bit.ly), damit man nicht gleich sieht, wohin der Link wirklich führt. Ein Klick kann gefährlich sein.
- **Aufforderung Eingabe sensibler Daten**
Die Nachricht will dich dazu bringen, persönliche Daten einzugeben – z. B. Passwörter, Bankdaten, TAN-Nummern oder Kreditkarteninfos. Das ist ein typisches Merkmal von **Phishing**.



Phishing Check

- Dringlichkeit / Drohung („Ihr Konto wird gesperrt“, „Sofort handeln!“)
- Unerwartete Nachrichten von Banken, Paketdiensten oder Behörden, die man nicht angefordert hat
- Rechtschreib- oder Grammatikfehler, ungewöhnliche Formulierungen, generisch Anrede („Sehr geehrter Kunde“)
- Aufforderung zur Eingabe sensibler Daten (Passwort, PIN, TAN, Kreditkartendaten, 2FA-Code)
- Links mit seltsamen oder ähnlich aussehenden Domains (z. B. bank-login.example.com, telekom.de statt telekomd.de)
- Kurzlinks ohne Kontext (z. B. bit.ly), unbekannte Absendernummern oder Shortcodes
- Anhänge (.zip, .exe, .scr, Office-Makros) – nicht öffnen, wenn unerwartet
- Widersprüchliche oder gefälschte Absenderadresse (Adresse stimmt nicht mit angezeigtem Namen überein)



Die besten Tipps, wie man sich vor gefährlichen oder betrügerischen E-Mails schützt

Absender prüfen:

echte Firmenadresse vs. gefälschte Domain
auf vollständige E-Mail-Adresse achten (nicht nur den sichtbaren Namen)

Link prüfen, ohne zu klicken:

Maus über den Link halten (Hover), um die echte URL im Browser/Client zu sehen
auf Tippfehler achten
auf zusätzliche oder ungewöhnliche Wörter achten

E-Mail-Header ansehen:

SPF/DKIM/DMARC-Ergebnisse prüfen
zeigt oft, ob die E-Mail wirklich von der angegebenen Domain kommt
meist sichtbar in Desktop-Clients oder Webmail-Diensten

Anhänge niemals direkt öffnen:

zuerst mit einem Virenskan prüfen
bei unerwarteten Anhängen immer nachfragen/abklären
insbesondere vorsichtig bei .zip, .exe, .scr oder Office-Makros

Rechtsgültige Kommunikation:

Banken/Behörden fragen selten per E-Mail nach Zugangsdaten
wichtige oder kritische Aktionen werden meistens auf offiziellen Portalen durchgeführt



Woran erkennt man eine Phishing-Mail? [1]

1. Verdächtige Absenderadresse

- Absenderadresse wirkt echt, ist aber leicht verfälscht
→ z. B. service@paypal.com statt service@paypal.com
- Große Firmen nutzen eigene Domains, keine privaten E-Mail-Adressen

2. Unpersönliche Anrede

- Formulierungen wie „Sehr geehrter Kunde“ oder „Hallo Nutzer“
- Seriöse Unternehmen sprechen dich **mit Namen** an

3. Dringlichkeit oder Drohungen

- „Ihr Konto wird gesperrt!“ / „Letzte Mahnung!“
- Ziel: Druck aufbauen, damit du **schnell klickst**

Woran erkennt man eine Phishing-Mail? [2]

4. Verdächtige Links oder Anhänge

- Linktext ≠ tatsächliche Adresse
→ Maus über Link bewegen, bevor du klickst
- Anhänge können **Viren oder Schadsoftware** enthalten (.zip, .exe, .xlsm)

5. Fehlerhafte Sprache

- Viele Rechtschreib- oder Grammatikfehler
- Ungewöhnliche Formulierungen → Hinweis auf Übersetzungssoftware

6. Unlogische Inhalte

- Bezieht sich auf **Konten oder Bestellungen**, die du nicht hast
- Oft mit gefälschten Logos oder Namen

Woran erkennt man eine Phishing-Mail? [3]

7. Aufforderung zu sensiblen Daten

- Kein seriöser Anbieter fragt per E-Mail nach:
 - Passwörtern
 - Kreditkartendaten
 - TANs oder PINs

Tipps zum Schutz

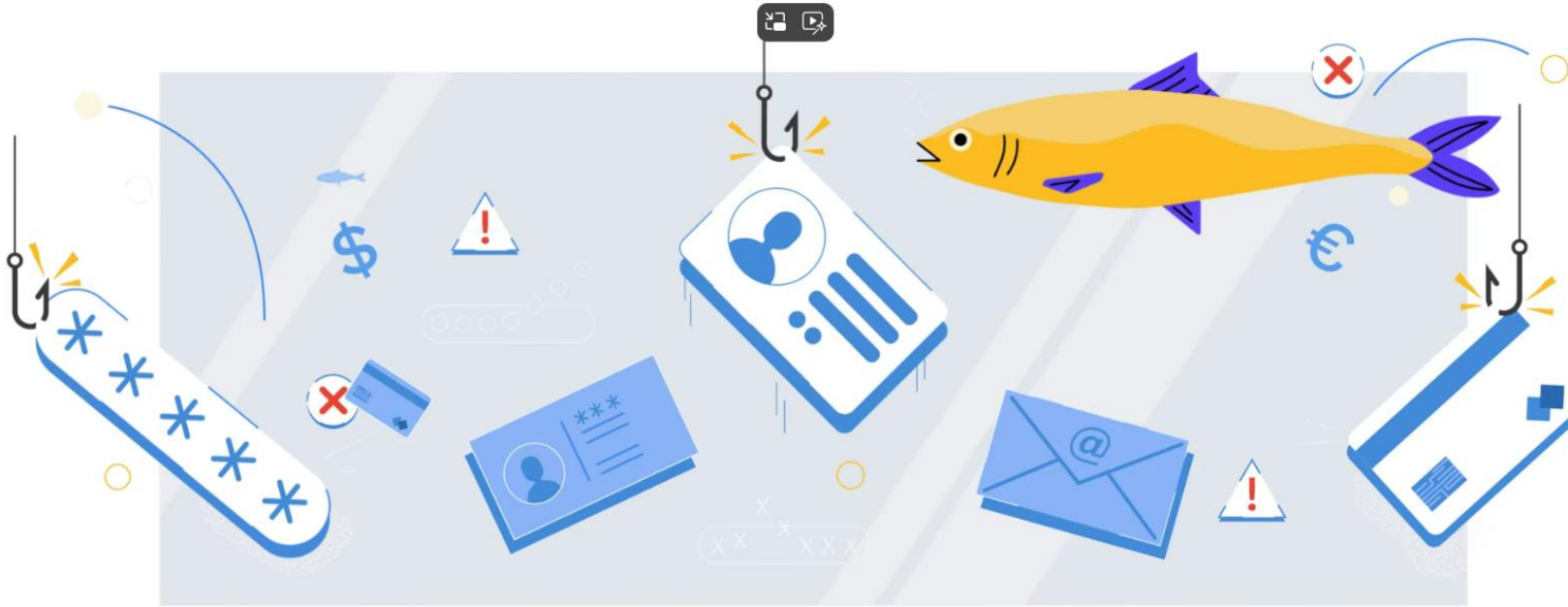
- Nie auf verdächtige Links klicken
- Keine Anhänge öffnen
- Absender prüfen (Domain, Schreibweise)
- Direkt auf die offizielle Website gehen, nicht über den E-Mail-Link
- Im Zweifel melden oder löschen

Woran erkennt man eine Phishing-Mail? [4]

Zusammenfassung

Eine Phishing-Mail erkennt man meist an einer verdächtigen Absenderadresse, unpersönlicher Anrede, Dringlichkeitsdruck, falschen oder gefährlichen Links und Anhängen, sprachlichen Fehlern, unlogischen Inhalten sowie der Aufforderung, persönliche Daten preiszugeben.

Erkennst Du Phishing?



Erkennen Sie Phishing?

Bei Phishing-Angriffen werden ahnungslose Nutzer dazu verleitet, personenbezogene oder finanzielle Informationen preiszugeben. Häufig werden dabei Inhalte bekannter, vertrauenswürdiger Unternehmen nachgeahmt.

Durch KI werden Phishing-Angriffe immer raffinierter, personalisierter und häufiger.

Sie glauben, Sie können erkennen, was echt und was gefälscht ist?

[Quiz starten](#)

<https://phishingquiz.withgoogle.com/>

Welche Gefahren gibt es? (Teil 5)

Quishing – Betrug mit QR-Codes

Quishing ist eine Betrugsmasche, bei der Kriminelle gefälschte QR-Codes verwenden, um dich auf gefährliche Webseiten zu locken. Dort versuchen sie, deine persönlichen Daten wie Bankdaten oder Passwörter zu stehlen oder Schadsoftware auf dein Gerät zu laden.

Diese QR-Codes findest du oft auf scheinbar echten Briefen, Postern oder an öffentlichen Orten. Wenn du den Code scannst, kannst du schnell in die Falle tappen.

So kannst du dich schützen:

1. Sei misstrauisch bei unbekanntem QR-Codes.
2. Schau dir die angezeigte Webseite genau an, bevor du sie öffnest.
3. Lade keine Apps über QR-Codes herunter.
4. Frag direkt bei der Bank oder Firma nach, ob der QR-Code echt ist.
5. Nutze eine Antiviren-App, die dich vor gefährlichen Webseiten warnt.

Merke

Scanne keine QR-Codes, wenn du nicht sicher bist, wohin sie führen!



Welche Gefahren gibt es? (Teil 5)

Gefälschte QR-Codes: Welche Gefahren lauern und wie du dich schützen kannst

1. Diebstahl persönlicher Daten

- Die Webseite könnte dich auffordern, sensible Informationen einzugeben, z. B.:
 - Bankdaten
 - Passwörter
 - Kreditkartennummern
 - Persönliche Daten wie Name, Adresse oder Geburtsdatum
- Diese Daten können von Kriminellen genutzt werden, um:
 - Geld von deinem Konto zu stehlen
 - Identitätsdiebstahl zu begehen

2. Installieren von Schadsoftware

- Die Webseite könnte dich dazu bringen, eine Datei oder App herunterzuladen, die Schadsoftware (z. B. Viren, Trojaner oder Ransomware) enthält.
- Diese Schadsoftware kann:
 - Deine Geräte blockieren, bis du ein Lösegeld zahlst (Ransomware)
 - Deine Daten ausspionieren (z. B. Passwörter oder Fotos)
 - Deine Geräte für weitere Betrugsaktionen missbrauchen

3. Kostenfallen

- Du könntest unbemerkt auf eine Abzock-Seite geleitet werden, die dich automatisch für teure Abos anmeldet oder Zahlungen auslöst.
- Manchmal werden versteckte Gebühren verlangt, wenn du auf Buttons klickst oder Bestätigungen gibst.



Welche Gefahren gibt es? (Teil 5)

Gefälschte QR-Codes: Welche Gefahren lauern und wie du dich schützen kannst

4. Weiterleitung an echte Seiten (für zusätzlichen Betrug)

- Manche Betrüger-Seiten leiten dich nach dem Datendiebstahl an eine echte Webseite weiter, damit du keinen Verdacht schöpfst.

5. Missbrauch deiner Online-Identität

- Wenn du Zugangsdaten eingibst, könnten diese verwendet werden, um sich in deinen Online-Konten (z. B. E-Mail, soziale Netzwerke oder Bankkonten) einzuloggen und dort weiteren Schaden anzurichten.

Was du sofort tun solltest, wenn du auf eine gefälschte Seite gelangt bist:

1. **Keine Daten eingeben:** Schließe die Webseite sofort.
2. **Überprüfe dein Gerät:** Scanne dein Smartphone oder Tablet mit einer Sicherheits-App.
3. **Passwörter ändern:** Wenn du auf der Webseite etwas eingegeben hast, ändere das Passwort für betroffene Konten so schnell wie möglich.
4. **Bank kontaktieren:** Wenn du Bankdaten eingegeben hast, informiere sofort deine Bank, um mögliche Schäden zu verhindern.
5. **Anzeige erstatten:** Melde den Vorfall der Polizei, damit sie den Betrug untersuchen können.
6. Vorsicht und schnelles Handeln können viel Schaden verhindern!



Welche Gefahren gibt es? (Teil 5)

Phishing-Arten

Es gibt verschiedene Arten von Phishing, die sich in ihrer Vorgehensweise und ihrem Ziel unterscheiden. Hier sind die gängigsten Phishing-Arten:

1. E-Mail-Phishing

- Beschreibung: Klassisches Phishing, bei dem Kriminelle täuschend echte E-Mails senden, die von vertrauenswürdigen Quellen wie Banken, Online Shops oder Behörden zu stammen scheinen.
- Ziel: Benutzer zur Preisgabe von sensiblen Daten wie Passwörtern, Bankinformationen oder Kreditkartendaten verleiten.
- Beispiel: Eine E-Mail von "deiner Bank" mit der Aufforderung, deine Kontodaten zu bestätigen, da das Konto angeblich gesperrt wurde.

2. Spear-Phishing

- Beschreibung: Zielgerichtetes Phishing, das sich an eine bestimmte Person oder Organisation richtet.
- Ziel: Informationen oder Zugang zu sensiblen Systemen zu erhalten, oft für Industriespionage oder Betrug.
- Beispiel: Eine personalisierte E-Mail mit deinem Namen und spezifischen Informationen über deine Arbeit, um Vertrauen zu erwecken.

3. Whaling (CEO-Fraud)

- Beschreibung: Eine spezielle Form des Spear-Phishings, die auf Führungskräfte oder wichtige Entscheidungsträger in Unternehmen abzielt.
- Ziel: Große Geldbeträge zu erbeuten oder vertrauliche Unternehmensdaten zu stehlen.
- Beispiel: Eine gefälschte E-Mail vom „CEO“ an den Finanzleiter mit der Aufforderung, eine dringende Überweisung zu tätigen.

4. Smishing (SMS-Phishing)

- Beschreibung: Phishing-Angriffe, die über SMS oder Instant-Messaging-Dienste wie WhatsApp durchgeführt werden.
- Ziel: Benutzer dazu bringen, auf schädliche Links zu klicken oder persönliche Informationen preiszugeben.
- Beispiel: Eine SMS von "deinem Paketdienst", in der ein Link enthalten ist, um angeblich die Zustellung zu verfolgen.

Welche Gefahren gibt es? (Teil 5)

Phishing-Arten

5. Vishing (Voice-Phishing)

- Beschreibung: Phishing-Angriffe über das Telefon, bei denen Betrüger als Support-Mitarbeiter, Bankangestellte oder Behördenvertreter auftreten.
- Ziel: Opfer dazu bringen, persönliche Daten oder Finanzinformationen am Telefon preiszugeben.
- Beispiel: Ein Anruf von „deiner Bank“, die behauptet, es gäbe unautorisierte Transaktionen, und deine Kartennummer verlangt.

6. Quishing (QR-Code-Phishing)

- Beschreibung: Betrug mit gefälschten QR-Codes, die Benutzer auf schädliche Webseiten weiterleiten.
- Ziel: Zugangsdaten stehlen, Schadsoftware installieren oder sensible Daten abfangen.
- Beispiel: Ein QR-Code auf einem Poster, der angeblich zu einem sicheren Wi-Fi-Netzwerk führt.

7. Clone-Phishing

- Beschreibung: Betrüger erstellen eine Kopie einer legitimen E-Mail (z. B. von einer Bank oder einem Dienstanbieter), ersetzen jedoch die Links durch schädliche.
- Ziel: Benutzer in die Falle locken, da die E-Mail legitim erscheint.
- Beispiel: Eine gefälschte „Rechnung“ von deinem Stromanbieter, die dich auffordert, auf einen Link zu klicken.

8. Pharming

- Beschreibung: Manipulation von DNS-Einstellungen, sodass Benutzer auf gefälschte Webseiten geleitet werden, auch wenn sie die korrekte URL eingeben.
- Ziel: Benutzer zur Eingabe sensibler Informationen auf einer täuschend echten, aber betrügerischen Webseite bewegen.
- Beispiel: Du gibst die URL deiner Bank ein, wirst aber auf eine gefälschte Seite weitergeleitet.

Welche Gefahren gibt es? (Teil 5)

Phishing-Arten

9. Social Media Phishing

- Beschreibung: Betrug auf Social-Media-Plattformen, bei dem Angreifer gefälschte Profile oder Nachrichten verwenden.
- Ziel: Vertrauen erlangen, um persönliche Informationen, Geld oder Zugriff auf Konten zu erhalten.
- Beispiel: Eine Nachricht von einem „Freund“, der angeblich in einer Notlage ist und um Geld bittet.

10. Angler-Phishing

- Beschreibung: Phishing-Angriffe, die auf Support-Anfragen in sozialen Netzwerken abzielen.
- Ziel: Opfer dazu bringen, auf schädliche Links zu klicken oder persönliche Daten anzugeben.
- Beispiel: Eine gefälschte Nachricht von einem "Support-Team" auf Twitter, das dich auffordert, Login-Daten zu teilen.

11. Malvertising (Malicious Advertising)

- Beschreibung: Angriffe über schädliche Online-Werbung.
- Ziel: Benutzer auf gefährliche Webseiten zu leiten oder Malware zu installieren.
- Beispiel: Eine Anzeige, die behauptet, du hast einen Preis gewonnen und deine Daten eingeben musst, um ihn zu erhalten.

12. Pop-up-Phishing

- Beschreibung: Pop-up-Fenster auf Webseiten, die behaupten, dein Computer sei infiziert oder du musst eine Software aktualisieren.
- Ziel: Schadsoftware installieren oder Daten abgreifen.
- Beispiel: Ein Pop-up mit der Warnung „Ihr Computer ist infiziert. Klicken Sie hier, um zu reparieren.“

Jede dieser Phishing-Arten hat das Ziel, Benutzer zu täuschen und vertrauliche Daten zu stehlen. Wachsamkeit und Vorsicht sind entscheidend, um sich zu schützen!

Wie kann man sich gegen Phishing schützen?

Um nicht in eine Phishing-Falle zu geraten und Deine persönlichen Informationen und finanziellen Daten zu schützen, solltest Du folgende bewährte Praktiken beachten:

- Sei skeptisch von wem die Mail ist
- Überprüfe die Absenderadresse
- Klicke nicht auf verdächtige Links
- Achte auf die Grammatik und Rechtschreibung (Das war früher, jetzt werden die Texte dank ChatGPT & Co meistens fehlerfrei geschrieben)
- Verwende sichere Websites
- Nutze Antivirensoftware und Firewalls
- Verwende starke Passwörter
- Sei vorsichtig bei Anrufen
- Verwende Zwei-Faktor-Authentifizierung
- Bilde Dich weiter
- Melde verdächtige Aktivitäten

Indem Du diese bewährten Praktiken befolgst und wachsam bleibst, kannst Du das Risiko, Opfer eines Phishing-Angriffs zu werden, erheblich reduzieren und Deine Online-Sicherheit stärken.

Welche Gefahren gibt es? (Teil 6)

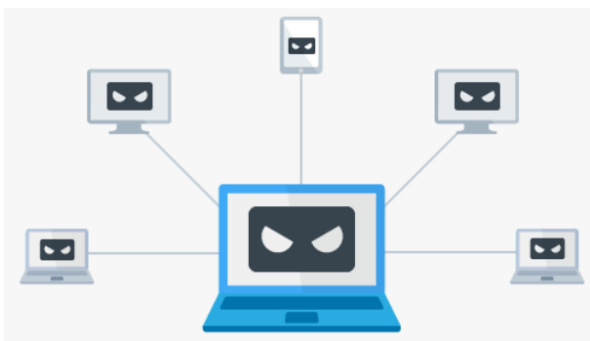


RANSOMSOFTWARE (RAMSOM = LÖSEGELD)

gefährliche Erpresser-Malware.

Blockiert den Computer, um ein Lösegeld zu fordern. Oftmals als FBI oder Polizei „getarnt“.

Beispiel so: „Sie haben illegal eine Software heruntergeladen, dafür müssen Sie eine Strafe zahlen.“



BOTNET (BOT = Robot „Roboter“)

vernetzt Rechner, um andere Systeme aus mehreren Quellen angreifen zu können. Hier werden die Rechen-, Festplatten- und die CPU-Kapazität gebündelt, um ein Super-Computer zu bilden, um z.B. ein Unternehmen anzugreifen.



Jeden Tag werden 30.000 Webseiten von Unternehmen oder Organisationen weltweit gehackt.

Welche Gefahren gibt es? (Teil 7)



KEYLOGGER

„Keylogger“ = *Keystroke Logger* = Tasten-Protokollierer)

Dabei handelt es sich um Überwachungssoftware oder -hardware, die aufzeichnet, was Du schreibst. Dies kann ein Programm auf Deinem Computer oder ein kleines Gerät sein, das an Deinen PC und Deine Tastatur angeschlossen wird und alles verfolgt, was Du tippst.



Basiselemente der IT-Sicherheit

Sie schützt vor Angriffen von außen und verhindert, dass Programme auf dem Gerät, z.B. Spyware, Kontakt zum Internet aufnehmen.

Firewall

Zwei-Faktor-Authentifizierung

Schütze dich zweifach. Neben dem ersten Faktor (Passwort), nutze einen zweiten Schritt, etwa deinen Fingerabdruck oder eine TAN.

Updates

Halte deine Software durch Sicherheitsupdates auf dem neusten Stand.

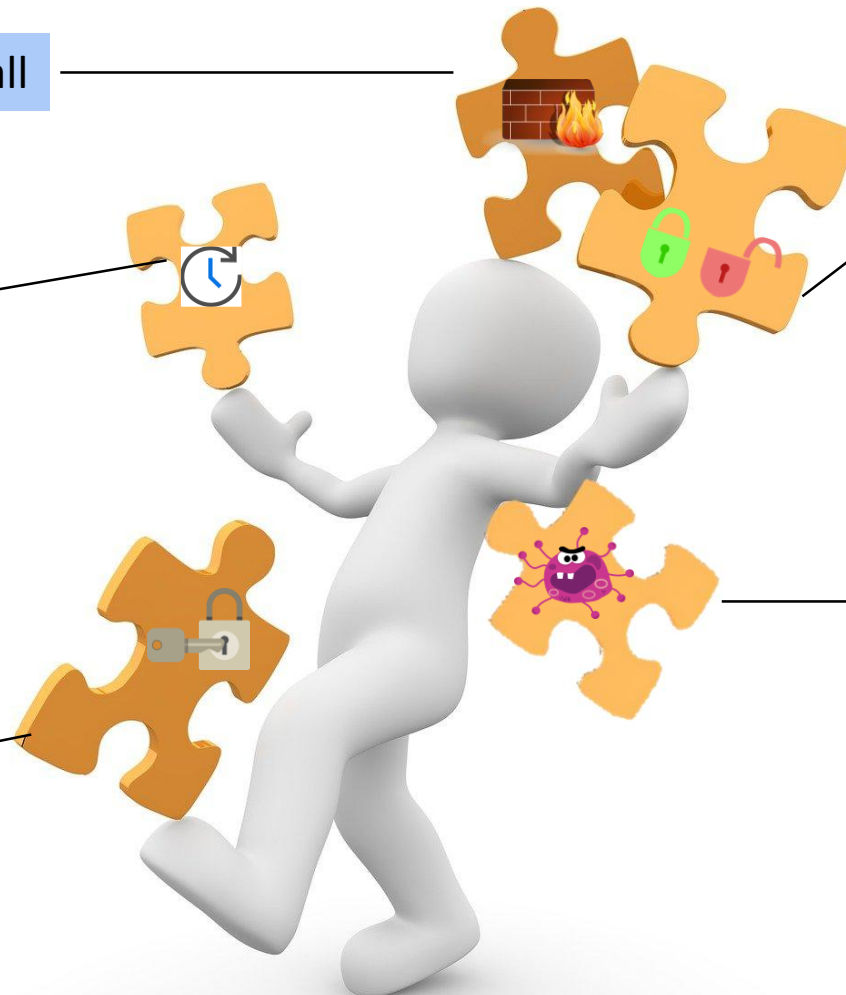
Virenschutz-Software

Die Software überprüft den gesamten Rechner auf Anzeichen einer Infektion

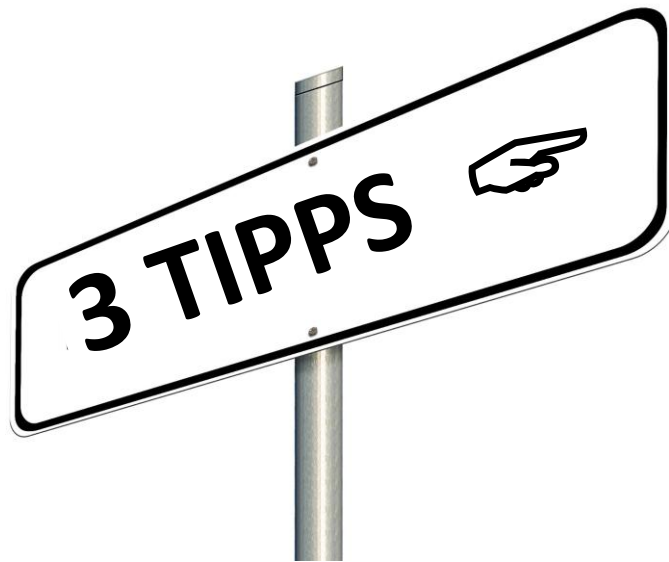
Passwörter

Verwende möglichst starke und unterschiedliche Passwörter.

Häufig vorhandener Schutz auf PCs und Laptops



Sicheres Online-Banking



1

Zugangsdaten sichern

Bewahre Zugangsdaten zum Online-Banking sicher auf.

2

Zwei Geräte nutzen

Die 2-Faktor-Authentifizierung schützt besser, wenn du tatsächlich zwei Geräte verwendest. Mache Banking an PC oder Tablet und hole dir die TANS auf deinem Handy.

3

Limit festlegen

Bei den meisten Girokonten lässt sich ein tägliches Limit für Überweisungen festlegen.

Weiterführende Information zum Nachlesen

Wir wollen, dass Sie sicher leben.
Ihre Polizei
Kompetent. Kostenlos. Neutral.

POLIZEILICHE KRIMINALPRÄVENTION
DER LÄNDER UND DES BUNDES

LEICHTE SPRACHE | ÜBER UNS | PARTNER | NEWSLETTER | KONTAKT

Suche nach Themen, Tipps und Hilfe

STARTSEITE & AKTIONEN | THEMEN & TIPPS | OPFERINFORMATIONEN | MEDIENANGEBOT | PRESSE

Startseite > Themen & Tipps > Gefahren im Internet > Viren und Trojaner

BETRUG
DIEBSTAHL
DROGEN
EINBRUCH
EXTREMISMUS
GEFAHREN IM INTERNET
Abfallen

Viren und Trojaner aussperren

Fast unbemerkt gelangen Viren, Trojaner und andere Schadprogramme auf den Rechner. Mit etwas Vorsicht und passender Software kann jeder seinen Computer und andere digitale Geräte einfach vor Infektionen schützen.

VIRUS CHECK

Vorlesen

<https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/viren-und-trojaner/>

Wie verbreiten sich Viren & Co.?



E-Mail Anhänge – immer noch einer der häufigsten Verbreitungsarten

Beispiel: Klicken Sie auf den Button, um Amazon aufzurufen:



Gefährliche Webseiten - gefährlich vor allem bei Raubkopien und Pornografie



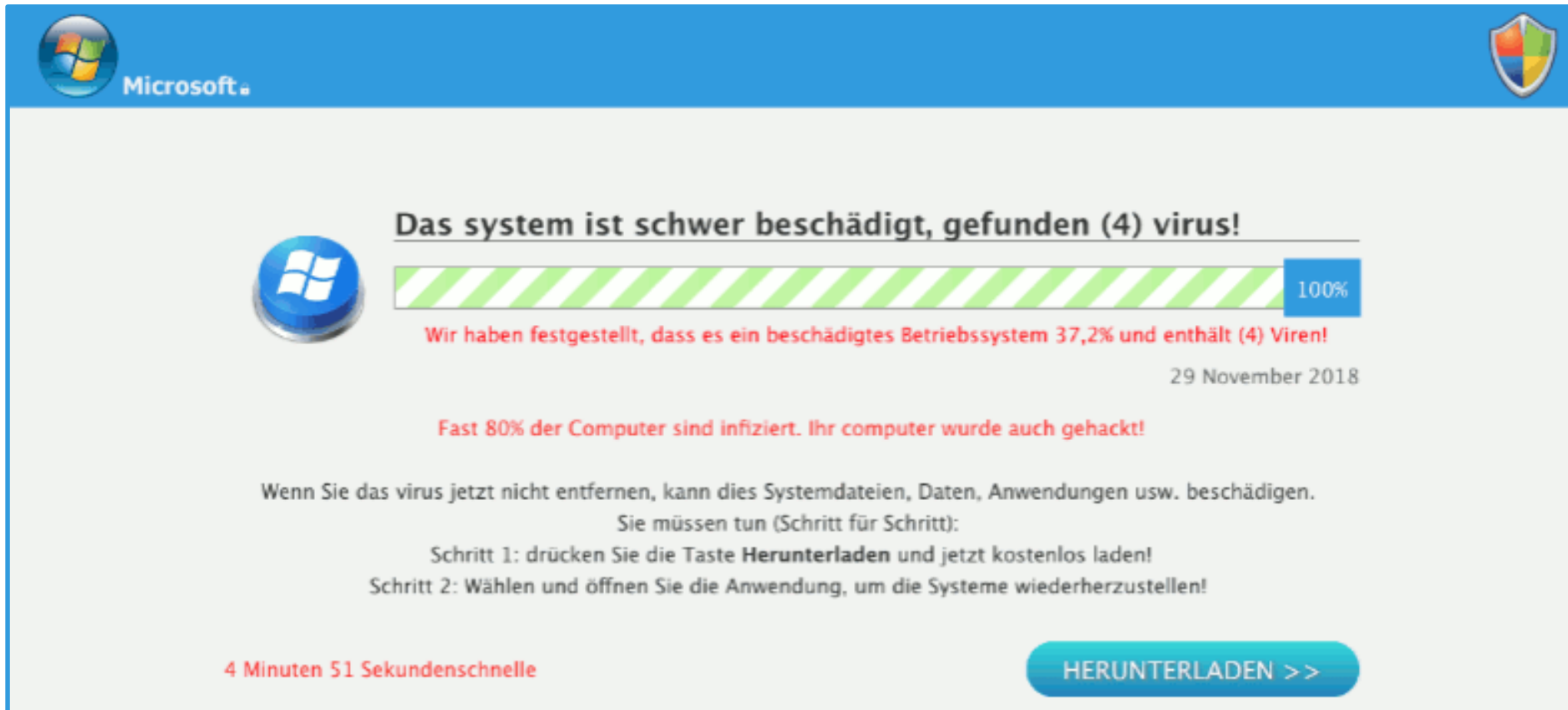
Freies WLAN

Netzwerke – wenn diese nicht ausreichend abgesichert sind, z.B. Internetcafé, WLAN)



Phishingversuche – vor allem E-Mail, Instant Messaging und Social Media

Fake-Virus (1)



Stell dir vor: Auf deinem Bildschirm erscheint dieses animierte Warnfenster. Du kannst es nicht schließen und hast scheinbar nur eine Option: auf „**Herunterladen**“ zu klicken.

Wie reagierst du? Was solltest du jetzt tun – und was auf keinen Fall?

Fake-Virus (2)

Was ist bei Fake-Virus zu tun?

- Ignoriere verdächtige Warnungen im Internet und auf Websites, insbesondere wenn sie unerwartet auftauchen.
- Lade keine Software herunter oder kaufe keine Dienste, die Dir von unbekanntem oder fragwürdigen Quellen angeboten werden.
- Aktualisiere regelmäßig Dein Betriebssystem und Deine Software, um Schwachstellen zu schließen, die von echten Cyberkriminellen ausgenutzt werden.

Wie verbreiten sich Viren & Co.?



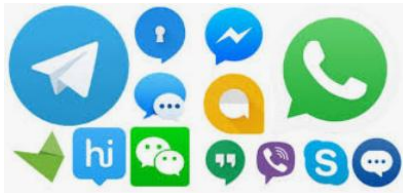
Infizierte Software – Gefahr vor allem bei Raubkopien und fragwürdigen Quellen



Hacker/Cracker - Gefahren eher für Unternehmen und VIPs

Die Telekom registriert bis zu 46 Millionen Cyberangriffe pro Tag

<https://www.tagesspiegel.de/wirtschaft/netzkriminalitaet-die-telekom-registriert-bis-zu-46-millionen-cyberangriffe-pro-tag/24375956.html>



Instant Messaging/Social Media – Oftmals werden Kontakte bzw. Freunde infiziert



Falsche Antivirussoftware – Du liest eine Meldung, dass Dein Rechner infiziert ist...

Wie kann man sich schützen?



Denken – Ist dies wirklich von meiner Bank, von meinem Freund, seriös...?



ZDDK: **Z**uerst **D**enken **D**ann **K**licken

<https://www.mimikama.org>

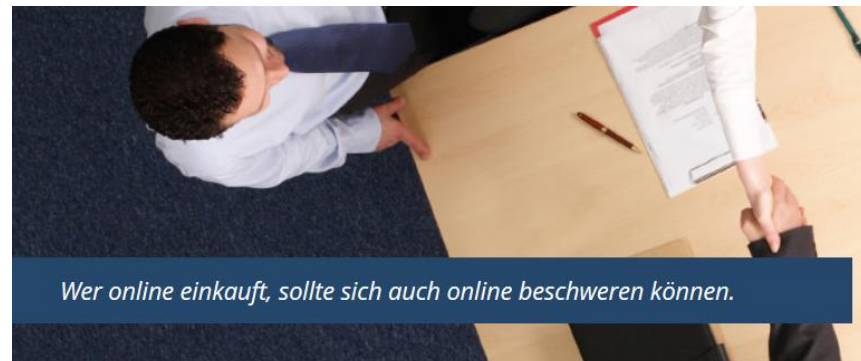
Abonnieren wird empfohlen

Was kannst Du tun,
wenn Du auf einen
Betrüger reingefallen
bist?



Kostenlose Schlichtung und Hilfe bei
Problemen im Internet

<https://ombudsmann.at>



<https://www.online-schlichter.de>

Wie kann man sich schützen?

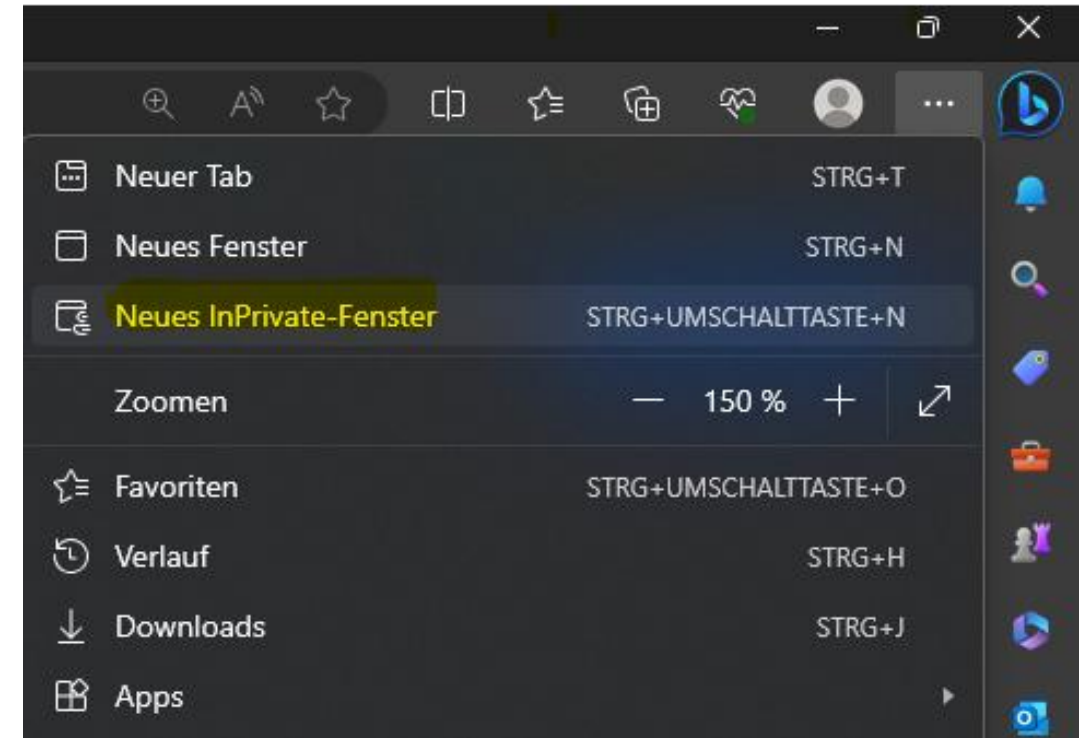
Browsereinstellungen am Beispiel Microsoft Edge

Microsoft Edge bietet verschiedene Funktionen und Einstellungen, um Deine Online-Aktivitäten zu schützen und Deine Privatsphäre zu wahren. Hier sind einige Schritte, die Du unternehmen kannst, um Deine Online-Sicherheit zu erhöhen:

Verwende den InPrivate-Modus

InPrivate ist der private Browsing-Modus von Microsoft Edge. Wenn Du InPrivate verwendest, werden Deine Browsing-Daten wie Verlauf, Cookies und temporäre Dateien nicht gespeichert. Um InPrivate zu starten:

- öffne Microsoft Edge
- klicke auf die drei Punkte oben rechts
- wähle "Neues InPrivate-Fenster"



Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Aktiviere den Tracking-Schutz

Microsoft Edge bietet eine Tracking-Prävention, mit der Du das Sammeln von Daten durch Websites und Werbetreibende einschränken kannst. Du kannst den Tracking-Schutz unter

- Einstellungen
- Datenschutz
- Suche und Dienste
- aktivieren

The screenshot shows the Microsoft Edge settings interface. On the left is a sidebar with 'Einstellungen' at the top, followed by a search bar and a list of categories: Profile, Datenschutz, Suche und Dienste (highlighted), Darstellung, Randleiste, Start, Startseite und neue Registerkarten, Teilen, kopieren und einfügen, Cookies und Websiteberechtigungen, Standardbrowser, Downloads, Family Safety, Sprachen, Drucker, System und Leistung, Einstellungen zurücksetzen, Smartphone und andere Geräte, Barrierefreiheit, and Infos zu Microsoft Edge. The main content area is titled 'Halo Metin, Ihre Privatsphäre ist uns wichtig.' and contains a section for 'Verhindern der Nachverfolgung'. This section includes a toggle for 'Tracking-Verhinderung' which is turned on. Below it are three options: 'Einfach', 'Ausgewogen (Empfohlen)', and 'Streng'. The 'Ausgewogen' option is selected. Below these are sections for 'Blockierte Tracker', 'Ausnahmen', and a toggle for 'Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen'. At the bottom, there is a 'Browserdaten löschen' section with a button to 'Browserdaten jetzt löschen' and a link to 'Zu löschende Elemente auswählen'.

Einstellungen

Einstellungen durchsuchen

- Profile
- Datenschutz, Suche und Dienste**
- Darstellung
- Randleiste
- Start, Startseite und neue Registerkarten
- Teilen, kopieren und einfügen
- Cookies und Websiteberechtigungen
- Standardbrowser
- Downloads
- Family Safety
- Sprachen
- Drucker
- System und Leistung
- Einstellungen zurücksetzen
- Smartphone und andere Geräte
- Barrierefreiheit
- Infos zu Microsoft Edge

Hallo Metin, Ihre Privatsphäre ist uns wichtig.
Wir schützen und respektieren Ihre Privatsphäre, und bieten Ihnen gleichzeitig die Transparenz und Kontrolle, die Sie verdienen. [Weitere Informationen zu unseren Bemühungen in Sachen Datenschutz](#)

Verhindern der Nachverfolgung ?

Websites verwenden Tracker, um Informationen über Ihr Surfverhalten zu sammeln. Websites nutzen diese Informationen unter Umständen, um Verbesserungen durchzuführen und Inhalte wie personalisierte Werbeanzeigen anzuzeigen. Einige Tracker sammeln und senden Ihre Informationen an Websites, die Sie nicht besucht haben.

Tracking-Verhinderung

Einfach	Ausgewogen (Empfohlen)	Streng
<ul style="list-style-type: none">• Lässt die meisten Tracker auf allen Websites zu• Inhaltsinformationen und Werbeanzeigen werden wahrscheinlich personalisiert• Websites werden wie erwartet funktionieren.• Blockiert bekannte schädliche Tracker	<ul style="list-style-type: none">• Blockiert Tracker von Websites, die Sie nicht besucht haben• Inhalte und Werbeanzeigen sind wahrscheinlich weniger stark personalisiert• Websites werden wie erwartet funktionieren.• Blockiert bekannte schädliche Tracker	<ul style="list-style-type: none">• Blockiert die meisten Tracker von allen Websites• Inhalt und Anzeigen verfügen wahrscheinlich über eine minimale Personalisierung• Teile von Websites funktionieren möglicherweise nicht.• Blockiert bekannte schädliche Tracker

Blockierte Tracker >
Websites anzeigen, für die das Tracking blockiert wurde

Ausnahmen >
Alle Tracker auf Websites zulassen, die Sie auswählen

Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen

Browserdaten löschen

Hierzu zählen Verlauf, Kennwörter, Cookies und mehr. Nur Daten aus diesem Profil werden gelöscht. [Verwalten Sie Ihre Daten.](#)

Browserdaten jetzt löschen Zu löschende Elemente auswählen

Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Passwort-Manager verwenden

Edge verfügt über einen integrierten Passwort-Manager, der sichere Passwörter erstellen und speichern kann. Verwende ihn, um sichere Passwörter für Deine Online-Konten zu erstellen und zu verwalten.

Wenn Du Dich auf einer Website anmeldest und ein Passwort eingibst, fragt Edge, ob Du das Passwort speichern möchtest. Du können "Ja" auswählen, um es zu speichern.

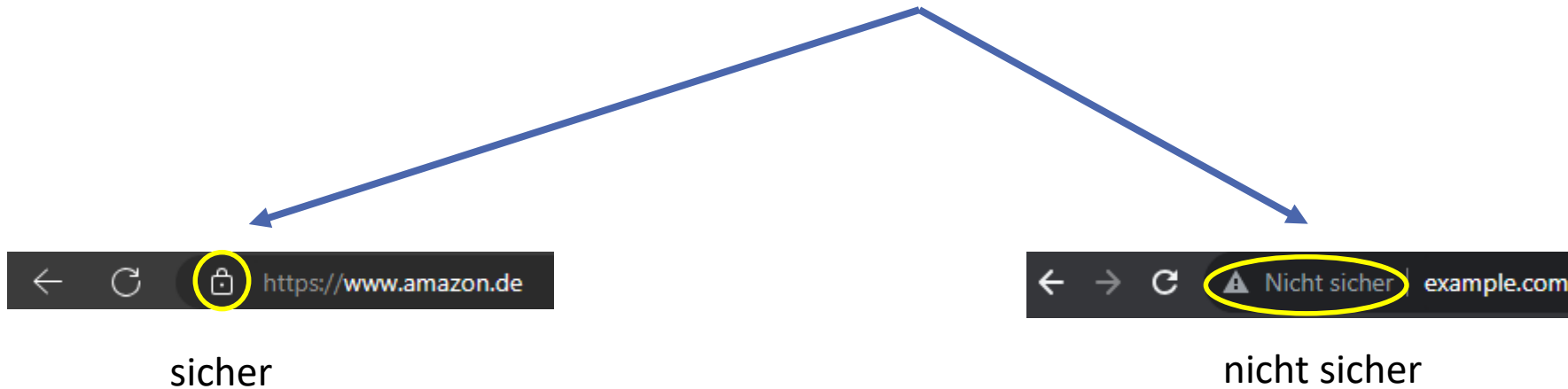


Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Sicherheitszertifikate überprüfen

Achten auf das Schlosssymbol in der Adressleiste von Edge, wenn Du sensible Informationen wie Kreditkartendaten eingibst. Das Schloss zeigt an, dass die Website eine sichere Verbindung verwendet.



Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Browser-Updates durchführen

Stelle sicher, dass Du immer die neueste Version von Microsoft Edge verwendest, da Updates häufig Sicherheitsverbesserungen enthalten.

The screenshot shows the Microsoft Edge settings application. The left sidebar contains various settings categories, with 'Einstellungen' (Settings) at the top and 'Infos zu Microsoft Edge' (Info about Microsoft Edge) at the bottom, both highlighted with yellow circles. The main content area is titled 'Info' and displays the following information:

- Microsoft Edge** (Version 117.0.2045.36 (Offizielles Build) (64-Bit))
- A notification: **Microsoft Edge ist auf dem neuesten Stand.** (Microsoft Edge is up to date.)
- A toggle for **Updates über getaktete Verbindungen herunterladen** (Download updates over metered connections), which is currently turned off.
- Text: Updates über getaktete Netzwerke automatisch herunterladen (z. B. ein Mobilfunknetz) und beim Neustart des Browsers anwenden. Es können Gebühren anfallen.
- Text: Die Verwendung dieses Browsers wird durch das Open-Source-Projekt [Chromium](#) und andere [Open-Source-Software](#) ermöglicht.
- Text: Microsoft Edge © 2023 Microsoft Corporation. Alle Rechte vorbehalten.
- Links: [Nutzungsbedingungen](#) - [Datenschutzbestimmungen](#) - [Microsoft-Servicevertrag](#)
- Microsoft Edge Insider** section with a button **Mehr erfahren** (Learn more).
- Text: **Sehen Sie, was als nächstes kommt! Laden Sie noch heute einen beliebigen Microsoft Edge-Vorschaukanal herunter.**
- Three options for the Insider program:
 - Seien Sie einer der Ersten, der sieht, was es Neues gibt** (Be one of the first to see what's new). Description: Probieren Sie die neuen Features in Microsoft Edge aus, bevor sie für die breite Öffentlichkeit freigegeben werden.
 - Treten Sie der Microsoft Edge Insider-Community bei** (Join the Microsoft Edge Insider community). Description: Bringen Sie sich ein und beteiligen Sie sich am Microsoft Edge-Team, um Fehler zu melden, frühes Feedback zu geben und Ideen zu diskutieren.
 - Finden Sie den richtigen Vorschaukanal für Sie** (Find the right preview channel for you). Description: Wir bieten drei Vorschaukanäle an: Beta, Dev und Canary. Sie können alle auf demselben Gerät installiert werden, und bei der Installation wird die veröffentlichte Version von Microsoft Edge, die Sie gerade verwenden, nicht deinstalliert.

Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Vorsicht beim Herunterladen

Lade keine Dateien oder Software von unsicheren oder unbekanntem Quellen herunter.

Edge wird Dich normalerweise warnen, wenn Du eine potenziell unsichere Datei herunterladen möchtest.

Auch Deine Antiviren-Software überprüft die Datei, ob sie virenfrei ist.

Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Deaktiviere ungenutzte Erweiterungen

Überprüfe regelmäßig Deine installierten Browsererweiterungen und deaktiviere oder entferne ungenutzte oder verdächtige Erweiterungen.



Werbung blockieren: Die Erweiterung analysiert die Inhalte einer Website, während Du sie besuchst, und erkennt Werbeanzeigen, Tracking-Skripte und Pop-ups.

Benutzerdefinierte Filter: Sie ermöglicht es dem Benutzer, benutzerdefinierte Filterregeln festzulegen, um bestimmte Anzeigen oder Elemente auf bestimmten Websites zu blockieren oder zuzulassen.

Weißliste: Benutzer können bestimmte Websites auf eine "Weißliste" setzen, um Anzeigen auf diesen Websites zu unterstützen.

Statistiken anzeigen: Die Erweiterung bietet möglicherweise Statistiken, wie viele Anzeigen sie blockiert hat, um dem Benutzer Einblick in ihre Wirksamkeit zu geben.

Aktualisierungen: Die Filterlisten der Erweiterung werden regelmäßig aktualisiert, um neue Werbenetzwerke und -methoden abzudecken.

Benachrichtigungen: Die Erweiterung kann Benachrichtigungen anzeigen, wenn sie Anzeigen oder Tracking-Aktivitäten blockiert, um dem Benutzer Feedback zu geben.

Optionen und Einstellungen: Sie ermöglicht es Benutzern, Einstellungen wie den Grad des Blockierens von Anzeigen und den Datenschutzmodus anzupassen.

Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Verwende ein sicheres Netzwerk

Stellen sicher, dass Du Dich nur in vertrauenswürdigen und sicheren WLAN-Netzwerken anmeldest. Öffentliche WLANs sind oft unsicher und könnten Deine Daten gefährden.



Wie kann man sich schützen?

Browsereinstellungen am Beispiel Microsoft Edge

Verwende ein VPN (Virtual Private Network)

Ein VPN kann Deine Online-Aktivitäten verschlüsseln und Deine Identität im Internet schützen. Du kannst ein VPN-Dienst abonnieren und in Microsoft Edge konfigurieren.



VPN – Vor- und Nachteile

Vorteile eines VPN

- Schutz der Privatsphäre
 - Die IP-Adresse wird verschleiert, wodurch du im Internet anonym unterwegs bist.
 - Websites und Dienste können deinen Standort und deine Identität schwerer nachverfolgen.
- Verschlüsselung der Daten
 - Besonders bei öffentlichem WLAN (z. B. im Café oder Hotel) werden deine Daten vor Hackern geschützt.
- Umgehung von Geoblocking
 - Zugriff auf Inhalte, die in bestimmten Ländern gesperrt sind (z. B. Streaming-Dienste wie Netflix, BBC, etc.).
- Zugang zu gesperrten Seiten
 - In Ländern mit starker Zensur kannst du mithilfe eines VPNs gesperrte Inhalte erreichen (z. B. soziale Medien, Nachrichtenseiten).
- Sicheres Arbeiten im Homeoffice
 - Firmen-VPNs ermöglichen einen geschützten Zugang auf interne Netzwerke und Daten.

Nachteile eines VPN

- Langsamere Internetgeschwindigkeit
 - Durch die Umleitung des Datenverkehrs über VPN-Server kann es zu Verzögerungen kommen.
- Vertrauenswürdigkeit des VPN-Anbieters
 - Nicht jeder Anbieter hält seine Versprechen. Einige loggen Nutzerdaten trotz gegenteiliger Behauptungen.
- Komplexität für Einsteiger
 - Für unerfahrene Nutzer kann die Einrichtung verwirrend sein, besonders bei manuellen Setups.
- Nicht jede App/Webseite lässt VPNs zu
 - Manche Dienste blockieren bekannte VPN-Server (z. B. Netflix, Banking-Apps).
- Kosten
 - Gute VPNs kosten Geld. Gratis-VPNs sind oft eingeschränkt oder unsicher.

Wie kann man sich schützen?

- **Passwort Schutz** – Komplexe Passwörter oder Passwort Manager verwenden, nicht die gleichen Passwörter verwenden
- **Updates** – Nicht nur Windows, sondern gesamte Software aktuell halten (z.B. Java, Office, Virenschutz uvm. (Keine win95, 98, XP, etc. für die es keine Sicherheitsupdates gibt)
- **Nachfragen** – IT Abteilung oder der Fachmann Deiner Wahl kennt (hoffentlich) die Antwort
- **USB-Stick** – Daten verschlüsseln, Virus Scan vor dem Öffnen, keine fremden USB Sticks anstecken und nur in geschützten PCs verwenden...
- **Sicherung** –Sichern der Daten auf externem Speicher bzw. in der Cloud
Achtung: Haltbarkeit bedenken (2-5 Jahre)
- **Office Files** – Gefahr vor Makro Viren kennen und verhindern
=> DOCX, XLSX, PPTX: keine Makros
=> DOCM, XLSM, PPTM Dateien, die Makros enthalten und werden sofort ausgeführt
- **Computerschutz** – Antivirus, Internet Security, Komplet Security



Wie kann man sich schützen?

- **Komplettschutz für den Computer** – Nicht nur ein Virenprogramm, sondern eine Software, die alle in den vorigen Seiten aufgezählten Schädlinge und für ein sicheres Surfen im Internet sorgt. Am besten 10-er Paket für alle anderen Geräte wie z.B. Handy, Tablet, Laptops, etc. Nicht im Laden, sondern im Internet einkaufen.
- **Sicheres Passwort** – Die größten Fehler bei Passwörtern sind:
 - Ein Passwort für alles
 - Zu einfache Passwörter (1234, 0815, 4711, qwertz, passwort1, Namen, Geburtsdatum, einfache Wörter, etc.)
 - Ein persönlicher Bezug (leicht zu erraten)
 - Auf einen Zettel schreiben (unter der Tastatur oder in Schublade)
 - Passwörter über Jahre verwenden
 - Zu kurzes Passwort, z.B. 5 Zeichen/1 Stunde
 - Umlaute in Passwörter (Macht Hackern schwer, Passwörter zu knacken. Aber an den nächsten Urlaub denken!)
 - Passwörter in Browser bzw. auf PC speichern



Wie kann man sich schützen?

Wie erstellt man sichere Passwörter?

- Mindestens 16-18 Zeichen, um so länger.
- Sonderzeichen, Groß/Kleinbuchstaben, Zahlen
- Eselsbrücken, Sprichwörter oder Motto

Beispiel: Kleider machen Leute. Die Ausnahme bestätigt die Regel. Oder?

Passwort= KmL.DAbdR.O?

Buchstaben durch andere Zeichen ersetzen, wie z.B. s=\$, e=3, L=7 selbst solche Zeichen ausdenken

- Passwortmanager nutzen, aber richtig (wenn man sehr viele Passwörter hat. Es muss ein absolut sicheres Passwort und durch Fingerabdruck gesichert sein.)



Datenschutz

Neugier der Internetkonzerne zügeln

- Decke auf, was Google über Dich weiß
- Schalte die neugierige Google-Dienste ab
- Nutze nur die wirklich benötigten Dienste
- Was speichert Microsoft, Facebook und Amazon über Dich



Unermesslicher Datenhunger

Auf der ganzen Welt betreibt Google Rechenzentren, in denen das Unternehmen Daten über die Nutzer seiner Angebote speichert.

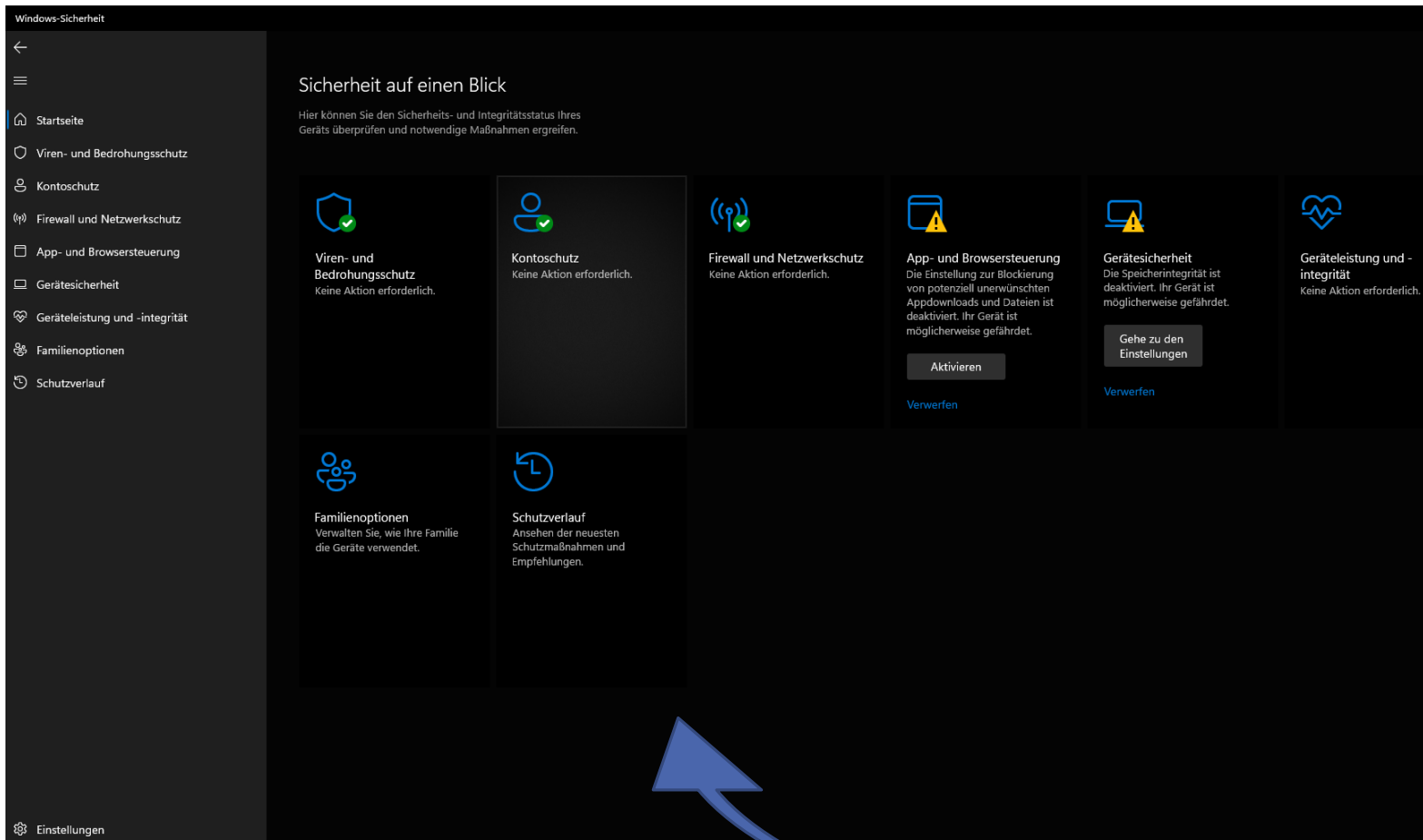
Google sammelt normalerweise Daten wie:

1. **Suchverlauf:** Die Suchbegriffe, die Du in die Google-Suchleiste eingibst.
2. **Standortverlauf:** Wenn Du den Standortverlauf aktiviert hast, kann Google Informationen über Orte, die Du besuchst, speichern.
3. **YouTube-Nutzung:** Wenn Du YouTube-Videos ansiehst oder hochlädst, werden diese Aktivitäten mit Deinem Konto verknüpft.
4. **Google Maps-Nutzung:** Informationen über Orte, die Du auf Google Maps suchst oder besuchst.
5. **Gmail-Daten:** Inhalte und Metadaten von E-Mails, die Du über Gmail sendest und empfängst.
6. **Android-Nutzung:** Wenn Du ein Android-Gerät verwendest, kann Google Informationen über App-Nutzung, Geräteaktivitäten und mehr sammeln.
7. **Google Kalender:** Wenn Du Google Kalender verwendest, werden Termine und Ereignisse gespeichert.
8. **Chrome-Browser:** Wenn Du den Chrome-Browser verwendest, kann Google Informationen über Deine Browsing-Aktivitäten sammeln, sofern Du mit einem Google-Konto angemeldet bist.

Es ist wichtig zu beachten, dass Google in der Regel die Möglichkeit bietet, diese Daten zu verwalten und zu löschen. Du kannst Deine Datenschutzeinstellungen in deinem Google-Konto anpassen, um festzulegen, welche Informationen gesammelt werden dürfen.

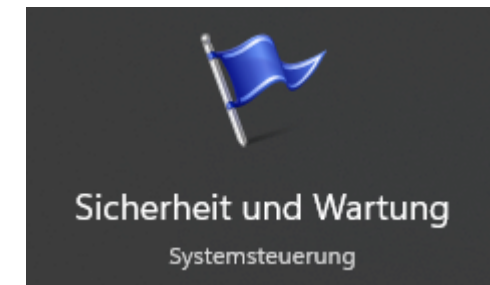
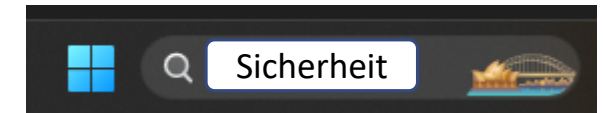
Um herauszufinden, welche Informationen Google über Dich gespeichert hat, kannst Du Dich in Dein Google-Konto einloggen und die Datenschutzeinstellungen überprüfen. Du findest dort oft Funktionen zum Herunterladen oder Löschen von Daten, die Google über Dich gesammelt hat. Beachte jedoch, dass dies nur für die Daten gilt, die mit dem jeweiligen Google-Konto verknüpft sind, mit dem Du angemeldet bist.

Sicherheitseinstellungen meines Computers (Windows 11)



So rufst Du die Seite auf:

Suche nach „Sicherheit“



Virenschutz

In Windows-Sicherheit anzeigen

Die Sicherheitseinstellungen von Windows 11 sind entscheidend, um Dein System vor potenziellen Bedrohungen zu schützen. Hier sind einige grundlegende Sicherheitsrichtlinien, die du beachten kannst:

1. **Windows-Updates**

Stelle sicher, dass Windows Update aktiviert ist, um die neuesten Sicherheitspatches und Updates zu erhalten. Automatische Updates sind empfohlen, um sicherzustellen, dass Dein System stets geschützt ist.

2. **Benutzerkontensteuerung (UAC)**

Die UAC stellt sicher, dass bestimmte Änderungen am System nur mit Deiner Zustimmung durchgeführt werden. Du kannst die UAC-Einstellungen in den Systemsteuerungen anpassen.

3. **Windows Defender Antivirus**

Windows 11 enthält den Windows Defender Antivirus, der in der Regel standardmäßig aktiviert ist. Stelle sicher, dass er auf dem neuesten Stand ist und führe regelmäßige Scans durch.

4. **Firewall**

Überprüfe die Einstellungen der Windows-Firewall, um sicherzustellen, dass sie aktiviert ist. Du kannst den Zugriff für bestimmte Anwendungen steuern und eingehenden Datenverkehr überwachen.

5. **BitLocker**

BitLocker ist eine Funktion für die Festplattenverschlüsselung, die in einigen Editionen von Windows 11 verfügbar ist. Damit kannst Du deine Daten auf der Festplatte vor unbefugtem Zugriff schützen.

6. **Windows Hello**

Nutze Windows Hello, um eine biometrische Authentifizierung (Gesichtserkennung oder Fingerabdruck) für die Anmeldung zu verwenden, wenn dein Gerät diese Funktionen unterstützt.

7. **App-Berechtigungen**

Überprüfe die Berechtigungen, die von installierten Apps angefordert werden. Du kannst dies in den Einstellungen unter "Datenschutz" überprüfen und festlegen, welche Apps auf welche Daten zugreifen dürfen.

8. **Windows-Sicherheit (Defender Security Center)**

Überwache regelmäßig das Windows-Sicherheitscenter, um sicherzustellen, dass keine Sicherheitsprobleme vorliegen. Du kannst es öffnen, indem Du in die "Einstellungen" gehst und zu "Update und Sicherheit" -> "Windows-Sicherheit" navigierst.

9. **Phishing-Schutz und SmartScreen**

Aktiviere den Phishing-Schutz und SmartScreen-Filter in Microsoft Edge, um vor schädlichen Websites geschützt zu sein.

10. **Cortana und Datenschutz**

Wenn Du Cortana nutzt, überprüfe die Datenschutzeinstellungen und passe sie nach Deinen Vorlieben an.

11. **Gastkonto**

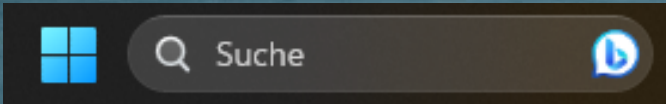
Falls Du Deinen Computer mit anderen teilst, erstelle separate Benutzerkonten und aktiviere kein Gastkonto. Dadurch werden die persönlichen Daten besser geschützt.

Es ist wichtig zu beachten, dass die genaue Vorgehensweise je nach der Windows 11-Version und den verfügbaren Funktionen variieren kann. Daher ist es ratsam, die Dokumentation von Microsoft zu konsultieren oder die neuesten Anleitungen online zu überprüfen.

Praxis



Übungen mit der Windows-Suche



Auf einem Windows-Computer arbeitet die Suchfunktion unten auf der Leiste mit künstlicher Intelligenz, kurz KI. Microsoft hat eine Funktion namens "Windows Search" eingebaut, die auf besonderen Computertechniken wie maschinellem Lernen und speziellen Rechenregeln basiert. Das hilft dabei, die Suche nach Dingen auf dem Computer schlauer und besser zu machen.

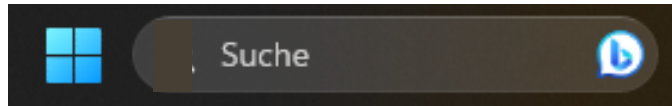
Aufgaben

1. Finde heraus, welche Schlagwörter du verwenden kannst, um das Desktop Hintergrundbild zu ändern.
2. Wonach musst du suchen, wenn du auf dem Rechner ein neues Benutzerkonto einrichten möchtest?
3. Finde heraus, mit welcher Windows Version du arbeitest.



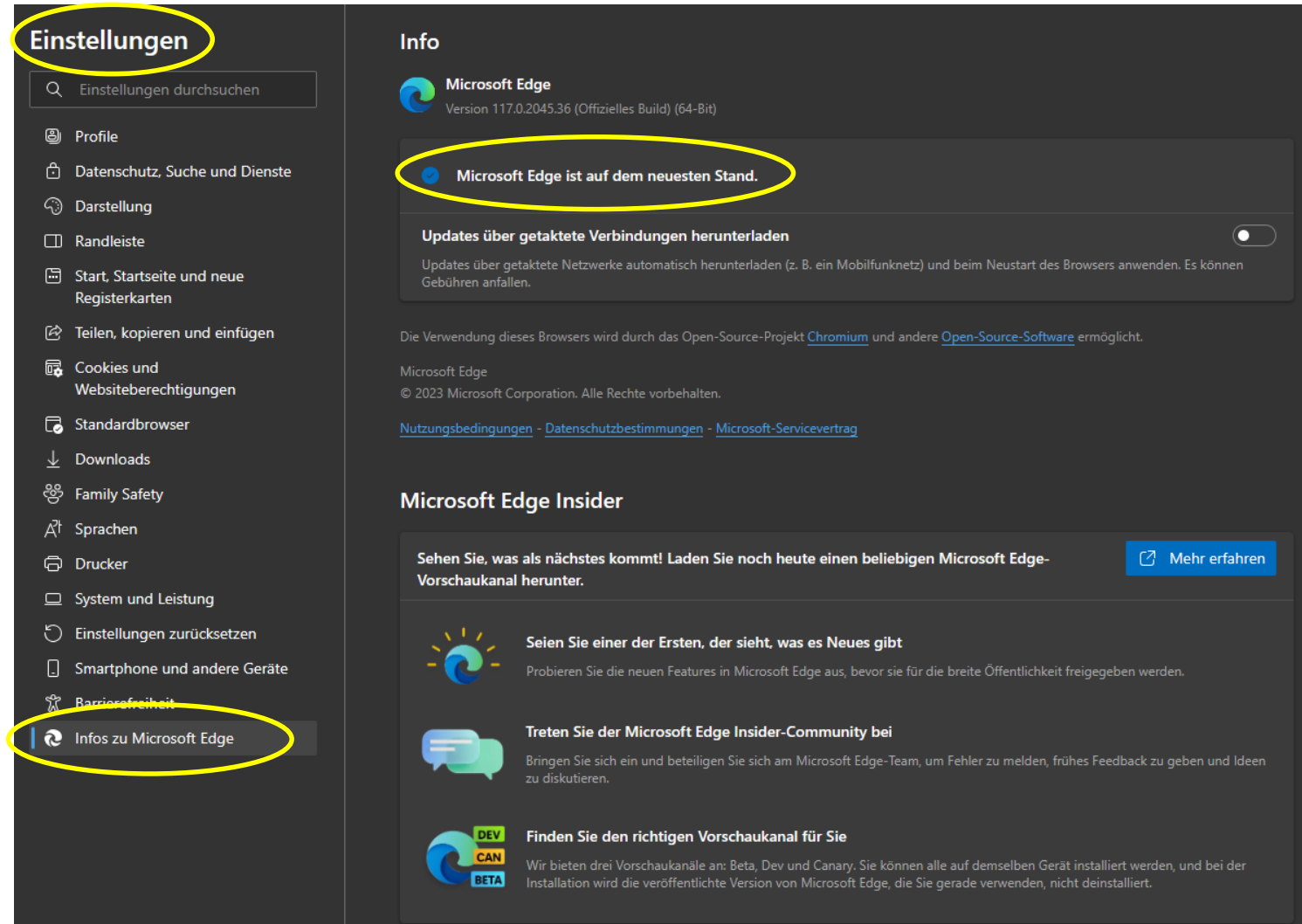
Überprüfe, ob dein Browser Microsoft Edge aktualisiert werden muss

Wonach musst du suchen?



Browser-Updates durchführen

Stelle sicher, dass du immer die neueste Version von Microsoft Edge verwendest, da Updates häufig Sicherheitsverbesserungen enthalten.



Einstellungen

- Einstellungen durchsuchen
- Profile
- Datenschutz, Suche und Dienste
- Darstellung
- Randleiste
- Start, Startseite und neue Registerkarten
- Teilen, kopieren und einfügen
- Cookies und Websiteberechtigungen
- Standardbrowser
- Downloads
- Family Safety
- Sprachen
- Drucker
- System und Leistung
- Einstellungen zurücksetzen
- Smartphone und andere Geräte
- Barrierefreiheit
- Infos zu Microsoft Edge**

Info

Microsoft Edge
Version 117.0.2045.36 (Offizielles Build) (64-Bit)

Microsoft Edge ist auf dem neuesten Stand.

Updates über getaktete Verbindungen herunterladen

Updates über getaktete Netzwerke automatisch herunterladen (z. B. ein Mobilfunknetz) und beim Neustart des Browsers anwenden. Es können Gebühren anfallen.

Die Verwendung dieses Browsers wird durch das Open-Source-Projekt [Chromium](#) und andere [Open-Source-Software](#) ermöglicht.

Microsoft Edge
© 2023 Microsoft Corporation. Alle Rechte vorbehalten.
[Nutzungsbedingungen](#) - [Datenschutzbestimmungen](#) - [Microsoft-Servicevertrag](#)

Microsoft Edge Insider

Sehen Sie, was als nächstes kommt! Laden Sie noch heute einen beliebigen Microsoft Edge-Vorschaukanal herunter. [Mehr erfahren](#)

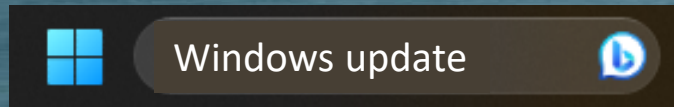
Seien Sie einer der Ersten, der sieht, was es Neues gibt
Probieren Sie die neuen Features in Microsoft Edge aus, bevor sie für die breite Öffentlichkeit freigegeben werden.

Treten Sie der Microsoft Edge Insider-Community bei
Bringen Sie sich ein und beteiligen Sie sich am Microsoft Edge-Team, um Fehler zu melden, frühes Feedback zu geben und Ideen zu diskutieren.

Finden Sie den richtigen Vorschaukanal für Sie
Wir bieten drei Vorschaukanäle an: Beta, Dev und Canary. Sie können alle auf demselben Gerät installiert werden, und bei der Installation wird die veröffentlichte Version von Microsoft Edge, die Sie gerade verwenden, nicht deinstalliert.

Überprüfe, ob dein Betriebssystem auf dem neuesten Stand ist

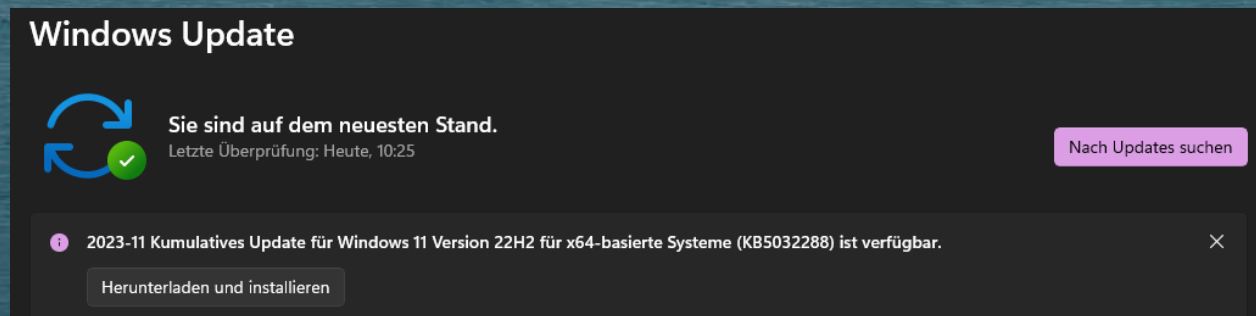
1 Schreibe in der Ecke unten links in die Suche



2



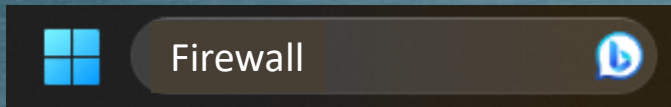
3

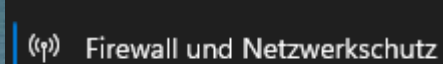


Das regelmäßige Aktualisieren des Windows-Betriebssystems ist entscheidend, um die Sicherheit und Stabilität des Computers zu gewährleisten. Updates enthalten wichtige Patches, um Sicherheitslücken zu schließen, Schadsoftware zu bekämpfen und potenzielle Angriffspunkte für Cyberkriminelle zu minimieren. Darüber hinaus verbessern Updates oft die Leistung, beheben Fehler und bieten neue Funktionen, die die Gesamterfahrung mit dem Betriebssystem optimieren.

Firewall Einstellungen prüfen

1 Schreibe in der Ecke unten links in die Suche



2 Klicke auf 

3 Schalte die Firewall ein oder aus:
Du kannst die Firewall für private
und öffentliche Netzwerke separat
aktivieren oder deaktivieren.

4 Speichere deine Änderungen:
Vergiss nicht, die Änderungen zu speichern,
nachdem du die Einstellungen angepasst hast.

Was ist Firewall?

Eine Firewall ist wie ein digitaler Sicherheitsdienst für deinen Computer oder dein Netzwerk. Sie überwacht den Datenverkehr zwischen deinem Gerät und dem Internet und entscheidet, welche Informationen durchgelassen werden dürfen und welche blockiert werden sollen. Die Firewall schützt so vor unerwünschten oder schädlichen Zugriffen aus dem Internet, ähnlich wie eine Schranke, die nur autorisierten Verkehr passieren lässt und unbefugten Zugang verwehrt.

Ist es zu empfehlen, die Firewall für private und öffentliche Netzwerke aktivieren?

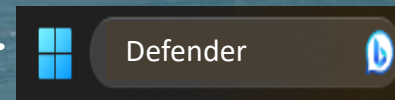
Auf jeden Fall! Die Firewall schützt deinen Computer vor böswilligen Angriffen, indem sie den Datenverkehr überwacht und kontrolliert. Es ist ratsam, die Firewall sowohl für private (zuhause, im Büro) als auch für öffentliche Netzwerke (Cafés, Flughäfen) einzuschalten, um deine Daten in verschiedenen Umgebungen zu sichern.

Windows Defender Einstellungen prüfen

Um Windows Defender zu aktivieren:

1. Öffne die "Einstellungen" über das Windows-Symbol.
2. Gehe zu "Update und Sicherheit".
3. Wähle "Windows-Sicherheit".
4. Überprüfe, ob Windows Defender auf "Ein" steht.

Alternativ:



Wenn du andere Antivirensoftware deaktivieren möchtest:

1. Deaktiviere die installierte Antivirensoftware.
2. Gehe zu "Windows-Sicherheit" in den Einstellungen.
3. Stelle sicher, dass Windows Defender aktiviert ist oder aktiviere es manuell in den "Einstellungen verwalten" unter "Viren- & Bedrohungsschutz".

Diese Schritte können je nach Windows-Version leicht variieren.

Was ist Windows Defender?

Windows Defender ist die eingebaute Antiviren- und Sicherheitssoftware von Microsoft für Windows. Es bietet Schutz vor Viren, Malware und anderen Bedrohungen, arbeitet im Hintergrund in Echtzeit, aktualisiert sich automatisch und integriert grundlegende Firewall-Funktionen. Es ist benutzerfreundlich und erfordert normalerweise keine separate Installation.

Sollte ich Windows Defender oder eine andere Antivirensoftware nutzen?

Windows Defender ist eine integrierte Antiviren- und Sicherheitssoftware von Microsoft für Windows. Es bietet grundlegenden Schutz vor Viren und Malware, erfordert keine separate Installation und wird automatisch aktualisiert. Die Entscheidung, es zu verwenden oder eine andere Antivirensoftware zu wählen, hängt von persönlichen Vorlieben und spezifischen Sicherheitsanforderungen ab. Einige Drittanbieter-Programme bieten erweiterte Funktionen, während Windows Defender eine benutzerfreundliche und kostenfreie Option darstellt. Unabhängig von der Wahl ist regelmäßiges Update und sicheres Online-Verhalten entscheidend für einen effektiven Schutz.

Surfen im Internet, ohne spuren zu hinterlassen

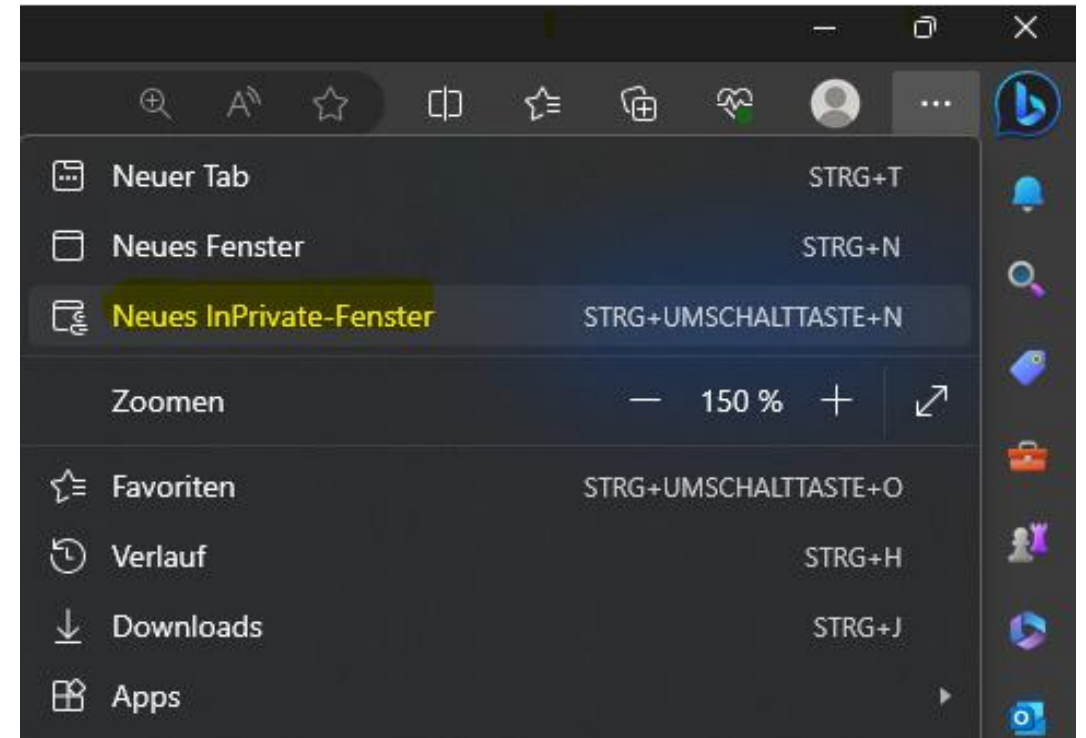
Browsereinstellungen am Beispiel Microsoft Edge

Microsoft Edge bietet verschiedene Funktionen und Einstellungen, um Deine Online-Aktivitäten zu schützen und Deine Privatsphäre zu wahren. Hier sind einige Schritte, die Du unternehmen kannst, um Deine Online-Sicherheit zu erhöhen:

Verwende den InPrivate-Modus

InPrivate ist der private Browsing-Modus von Microsoft Edge. Wenn Du InPrivate verwendest, werden Deine Browsing-Daten wie Verlauf, Cookies und temporäre Dateien nicht gespeichert. Um InPrivate zu starten:

- 1 Öffne Microsoft Edge
- 2 Klicke auf die drei Punkte oben rechts
- 3 Wähle "Neues InPrivate-Fenster"



Tracking Schutz

Browsereinstellungen am Beispiel Microsoft Edge

Aktiviere den Tracking-Schutz

Der Tracking-Schutz (auch als "Tracking Prevention" bezeichnet) bezieht sich auf Funktionen, die entwickelt wurden, um Benutzer vor unerwünschtem Tracking beim Surfen im Internet zu schützen. Tracking bezieht sich auf die Praxis, dass Websites und Werbetreibende Informationen über Dein Online-Verhalten sammeln, um Dein Nutzerverhalten zu analysieren und Dir gezielte Werbung anzuzeigen.

Microsoft Edge bietet eine Tracking-Prävention, mit der Du das Sammeln von Daten durch Websites und Werbetreibende einschränken kannst. Du findest den Tracking-Schutz unter:

- 1 Einstellungen
- 2 Datenschutz
- 3 Suche und Dienste
- 4 aktivieren

Diese Schritte können je nach Windows-Version leicht variieren.

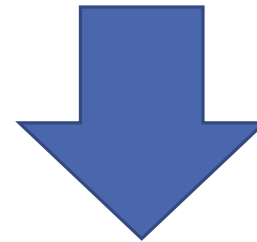
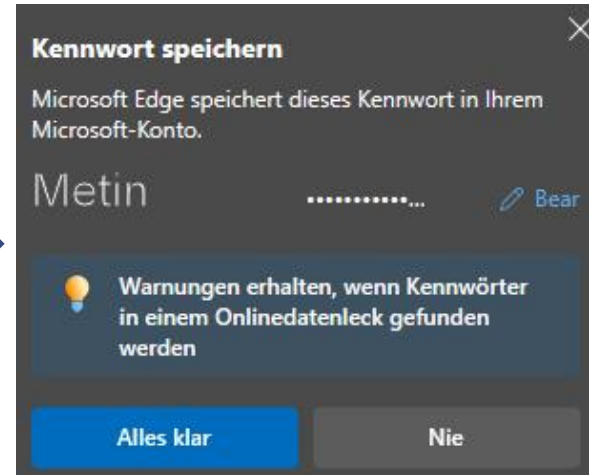
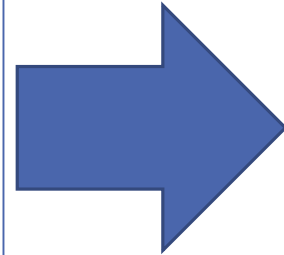
The screenshot shows the Windows Settings app with the 'Einstellungen' (Settings) menu on the left. The 'Datenschutz, Suche und Dienste' (Privacy, Search, and Services) option is selected. The main content area displays a privacy message: 'Hallo Metin, Ihre Privatsphäre ist uns wichtig.' Below this, the 'Verhindern der Nachverfolgung' (Prevent tracking) section is active, indicated by a blue toggle switch. Three tracking prevention levels are shown: 'Einfach' (Simple), 'Ausgewogen' (Balanced, marked as 'Empfohlen' or Recommended), and 'Streng' (Strict). The 'Ausgewogen' option is highlighted with a blue border. Below these options, there are sections for 'Blockierte Tracker' (Blocked trackers), 'Ausnahmen' (Exceptions), and a toggle for 'Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen' (Always use strict tracking prevention in InPrivate browsing). At the bottom, there is a 'Browserdaten löschen' (Clear browser data) section with a 'Browserdaten jetzt löschen' button and a 'Zu löschende Elemente auswählen' (Select items to delete) button.

Passwörter für Zugänge/Accounts speichern?

Browsereinstellungen am Beispiel Microsoft Edge

Passwort-Manager verwenden

Microsoft Edge verfügt über einen integrierten Passwort-Manager, der sichere Passwörter erstellen und speichern kann. Verwende ihn, um sichere Passwörter für Deine Online-Konten zu erstellen und zu verwalten.



Wenn Du Dich auf einer Website anmeldest und ein Passwort eingibst, fragt Edge, ob Du das Passwort speichern möchtest. Du kannst "Ja" bzw. „Alles klar“ auswählen, um es zu speichern.

Wie erkenne ich, ob eine Internetseite sicher oder unsicher ist? (1)

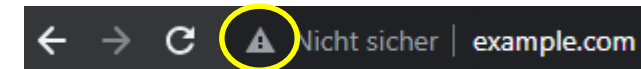
Es gibt mehrere Hinweise und Merkmale, anhand derer du feststellen kannst, ob eine Internetseite sicher oder unsicher ist. Hier sind einige wichtige Aspekte:

SSL-Verschlüsselung (HTTPS)

Überprüfe die URL der Website. Sichere Seiten beginnen mit "https://" anstelle von "http://". Das "s" steht für "sicher" und zeigt an, dass die Verbindung zwischen deinem Browser und der Website verschlüsselt ist.



sicher



nicht sicher

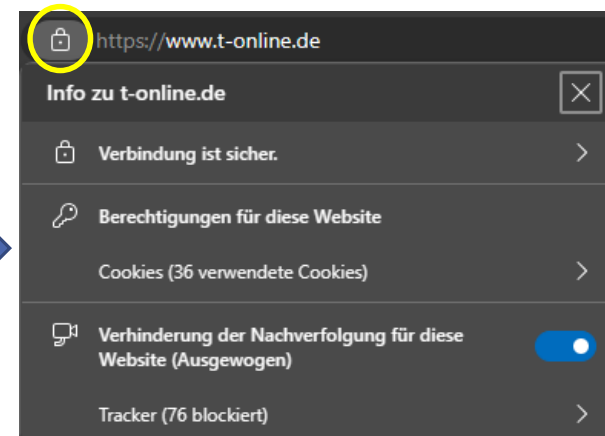
Schlosssymbol in der Adressleiste

Ein geschlossenes Vorhängeschloss neben der URL oder die grüne Adressleiste signalisieren ebenfalls eine sichere Verbindung.



Zertifikatsinformationen prüfen

Du kannst auf das Schlosssymbol in der Adressleiste klicken und die Zertifikatsinformationen anzeigen. Überprüfe, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.



Wie erkenne ich, ob eine Internetseite sicher oder unsicher ist? (2)

Es gibt mehrere Hinweise und Merkmale, anhand derer du feststellen kannst, ob eine Internetseite sicher oder unsicher ist. Hier sind einige wichtige Aspekte:

Website-Ruf und –Bewertungen

Nutze Dienste wie Google Safe Browsing*, Norton Safe Web oder andere Website-Bewertungsdienste, um Informationen über den Ruf einer Website zu erhalten.

Prüfe die URL-Struktur

Achte auf Rechtschreibfehler oder verdächtige Zeichen in der URL, die auf Phishing-Versuche hinweisen könnten.

Achte auf sichere Zahlungsoptionen

Bei Online-Shops: Achte darauf, dass sichere Zahlungsoptionen wie PayPal oder verschlüsselte Kreditkartenverarbeitung angeboten werden.

Aktualisiere deinen Browser und deine Sicherheitssoftware

Halte deinen Browser und deine Sicherheitssoftware auf dem neuesten Stand, um von den neuesten Sicherheitsfunktionen zu profitieren.

Warnmeldungen von Browsern beachten

Moderne Browser zeigen oft Warnungen an, wenn sie unsichere oder potenziell schädliche Websites erkennen. Nimm diese Warnungen ernst. Wenn eine Website unsicher erscheint oder Zweifel bestehen, ist es ratsam, die Interaktion mit der Seite zu vermeiden und sie zu verlassen. Sicherheitsbewusstsein und Achtsamkeit sind entscheidend, um online sicher zu bleiben.

*Google Safe Browsing ist ein Dienst von Google, der dazu dient, Internetnutzer vor schädlichen Aktivitäten im Netz zu schützen. Der Dienst überprüft Websites auf potenzielle Bedrohungen und warnt Nutzer vor dem Besuch von unsicheren Seiten.

Wie erkenne ich, ob eine Internetseite sicher oder unsicher ist? (3)

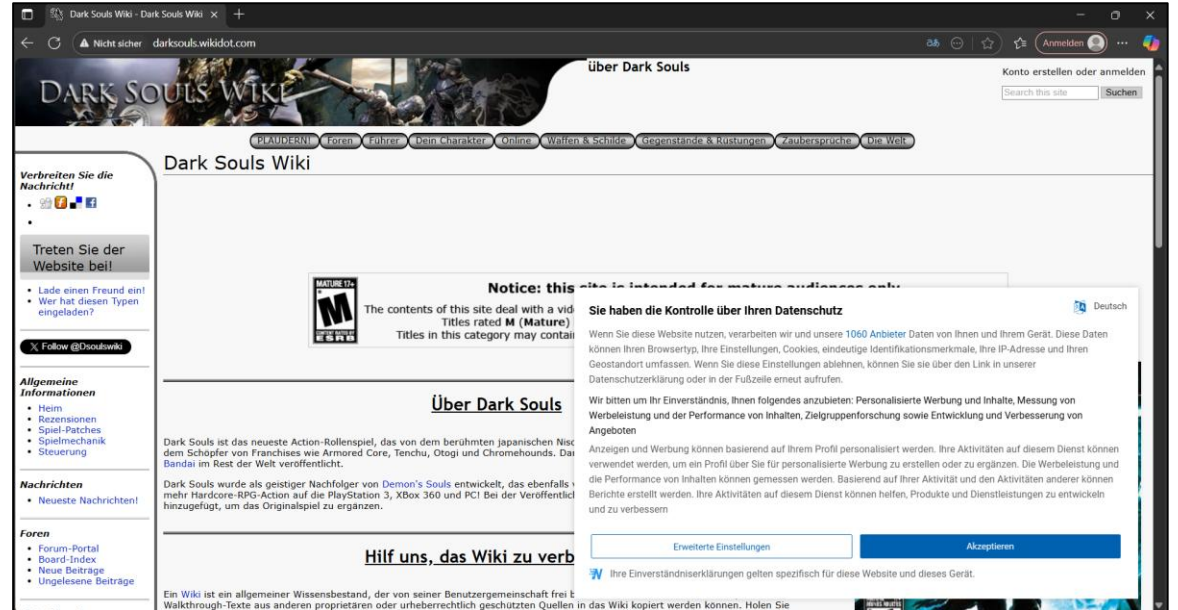
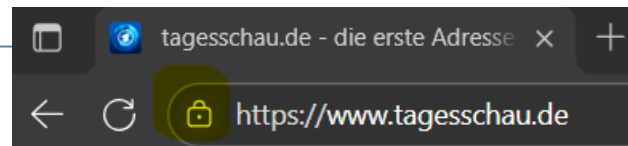


tagesschau.de

Die Webseite gehört zur ARD und wird von einem öffentlich-rechtlichen Sender professionell betrieben.

Sie nutzt eine sichere HTTPS-Verbindung, wodurch Daten verschlüsselt übertragen werden.

Insgesamt gilt sie als sehr **vertrauenswürdig und sicher**.

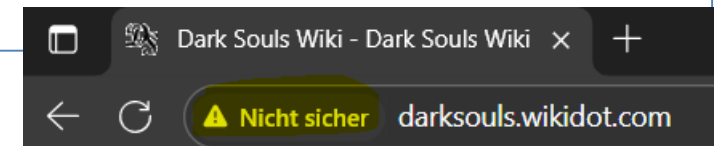


darksouls.wikidot.com

Diese Seite ist ein von Nutzern erstelltes Community-Wiki, das auf der Plattform Wikidot gehostet wird.

Nicht alle Wikidot-Seiten erzwingen eine verschlüsselte Verbindung, was ein Sicherheitsrisiko darstellen kann.

Daher sollte man sie **mit Vorsicht verwenden** und keine sensiblen Daten eingeben.



Tipps beim Surfen im Internet

- Auch im Web gibt es Regeln
- Schütze Deine Privatsphäre
- Nicht alles ist wahr
- Urheberrechte beachten
- Das Recht am eigenen Bild
- Quellenangaben nicht vergessen
- Umsonst gibt es Nichts
- Online-Freunde niemals alleine treffen



Sicherer Umgang beim Surfen im Internet

Grundregeln

- Immer aktuelle Betriebssystemupdates nutzen
- Nie ohne aktiven Antivirenschutz im Internet surfen
- Keine illegalen Seiten aufsuchen
- Keine persönlichen Daten und Bankverbindungen eintragen, wenn Du die Seite nicht als sicheren Anbieter kennst
- Die Wahl des richtigen Browsers
- PlugIns (Zusatzprogramme) für Browser nur von sicheren Originalseiten installieren



Top 10 der Regeln für Internetsicherheit

1. Beschränke Dich auf wenige, aber seriöse persönliche Informationen.
2. Achte auf Deine Datenschutzeinstellungen.
3. Achte auf Deine Surfgewohnheiten.
4. Nutze eine sichere Internetverbindung.
5. Wähle Downloads vorsichtig aus.
6. Verwende starke Passwörter.
7. Tätige Einkäufe nur auf sicheren Seiten.
8. Wähle Deine Beiträge vorsichtig aus.
9. Sei vorsichtig mit Online-Bekanntschäften.
10. Halte Deine Antiviren-Software immer auf dem neuesten Stand.



Sicher im WLAN

- Fakt ist, dass WLAN-Betreiber von öffentlichen WLAN-Zugängen können NIE ausschließen, dass ihre Router doch nicht manipuliert werden. Sollte dies der Fall sein, dann landen Eure Daten direkt bei Kriminellen, die Euch ausspionieren. D.h. sie wissen, welche Internetseiten Ihr besucht habt, lesen Passwörter und Benutzernamen aus.
- Ein bisschen rumsurfen ist kein Problem, aber Finger weg von:
 - Online Shopping
 - Online Banking & Co
- Da also kein Mensch weiß, wer noch so im kostenlosen WLAN rumgeistert, könntet Ihr für Eure Daten ein VPN nutzen. Das ist ein „virtuelles privates Netzwerk, das für Eure Daten einen sicheren verschlüsselten Tunnel baut. VPNs gibt`s als APPs für Smartphones. Reisende und viel WLAN-Nutzer sollten dies beherzigen. Mehr Infos unter <http://sicherdigital.de>



Sicher im WLAN

Zusammenfassung

- Jeder zweiter Internetnutzer war innerhalb der letzten 12 Monate schon mal Opfer von Cyberkriminalität. Quelle: DigitalverbandBitkom.
- Bitte folgende Tipps beachten:
 - Software-Updates installieren
 - Zahlen PIN verwenden (SIM-Karte und Bildschirm)
 - Virenschutzprogramm installieren
 - Back-ups machen



E-Mail

Was kann man mit dem Computer und im Internet machen?

Computer und das Internet sind aus unserem Alltag kaum noch wegzudenken. Sie bieten uns eine Vielzahl von Möglichkeiten, unsere Zeit zu verbringen, zu lernen und zu arbeiten. Hier sind einige Beispiele für Dinge, die man mit einem Computer und im Internet machen kann:

- **Informationen suchen**

Das Internet ist eine riesige Wissensdatenbank. Mit nur wenigen Klicks können wir Informationen zu jedem Thema finden.

- **In Kontakt bleiben**

Wir können mit Freunden und Familie über E-Mail, soziale Netzwerke und Instant Messaging in Kontakt bleiben.

- **Unterhaltung**

Wir können Musik hören, Filme und Videos ansehen, spielen und lesen.

- **Arbeiten**

Wir können mit dem Computer und im Internet Texte schreiben, Präsentationen erstellen, Tabellenkalkulationen erstellen und vieles mehr.

- **Lernen**

Wir können mit dem Computer und im Internet neue Sprachen lernen, an Kursen teilnehmen, Bücher lesen und vieles mehr. Die Möglichkeiten, die uns Computer und das Internet bieten, sind vielfältig. Es liegt an uns, zu entscheiden, wie wir sie nutzen wollen.

Hier sind einige zusätzliche Tipps für die Nutzung von Computern und dem Internet:

- Seid kritisch gegenüber den Informationen, die Ihr im Internet findet. Nicht alles, was Ihr online liest, ist wahr.
- Schütze Deine Ihre Privatsphäre. Sei vorsichtig, welche persönlichen Informationen Du im Internet preisgibst.
- Setze Dir Grenzen. Es ist wichtig, sich auch Zeit für andere Aktivitäten zu nehmen, als nur am Computer zu sitzen.
- Computer und das Internet sind ein wertvolles Werkzeug. Mit ihnen können wir unsere Zeit produktiv nutzen, lernen und Spaß haben. Es liegt an uns, sie verantwortungsbewusst zu nutzen.

E-Mail

Was ist eine E-Mail?

Eine E-Mail ist im Grunde genommen ein elektronischer Brief. Das "E" steht für "elektronisch" und "Mail" ist das englische Wort für "Post". E-Mails können über das Internet verschickt werden und eignen sich deshalb gut für den Austausch von Nachrichten mit Menschen auf der ganzen Welt.

Im Gegensatz zu SMS haben E-Mails keine Begrenzung hinsichtlich der Länge des Textes. Außerdem sind E-Mails meistens kostenlos. Ähnlich wie ein klassischer Brief eignet sich die E-Mail für längere Nachrichten und Anliegen

Geschichte der E-Mail

Die Geschichte der E-Mail beginnt in den 1960er Jahren mit der Entwicklung des Arpanet, dem Vorläufer des Internets. Damals nutzten Wissenschaftler dieses Netzwerk hauptsächlich, um Dateien zwischen Computern auszutauschen.



Welche Informationen und Werkzeuge benötigt man, um eine E-Mail zu schreiben? (1)

- **E-Mail-Adresse**

Du benötigst die E-Mail-Adresse des Empfängers, an den du Deine Nachricht senden möchtest.

Lokaler Teil:

Der lokale Teil steht vor dem @-Zeichen und kann frei gewählt werden. Er kann zum Beispiel den Namen, die Vornamen, eine Kombination aus beidem oder einen Nickname enthalten.

Zulässige Zeichen:

Groß- und Kleinbuchstaben, Zahlen, Unterstriche (_), Punkte (.), Minuszeichen (-)

Sonderzeichen wie \$, %, & oder ! sind **nicht** erlaubt.

Länge: Der lokale Teil darf **maximal 64 Zeichen** lang sein.

So funktioniert eine E-Mail-Adresse:

Wenn du eine E-Mail an jemanden sendest, wird die E-Mail an den Server des Empfängers weitergeleitet. Der Server sucht dann nach dem Postfach des Empfängers, indem er den lokalen Teil der E-Mail-Adresse verwendet. Ist das Postfach gefunden, wird die E-Mail dort abgelegt und der Empfänger kann sie lesen.



Beispiel

Vorname.Nachname@web.de

Frei wählbar

Server, auf dem das Postfach des Empfängers liegt

Welche Informationen und Werkzeuge benötigt man, um eine E-Mail zu schreiben? (1)

- **E-Mail-Client oder –Dienst**
Du kannst eine E-Mail über verschiedene Plattformen und Dienste verfassen, wie z. B. Gmail, Outlook, Yahoo Mail, etc. Du kannst auch E-Mail-Clients wie Mozilla Thunderbird oder Microsoft Outlook auf Deinem Computer verwenden.
- **Internetverbindung**
Eine aktive Internetverbindung ist erforderlich, um E-Mails zu senden. Dies gilt sowohl für Webmail-Dienste als auch für E-Mail-Clients.
- **Betreff**
Ein aussagekräftiger Betreff gibt dem Empfänger einen schnellen Überblick über den Inhalt der E-Mail.
- **Nachricht**
Der Hauptteil der E-Mail enthält den eigentlichen Text. Hier erklärst Du den Zweck Deiner Nachricht oder teilst Informationen.
- **Korrekte Anrede**
Je nach Beziehung und Formalität verwendest Du eine angemessene Anrede, wie "Sehr geehrte Damen und Herren" oder "Liebe/r [Name]".



Welche Informationen und Werkzeuge benötigt man, um eine E-Mail zu schreiben? (2)

- **Abschlussformel**
Beende Deine E-Mail mit einer höflichen Abschlussformel, wie zum Beispiel "Mit freundlichen Grüßen" oder "Beste Grüße".
- **Signatur**
Du solltest Deine Signatur hinzufügen, die Deinen Namen, Deine Position und gegebenenfalls Deine Kontaktdaten enthält.
- **Anhänge**
Falls Du Dateien oder Dokumente mitsenden möchtest, solltest Du sicherstellen, dass sie relevant sind und an die E-Mail angehängt werden.
- **Korrekturlesen**
Es ist wichtig, Deine E-Mail auf Grammatik- und Rechtschreibfehler zu überprüfen, um einen professionellen Eindruck zu hinterlassen.
- **Optionale CC und BCC**
Wenn Du die E-Mail an weitere Empfänger kopieren möchtest (CC - Carbon Copy) oder dies verdeckt tun möchtest (BCC - Blind Carbon Copy), kannst Du diese Optionen verwenden.
- **Korrekte E-Mail-Adresse des Absenders**
Stelle sicher, dass die E-Mail von Deiner korrekten E-Mail-Adresse gesendet wird.



Was ist der Unterschied zwischen einer normalen E-Mail und einer verschlüsselten E-Mail?



Normale E-Mail

Funktionsweise

Eine normale E-Mail funktioniert ähnlich wie eine Postkarte. Jeder, der Zugriff auf die Übertragungswege (z. B. E-Mail-Server oder Netzwerke) hat, kann den Inhalt der Nachricht lesen.

Sicherheitsrisiken

- Der Inhalt der Nachricht kann abgefangen und gelesen werden.
- Persönliche Daten oder vertrauliche Informationen sind nicht geschützt.
- Es besteht das Risiko, dass die E-Mail von Unbefugten verändert oder missbraucht wird.

Beispiel einer normalen E-Mail

Du schickst deinem Freund eine E-Mail mit deinem Geburtstagstermin. Jeder, der die E-Mail unterwegs abfängt, kann diese Information sehen.



Verschlüsselte E-Mail

Funktionsweise

Eine verschlüsselte E-Mail funktioniert wie ein Brief in einem verschlossenen Umschlag. Nur der Absender und der Empfänger können den Inhalt sehen, da er durch eine Art „Code“ geschützt ist.

- **Ende-zu-Ende-Verschlüsselung:** Der Inhalt der Nachricht wird vor dem Versand verschlüsselt. Nur der Empfänger, der den passenden „Schlüssel“ hat, kann die E-Mail entschlüsseln und lesen.
- **Transportverschlüsselung (TLS):** Schützt die E-Mail auf dem Weg von Absender zu Empfänger, aber nicht den Inhalt selbst.

Vorteile:

- Vertrauliche Inhalte sind vor unbefugtem Zugriff geschützt.
- Selbst wenn die Nachricht abgefangen wird, können Dritte sie nicht lesen.
- Gewährleistet die Echtheit und Integrität der Nachricht.

Beispiel einer verschlüsselten E-Mail

Du schickst deinem Steuerberater sensible Finanzdaten. Selbst wenn ein Hacker die E-Mail abfängt, kann er den Inhalt ohne den passenden Schlüssel nicht lesen.

Welche E-Mail-Dienste bieten die Möglichkeit, E-Mails sicher zu verschlüsseln?

- **Proton Mail**
Ein in der Schweiz ansässiger Dienst, der Ende-zu-Ende-Verschlüsselung bietet. Proton Mail legt großen Wert auf Datenschutz und Privatsphäre.
- **Tuta**
Ehemals bekannt als Tutanota, ist ein deutscher E-Mail-Dienst mit integrierter Ende-zu-Ende-Verschlüsselung. Tuta betont Nachhaltigkeit und verwendet 100% erneuerbare Energie.
- **Mailbox.org**
Ein deutscher Anbieter, der sichere E-Mail-Kommunikation mit PGP-Verschlüsselung ermöglicht. Mailbox.org bietet zudem Kalender-, Kontakt- und Cloud-Speicherfunktionen.
- **Posteo**
Ein weiterer deutscher Dienst, der auf Sicherheit und Datenschutz setzt. Posteo bietet verschlüsselte E-Mail-Kommunikation und legt Wert auf Nachhaltigkeit.
- **Mailfence**
Ein belgischer Anbieter, der OpenPGP-basierte Ende-zu-Ende-Verschlüsselung und digitale Signaturen bietet. Mailfence kombiniert E-Mail mit Kalender-, Kontakt- und Dokumentenfunktionen.
- **Hushmail**
Ein kanadischer Dienst, der PGP-verschlüsselte E-Mails anbietet. Hushmail ist besonders im Gesundheits- und Rechtssektor beliebt.

Bitte beachte, dass einige dieser Dienste kostenpflichtig sind oder erweiterte Funktionen gegen Gebühr anbieten. Es ist wichtig, die jeweiligen Datenschutzrichtlinien und Sicherheitsfunktionen der Anbieter zu prüfen, um den für Deine Bedürfnisse passenden Dienst auszuwählen.

Wie funktioniert die Verschlüsselung technisch? (Sehr einfach erklärt)

Stell dir vor, du möchtest deiner Freundin eine geheime Nachricht schicken. Du willst sicherstellen, dass niemand außer ihr die Nachricht lesen kann. Dafür gibt es zwei einfache Methoden:

1. Schlüssel-Paar-Methode (Öffentlicher und Privater Schlüssel)

- Öffentlicher Schlüssel: Stell dir vor, das ist ein offener Briefkasten, in den jeder etwas einwerfen kann. Diesen Schlüssel gibst du deiner Freundin.
- Privater Schlüssel: Das ist der Schlüssel zum Öffnen des Briefkastens. Den hast nur du.

So funktioniert es:

- Deine Freundin verschlüsselt die Nachricht mit deinem öffentlichen Schlüssel.
- Du bekommst die Nachricht und entschlüsselst sie mit deinem privaten Schlüssel.

Niemand kann die Nachricht lesen, weil nur du den privaten Schlüssel hast.

2. Geheimer Schlüssel (Symmetrische Verschlüsselung)

Das ist, als würdest du und deine Freundin denselben Geheimcode nutzen.

So funktioniert es:

- Du verschlüsselst die Nachricht mit dem Geheimcode.
- Deine Freundin benutzt denselben Geheimcode, um die Nachricht zu entschlüsseln.

Einfach gesagt:

- Bei der Verschlüsselung wird der Text so verändert, dass er wie Geheimsprache aussieht.
- Nur die Person mit dem passenden Schlüssel kann den Text wieder in normale Sprache zurückverwandeln.

Wie können E-Mails verschlüsselt werden, wenn Sender und Empfänger verschiedene E-Mail-Dienste nutzen? (Einfach erklärt)

Wenn du und die Person, mit der du E-Mails austauschen möchtest, verschiedene E-Mail-Dienste verwendet, gibt es dennoch Möglichkeiten, die Nachrichten sicher zu verschlüsseln. Hier sind einfache Erklärungen:

1. Methode

Benutze ein gemeinsames Passwort

So funktioniert's:

1. Du schreibst eine E-Mail und schützt sie mit einem Passwort.
2. Dieses Passwort gibst du der anderen Person (z. B. am Telefon oder per SMS).
3. Die andere Person gibt das Passwort ein, um die E-Mail zu öffnen.

Beispiel:

- Du benutzt ProtonMail und die andere Person hat Gmail.
- Du schickst eine verschlüsselte E-Mail über ProtonMail und gibst ein Passwort vor.
- Die andere Person erhält die E-Mail, öffnet sie aber nur mit dem Passwort, das du ihr gegeben hast.

Wie können E-Mails verschlüsselt werden, wenn Sender und Empfänger verschiedene E-Mail-Dienste nutzen? (Einfach erklärt)

2. Methode

Gemeinsame Verschlüsselungsprogramme nutzen

So funktioniert's:

- Beide installieren ein kleines Programm oder ein Browser-Plugin, das die Nachrichten verschlüsselt.
- Vor dem Senden verschlüsselst du die Nachricht, und nur die andere Person mit dem passenden Programm kann sie entschlüsseln.

Beispiel

- Ihr könnt ein einfaches Tool wie Mailvelope benutzen, das direkt in den Browser integriert ist.
- Beide tauschen einmalig „Schlüssel“ aus (sozusagen eine Art digitaler Code).
- Danach kann jeder die Nachrichten verschlüsseln und sicher lesen.

Wie können E-Mails verschlüsselt werden, wenn Sender und Empfänger verschiedene E-Mail-Dienste nutzen? (Einfach erklärt)

3. Methode

Login in ein sicheres Portal

So funktioniert's:

- Du schickst die Nachricht über ein spezielles, sicheres Portal.
- Der Empfänger erhält eine Benachrichtigung und loggt sich im Portal ein, um die Nachricht zu lesen.

Beispiel:

- Dienste wie Microsoft oder Tresorit bieten sichere Portale an, in die sich der Empfänger einloggen muss.

Einfach gesagt

- Mit Passwort: Du schützt die Nachricht und teilst das Passwort.
- Mit Tool: Beide nutzen ein einfaches Programm, um Nachrichten zu verschlüsseln.
- Mit Portal: Du lädst die Nachricht hoch, der Empfänger holt sie ab.

Das klingt vielleicht anfangs kompliziert, aber in der Praxis sind die meisten Dienste sehr nutzerfreundlich und führen dich Schritt für Schritt durch den Prozess.

Gmail – vertraulich senden

Was bedeutet „Vertraulich senden“?

- E-Mail wird geschützt geöffnet
- Weiterleiten / Kopieren gesperrt
- Zeitlich begrenzt
- Optional SMS-Code

So aktivierst du den Modus

1. Neue E-Mail schreiben
2. Schloss-Uhr Symbol
3. Ablaufdatum & Code
4. Senden

So aktivierst du den Modus

- Zugriff endet automatisch
- Wahl: 1 Tag bis 5 Jahre

SMS Passcode

- Empfänger erhält Code
- Ohne Code kein Zugriff

Grenzen

- Kein absolut geheimer Modus
- Screenshots möglich
- Nicht für streng geheime Daten

E-Mail-Account erstellen

Auswahl des E-Mail-Dienstes

Wahl des Anbieters

- Berücksichtigung von Datenschutzrichtlinien, Benutzerfreundlichkeit und Zusatzfunktionen
- Beliebte Anbieter wie Gmail, Outlook und Yahoo bieten weitreichende Dienstleistungen an.

Anmeldung und Registrierung

Schritte zur Anmeldung

- Eingabe persönlicher Daten wie Name, Geburtsdatum und ggf. Telefonnummer
- Auswahl eines starken Passworts mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Verifikation:
 - Bestätigung durch Klick auf einen Link in der Bestätigungsmail oder durch SMS-Code
- Profileinstellungen:
 - Anpassung von Benutzerinformationen wie Signatur, Profilbild und Datenschutzeinstellungen
 - Sensible Daten nur begrenzt oder gar nicht teilen, um die Privatsphäre zu wahren

Kostenlose E-Mail Anbieter

Die besten Anbieter für kostenlose E-Mail-Adressen



[Hinzufügen eines E-Mail-Kontos zu Outlook - Microsoft-Support](#)



[E-Mail: mit @magenta.de sicher mailen | Telekom](#)



[Neue E-Mail-Adresse erstellen – kostenlos | GMX](#)



[Gmail-Konto erstellen - Gmail-Hilfe \(google.com\)](#)



[Neue kostenlose E-Mail-Adresse erstellen | WEB.DE](#)

E-Mail schreiben und versenden

Verfassen einer E-Mail

Betreffzeile

- Klare und präzise Formulierung des Themas
- Vermeidung von reißerischen oder spam-verdächtigen Begriffen

Anrede und Inhalt

- Höfliche Anrede, beispielsweise "Sehr geehrte/r [Name],"
- Strukturierte Darstellung des Inhalts mit Absätzen und Bullet Points für bessere Lesbarkeit

Anhänge hinzufügen

- Beachtung der maximalen Anhangsgröße des E-Mail-Dienstes
- Verwendung von Cloud-Speicher (z.B. Google Drive, Dropbox) bei großen Dateien

Versenden der E-Mail

Empfängeradresse

- Sorgfältige Überprüfung auf korrekte Eingabe
- Vermeidung von Tippfehlern, da dies zu Fehlzustellungen führen kann

CC und BCC verwenden

- Verständnis für die Funktionen von CC (Carbon Copy) und BCC (Blind Carbon Copy)
- Verwendung von CC für sichtbare Empfänger und BCC für verdeckte Empfänger

E-Mail-Überprüfung

- Gründliches Durchlesen vor dem Versenden, um Rechtschreibfehler zu vermeiden
- Überprüfung von Anhängen und Links auf Korrektheit und Funktionalität

E-Mail Sicherheitsmaßnahmen

Schutz des E-Mail-Accounts

Starke Passwörter

- Verwendung von Passwort-Manager-Tools für sichere Passwortgenerierung und –verwaltung
- Regelmäßige Aktualisierung des Passworts, idealerweise alle 3-6 Monate

Zwei-Faktor-Authentifizierung (2FA)

- Aktivierung der 2FA für zusätzliche Sicherheit
- Verwendung von Authentifizierungs-codes, die regelmäßig erneuert werden

Schutz vor Phishing und Malware

Misstrauisch sein

- Identifikation von Phishing-E-Mails durch Überprüfung der Absenderadresse und ungewöhnlicher Anfragen
- Vorsicht bei unerwarteten Anhängen und Links, besonders in E-Mails von unbekanntem Absendern

Antivirensoftware

- Installation und regelmäßige Aktualisierung von zuverlässiger Antivirensoftware
- Automatische Überprüfung von E-Mail-Anhängen auf potenzielle Bedrohungen

Datenschutz beachten

E-Mail-Verschlüsselung

- Verwendung von verschlüsselten Verbindungen (SSL/TLS) für sichere Datenübertragung
- Optionen für Ende-zu-Ende-Verschlüsselung nutzen, wenn vertrauliche Informationen ausgetauscht werden

Vertrauliche Informationen

- Vermeidung von sensiblen Daten in E-Mails, insbesondere wenn keine Verschlüsselung verwendet wird
- Nutzung sicherer Kommunikationswege wie verschlüsselte Messaging-Apps für besonders sensible Themen

In wenigen Schritten zur perfekten E-Mail (Teil: 1)

Das Verfassen einer E-Mail erfordert einige grundlegende Schritte, um sicherzustellen, dass deine Nachricht klar, höflich und effektiv ist. Hier sind die wichtigsten Aspekte, die du beim Schreiben einer E-Mail beachten solltest:

1. **Betreff**

Der Betreff sollte prägnant und aussagekräftig sein, um dem Empfänger einen schnellen Überblick über den Inhalt der E-Mail zu geben.

2. **Anrede (Gruß):**

Verwende eine angemessene Anrede, je nachdem, wie gut du die Person kennst. "Sehr geehrte Damen und Herren" ist eine formale Anrede, während "Liebe/r [Name]" eher informell ist.

3. **Einleitung**

Beginne Deine E-Mail mit einer kurzen Einleitung, in der Du den Grund für deine Nachricht erläuterst. Du kannst auch höfliche Floskeln verwenden, wie z. B. "Ich hoffe, diese E-Mail findet Sie gut.,,

4. **Hauptteil**

Im Hauptteil der E-Mail erklärst Du den Hauptzweck deiner Nachricht. Strukturiere Deine Informationen klar und präzise. Vermeide es, zu lange Absätze zu schreiben, und füge bei Bedarf Absätze ein.

5. **Höfliche Sprache**

Verwende höfliche und respektvolle Sprache. Beachte dabei die kulturellen Gepflogenheiten und die Beziehung, die Du zu der Person hast.

6. **Klarheit und Prägnanz**

Formuliere Deine Sätze klar und vermeide es, zu technisch oder umständlich zu schreiben. Kürze irrelevante Informationen, um die Klarheit zu bewahren.

In wenigen Schritten zur perfekten E-Mail (Teil: 2)

7. **Schluss**

Beende deine E-Mail mit einer höflichen Schlussformel, wie zum Beispiel "Mit freundlichen Grüßen" oder "Beste Grüße". Falls du eine Antwort erwartest, kannst du dies auch deutlich machen.

8. **Unterschrift**

Füge deine vollständige Signatur hinzu, einschließlich deines Namens, deiner Position, deiner Kontaktdaten und gegebenenfalls deines Unternehmens oder deiner Organisation.

9. **Dateianhänge**

Falls du Dateien anhängen möchtest, füge sie der E-Mail hinzu und erwähne dies kurz im Text.

10. **Korrekturlesen**

Bevor du die E-Mail sendest, überprüfe sie sorgfältig auf Grammatik- und Rechtschreibfehler. Ein fehlerfreier Text vermittelt einen professionellen Eindruck.

11. **Empfänger prüfen**

Stelle sicher, dass du die richtige E-Mail-Adresse des Empfängers angegeben hast, um sicherzustellen, dass deine Nachricht den richtigen Empfänger erreicht.

12. **Anhang**

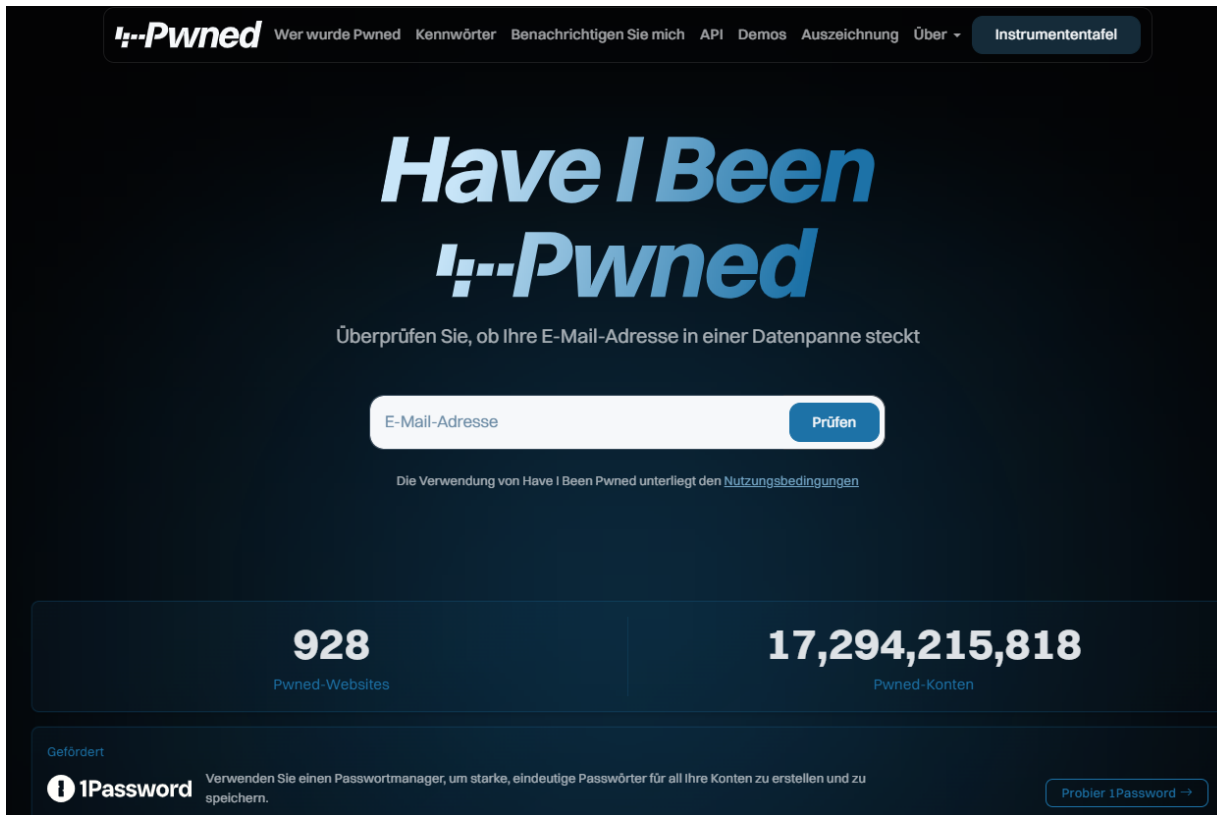
Wenn du Anhänge beifügst, vergewissere dich, dass sie relevant sind und die richtigen Dateiformate haben.

13. **Antwort auf frühere E-Mails**


Falls deine E-Mail eine Antwort auf eine vorherige Nachricht ist, zitiere bei Bedarf den relevanten Text, um den Zusammenhang herzustellen.


Überprüfe, ob Deine E-Mail-Adresse in einem Datenleck war

Auf dieser Website kann man ganz einfach seine E-Mail-Adresse eingeben, um zu sehen, ob sie jemals Teil eines Datenlecks war. Die Seite ist vertrauenswürdig und hilft dabei, die eigene Sicherheit im Blick zu behalten."



The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top, there is a navigation bar with the logo and links for 'Wer wurde Pwned', 'Kennwörter', 'Benachrichtigen Sie mich', 'API', 'Demos', 'Auszeichnung', 'Über', and 'Instrumententafel'. The main heading reads 'Have I Been Pwned' in a large, stylized font. Below this, a subtitle says 'Überprüfen Sie, ob Ihre E-Mail-Adresse in einer Datenpanne steckt'. A search form is present with a text input field labeled 'E-Mail-Adresse' and a blue button labeled 'Prüfen'. A small note below the form states 'Die Verwendung von Have I Been Pwned unterliegt den Nutzungsbedingungen'. At the bottom, two statistics are displayed: '928 Pwned-Websites' and '17,294,215,818 Pwned-Konten'. A footer section promotes '1Password' with the text 'Gefördert' and 'Verwenden Sie einen Passwortmanager, um starke, eindeutige Passwörter für all Ihre Konten zu erstellen und zu speichern.', along with a button 'Probier 1Password →'.

 Have I been pwned?

 Wurde ich gehackt?

Prüfe hier:

<https://haveibeenpwned.com>

Schütze Deine E-Mail - So findest du heraus, ob sie im Internet auftaucht

Dienst / Tool	Beschreibung + URL
<ul style="list-style-type: none">• Have I Been Pwned	<p>Dieses Online-Tool hilft Dir herauszufinden, ob Deine E-Mail-Adresse in einem bekannten Datenleck enthalten ist.</p> <p>https://haveibeenpwned.com</p>
<ul style="list-style-type: none">• Identity Leak Checker (Hasso-Plattner-Institut)	<p>Dies ist ein deutscher, staatlich unterstützter Dienst. Er prüft auch weitere persönliche Daten wie Name oder Adresse.</p> <p>https://sec.hpi.de/leak-checker/search?lang=de</p>
<ul style="list-style-type: none">• Leak Checker – Universität Bonn	<p>Ein deutsches Projekt, geeignet für Einsteiger zur schnellen Überprüfung Deiner E-Mail.</p> <p>https://leakchecker.uni-bonn.de/de/index</p>
<ul style="list-style-type: none">• Firefox Monitor	<p>Benachrichtigt Dich auch zukünftig automatisch, falls deine E-Mail in neuen Datenlecks auftaucht.</p> <p>https://monitor.firefox.com</p>
<ul style="list-style-type: none">• DeHashed	<p>Suchmaschine für gestohlene Daten wie E-Mail, Nutzernamen oder IP-Adresse.</p> <p>https://dehashed.com</p>
<ul style="list-style-type: none">• DataBreach.com	<p>Ein einfaches Tool zur schnellen Überprüfung, ob Deine Daten betroffen sind.</p> <p>https://databreach.com</p>
<ul style="list-style-type: none">• Free Compromised Email Check – NameScan	<p>Kostenloser Check, um herauszufinden, ob Deine E-Mail kompromittiert (gehackt, gefährdet) wurde.</p> <p>https://namescan.io/freeemailcompromisedcheck</p>

Online einkaufen

Woran erkennt man einen seriösen Onlineshop? (1)

Die Erkennung eines seriösen Onlineshops ist entscheidend, um sicherzustellen, dass deine persönlichen Daten geschützt sind und du qualitativ hochwertige Produkte oder Dienstleistungen erhältst. Hier sind einige Merkmale, auf die du achten kannst:

- 1 HTTPS-Verbindung**
Ein seriöser Onlineshop verwendet eine verschlüsselte Verbindung. Achte darauf, dass die URL mit "https://" beginnt. Das "s" steht für Sicherheit, und dies zeigt an, dass die Daten während der Übertragung verschlüsselt sind.
- 2 Kontaktinformationen**
Ein seriöser Shop stellt klare Kontaktinformationen zur Verfügung. Überprüfe, ob die Website eine physische Adresse, eine Telefonnummer und eine E-Mail-Adresse angibt. Fehlende oder schwer zu findende Kontaktdaten können auf Unseriosität hinweisen.
- 3 Bewertungen und Erfahrungen**
Suche nach Bewertungen und Erfahrungen anderer Kunden. Vertrauenswürdige Shops haben oft Bewertungen auf ihrer Website oder auf unabhängigen Plattformen wie Trustpilot. Liest sowohl positive als auch negative Bewertungen, um ein ausgewogenes Bild zu erhalten.
- 4 Professionelles Design**
Ein seriöser Onlineshop investiert in ein professionelles und sauberes Webdesign. Achte auf eine klare Struktur, leicht verständliche Navigation und hochwertige Produktbilder.
- 5 Transparente Geschäftsbedingungen**
Überprüfe die Geschäftsbedingungen des Shops. Ein seriöser Anbieter gibt klare Informationen zu Rückgaberecht, Garantie, Lieferzeiten und Zahlungsmodalitäten. Wenn diese Informationen schwer zu finden oder vage sind, sei vorsichtig.

Woran erkennt man einen seriösen Onlineshop? (2)

6

Sicherheitszertifikate

Ein seriöser Onlineshop verwendet Sicherheitszertifikate. Achte auf Symbole wie das Schlosssymbol in der Adressleiste oder Sicherheitszertifikate von Drittanbietern wie Norton oder McAfee.

7

Vielfältige Zahlungsoptionen

Seriöse Shops bieten oft eine Auswahl an sicheren Zahlungsoptionen an. Dazu gehören gängige Kreditkarten, PayPal oder andere vertrauenswürdige Zahlungsmethoden.

8

Überprüfung der URL

Achte darauf, dass die URL des Onlineshops korrekt geschrieben ist. Phishing-Seiten versuchen manchmal, legitime Websites nachzuahmen, indem sie ähnliche URLs verwenden.

9

Kundenservice-Responsivität

Kontaktiere den Kundenservice vor dem Kauf mit einer Frage, um die Reaktionszeit und die Qualität des Supports zu überprüfen. Ein seriöser Shop sollte schnell und hilfreich antworten.

10

Social-Media-Präsenz

Seriöse Shops sind oft in sozialen Medien aktiv. Überprüfe ihre Präsenz auf Plattformen wie Facebook, Instagram oder Twitter. Dies kann zusätzliche Einblicke in ihre Reputation geben.

Indem du diese Kriterien berücksichtigst, kannst du das Risiko minimieren, auf betrügerische Onlineshops hereinzufallen, und sicherstellen, dass deine Online-Einkäufe sicher sind.

Woran erkennt man einen seriösen Onlineshop? (3)



<https://www.trustedshops.de/>



<https://www.gepruefter-webshop.de/>



<https://ehi-siegel.de/>



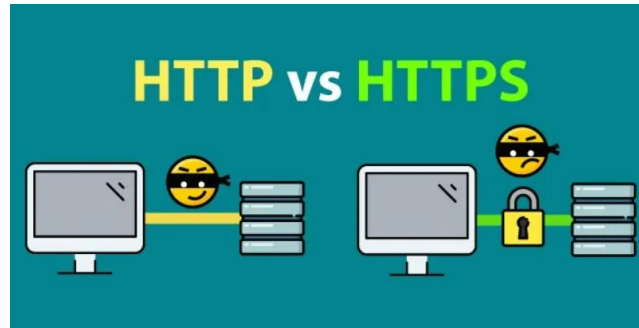
<https://www.datenschutz-cert.de/>



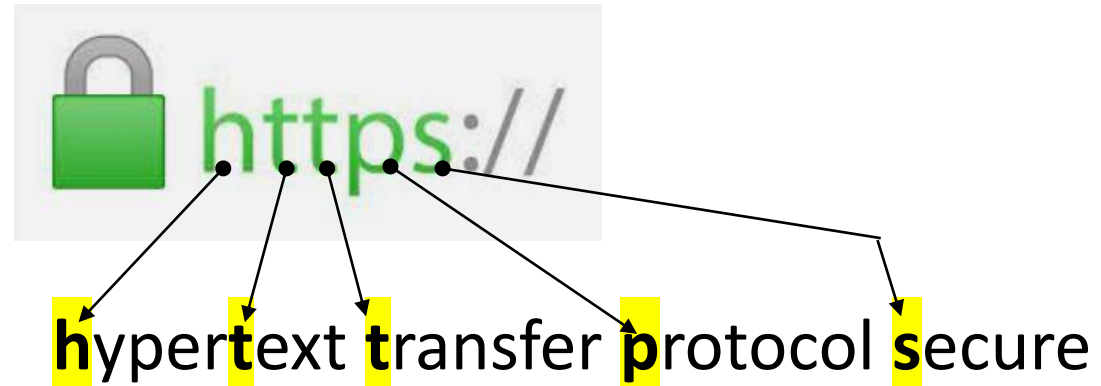
<https://www.tuvsud.com/de-de>

Woran erkennt man einen seriösen Onlineshop? (4)

- Online-Shop im deutschen Unternehmensregister suchen
- Auf eine sichere Verschlüsselung achten



- <https://www.amazon.de/>
- <https://www.ebay.de/>
- <https://www.otto.de/>
- <https://shop.rewe.de/>



[secure=sicher]

Alle Daten werden verschlüsselt an den jeweils anderen Computer gesendet.

Worauf müssen Konsumenten beim online einkaufen achten?

6

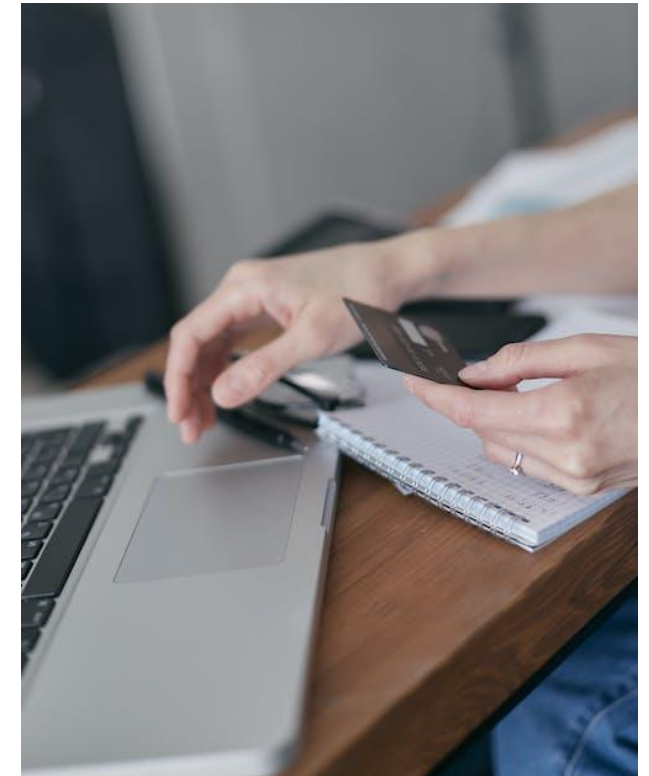


Um sicher zu gehen,
solltet Ihr in erster
Linie bei bekannten
Online-Händlern über
bekannte Apps kaufen.

Welche Gefahren gibt es beim Online-Einkauf?

Der Einkauf beginnt oft schon beim Angebot – hier gilt es aufmerksam die Angebote zu beachten und zu überprüfen, von wem diese Angebote stammen.

1. **Nicht auf E-Mail-Angebote klicken (Prüft E-Mail-Angebote ganz genau).**
*In sogenannten Phishing Mails werden Sonderangebote von vermeintlichen Online-Händlern dargestellt. Websites von Amazon oder anderen bekannten Online-Händlern werden nachgestellt und können tatsächlich sehr ähnlich aussehen. Dieses Phänomen ist seit der Corona-Krise und dem verstärkten Umsatz von Online-Shops noch stärker in Erscheinung getreten. Um sicherzugehen, dass es sich hier um keinen Betrug handelt, solltet Ihr **nicht** auf den Link in der Mail klicken, sondern lieber direkt auf die Seite des Anbieters gehen, um dort weiter zu surfen.*
2. **Vermeidet Zahlungen per Vorkasse.**
Hier setzt Ihr Euch dem Risiko aus, das Geld vor dem Erhalt der Ware an den Händler zu überweisen. Spätere Beanstandungen und Erstattungen lassen sich bei Vorkasse oft schwer durchsetzen.



Welche Bezahlverfahren sind beim Online Einkauf sicher?

Zahlung über Kreditkarte

Visa Secure oder Mastercard – Beim Bezahlprozess solltet Ihr darauf achten, sichere Bezahlprozesse auszuwählen. Mit der VR-SecureCARD App könnt Ihr die Zahlung direkt in der App oder per SMS inklusive der individuellen TAN auf Euer Mobiltelefon freigeben, um Online-Zahlungen mit der Kreditkarte zu schützen.



Zahlung per PayPal

PayPal bietet einen Käuferschutz per Treuhandverfahren an, wenn die Ware nicht geliefert wurde oder nicht der Beschreibung entspricht. Ihr erhaltet den Verkaufspreis und die Versandkosten zurück.

<https://www.paypal.com/de/webapps/mpp/paypal-safety-and-security>



Welche Bezahlverfahren sind beim Online Einkauf sicher?

Zahlung per Rechnung

Erst nach dem Erhalt der Ware wird der Rechnungsbetrag beglichen – das gibt Euch 100 % Sicherheit.



Zahlung per SEPA Lastschrift

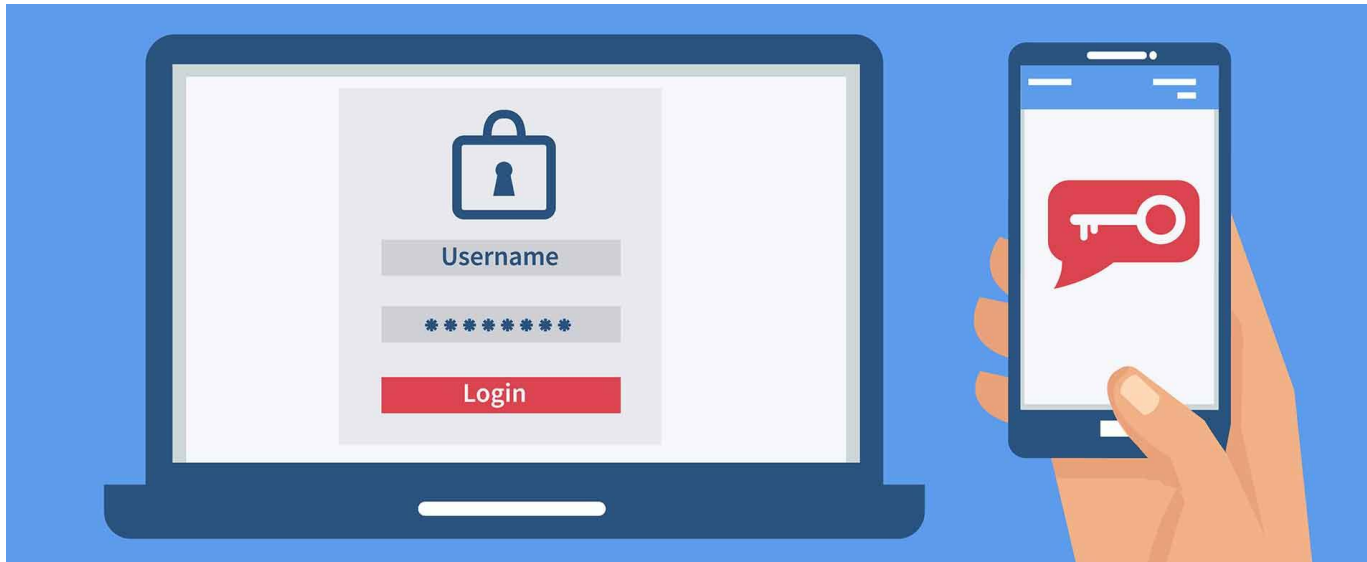
Eine Zahlung per SEPA Lastschrift kann von dem Käufer bei Beanstandung oder nicht gelieferter Ware immer zurückgebucht werden.



Die 2-Faktor Authentifizierung bringt zusätzliche Sicherheit bei der Zahlung

Mit der 2-Faktor Authentifizierung habt Ihr noch mehr Sicherheit beim Einkaufen. Hier ist das Prinzip, dass eine Zahlung immer über **zwei Wege** bestätigt werden muss:

- Zum Beispiel den **Login mit Eurem Passwort und einer SMS**, die Euch auf Euer Mobiltelefon geschickt wird, oder
- in einer **vom Anbieter zur Verfügung gestellten App** angezeigt wird.



Welches Bezahlungssystem ist das Beste?

1

Klarna™

Mit **Klarna** kannst Du deine Bestellungen per

- Sofortüberweisung
- Lastschrift oder
- Kreditkarte

sofort bezahlen.

All Deine Einkäufe kannst Du jederzeit in der **Klarna** App einsehen und verwalten.

Ist es sicher mit Klarna zu bezahlen?

Bei Trustpilot haben über 46.000 Nutzer bereits bewertet. Derzeit kommt **Klarna** dort auf eine Wertung von 4,2 (von 5 maximalen) Sternen (Stand: 30.11.2021). Auch in den Google-Rezensionen wird **Klarna** mit 4,9 von 5 Sternen von Nutzern als sehr zuverlässig und seriös bewertet.

Wie funktioniert das Bezahlen mit Klarna?

Über die **Klarna App** kann der User angeben, wenn er ein Produkt retournieren möchte, und ist die Retoure erstmal angekündigt, pausiert die dazugehörige Rechnung. Wird nur ein Teil des Einkaufs zurückgeschickt, so wird die Rechnung ebenfalls automatisch aktualisiert.

Für weitere Informationen über Klarna suche wie folgt mit Google



Oder schreibe im Suchfeld
Was ist Klarna

https://www.youtube.com/watch?v=BVT_Xmvz_OE&t=4s

Welches Bezahlungssystem ist das Beste? 2



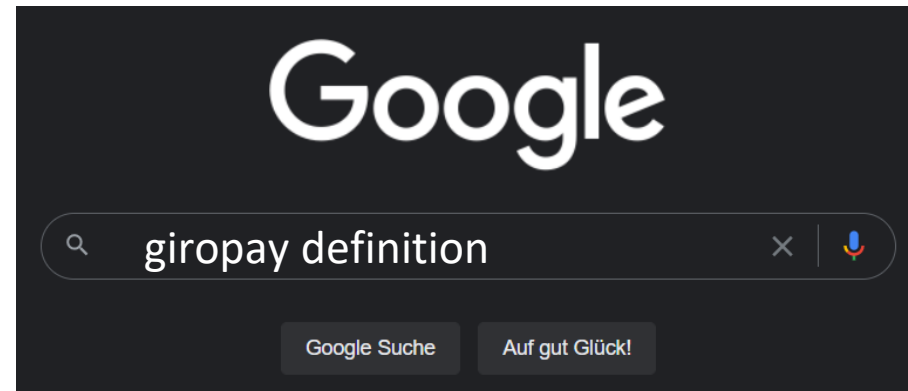
▪ Was ist giropay Zahlungsart?

giropay ist ein Online-Bezahlverfahren, das eine schnelle, einfache und sichere Bezahlung von Waren und Dienstleistungen im Internet per Online-Überweisung ermöglicht. Es wurde im Februar 2006 von Teilen der deutschen Kreditwirtschaft gegründet.

▪ Was muss ich bei giropay beachten?

giropay basiert auf dem Online-Banking mit PIN und TAN und ermöglicht die Bezahlung per Online-Überweisung. Sie benötigen für die Zahlung mit **giropay** lediglich ein Girokonto mit Online-Banking-Zugang. Eine Registrierung bei Ihrer Bank oder Sparkasse für die Nutzung von **giropay** ist nicht nötig.

Für weitere Informationen über giropay suche wie folgt mit Google



Oder schreibe im Suchfeld
Was ist giropay

https://www.youtube.com/watch?v=BVT_Xmvz_OE&t=4s

Welches Bezahlungssystem ist das Beste? 3



Was ist PayPal und wie funktioniert es?

PayPal ist ein Bezahlungsdienst, mit dem man online seine Einkäufe bezahlen kann. Dafür erstellt man ein PayPal-Konto und hinterlegt dort beispielsweise seine Bankdaten. Bei einer Online-Bezahlung per PayPal zieht PayPal dann den nötigen Betrag automatisch von eurem Bankkonto ab und überweist ihn zum Verkäufer.

Übersetzt **bedeutet PayPal** "Bezahlungsfreund"

Suche mit Google nach den folgenden Schlagwörtern

Paypal definition

um die Antworten auf die rechts aufgeführten Fragen zu erhalten.

Was ist PayPal und wie funktioniert es?

Was heißt PayPal auf Deutsch?

Ist es sicher mit PayPal zu bezahlen?

Was sind die Vorteile von PayPal?

Wie hoch sind die Gebühren bei PayPal?

Was braucht man um ein PayPal-Konto zu eröffnen?

Wie verdient man mit PayPal Geld?

Was bedeutet bei PayPal an Freunde senden?

Wie lange dauert es bis über PayPal Geld ankommt?

Warum ist PayPal nicht sicher?

Wie sicher ist PayPal bei Privatverkauf?

Wer zahlt den Käuferschutz bei PayPal?

Handy absichern

Kleines Einmaleins der Sicherheit

Ein Smartphone ist heutzutage nichts anderes als ein mobiler Computer - und dementsprechend genauso anfällig für Viren, Trojaner oder Malware. Es gibt jedoch einige Einstellungen, die Du vornehmen kannst, um Dein (Android)-Handy sicherzumachen. Einige davon sogar ohne Drittsoftware.



Kleines Einmaleins der Sicherheit

Möchtest Du Dein (Android)-Handy absichern, dann benötigst Du nicht unbedingt Drittsoftware – dennoch wird es empfohlen. Denn nur ein richtiger Virenschutz lässt Dich im Netz sicher surfen. Aber auch Dein Userverhalten bestimmt, wie anfällig Du für Schadsoftware, Betrüger und Co. bist.



10 Tipps, wie Du Dein Handy richtig absichern kannst

1

1. PIN oder Passwort statt Muster. Schütze Dich mit dem richtigen Sperrtyp.
2. Regelmäßige Backups. Sichere Deine Daten vor Systemcrashes oder Verlust in einer Cloud oder auf Deinem Rechner.
3. Manuelle WLAN-Verbindung. Entscheide stets selbst, mit welchem WLAN Du Dich verbindest und deaktiviere die automatische WLAN-Netzsuche.
4. Überprüfe die Berechtigungen Deiner Apps. Unter Einstellungen - Anwendungen kannst Du prüfen, welche Apps wie auf Dein Smartphone zugreifen. Nicht alle Apps brauchen Deine Kamera oder Dein Mikrofon, schalte diese manuell aus.
5. Lade Apps stets über den Google Play Store (Android). Dieser scannt vorab, ob eine App Schadsoftware mitbringt oder nicht.



10 Tipps, wie Du Dein Handy richtig absichern kannst

2

6. Surfe nur auf Deinen bekannten Seiten. Bist Du Dir nicht sicher, ob Du diesen oder jenen Link wirklich anklicken kannst, dann lasse es zur Sicherheit lieber.
7. Installiere einen Virenschutz. Mit diesem kannst Du regelmäßig Dein Gerät auf Malware und Co. überprüfen und diese, falls nötig, entfernen lassen.
8. Lösche unbekannte SMS mit Links. Kommt Dir eine Nachricht unbekannt vor, dann solltest Du diese ignorieren. Ähnlich wie Spam-Mails kannst Du auch Spam-SMS erhalten.
9. Werbeanrufe ignorieren. Manch unbekannte Nummer kann eine Bandansage oder ein Werbeanruf sein. Falls Du doch einmal rangehen solltest, lege besser sofort wieder auf.
10. VPN im öffentlichen Netz. Nutze einen VPN-Client, wenn Du im öffentlichen WLAN digital unterwegs sind.



Bei Diebstahl oder Verlust: Smartphone mit PIN sichern

Auch wenn Du den besten Virenschanner auf Deinem (Android)-Smartphone installiert hast, bei Geräteverlust wird Dir dieser auch nur bedingt weiterhelfen. Der erste Schritt beim Absichern Deines Handys ist der PIN, besser noch das Passwort.

- Unter Einstellungen - Sicherheit - Sperrtyp kannst Du wählen, wie Du Dein Smartphone entsperren möchtest. Den besten Schutz bietet das Passwort. Wer jedoch nicht jedes Mal einen Zahlen- und Buchstaben-Code eingeben möchte, wenn er auf sein Handy guckt, sollte zumindest eine PIN einstellen.
- Auch die Funktion Automatisch sperren sollte aktiviert sein. Hier sperrt sich Dein Smartphone wenige Sekunden, nachdem Du den Bildschirm deaktiviert haben.
- Möchtest Du dennoch auf Nummer Sicher gehen und hast ein Passwort aktiviert, dann musst Du dieses nicht zwangsläufig immer eingeben. Mit der Funktion Smart Lock gibst Du Deinem Handy zu verstehen, dass es sich Zuhause nicht sperren muss.



Android-(Handy) und Sicherheit: Vieles ist vorinstalliert

Möchtest Du Dich gegen Datenklau absichern, dann kannst Du auch ohne zusätzliche Programme bereits einige Sicherheitslücken schließen. Denn der vorinstallierte Google Play Store, über den Du nahezu alle Apps beziehen kannst, hat viele Features inklusive - wenn Du diese auch nutzen möchtest.

- Automatische Aktualisierung:
Damit Deine Apps auch immer auf dem neuesten Sicherheitsstand sind, müssen sich diese regelmäßig updaten. Dies ist grundsätzlich voreingestellt.
- Unter Einstellungen findest Du die Automatischen App-Updates. Du kannst hier zudem einstellen, dass Updates nur im WLAN installiert werden sollen. Das spart Datenvolumen.



Weiteres Feature aus dem Google Play Store: Play Protect

Google bringt mit Play Protect bereits ein Programm mit, das vermeintlich unsichere Apps abblockt und regelmäßig auf Sicherheitsstandards überprüft. Ab Android 8 ist dies inklusive. Darüber hinaus solltest Du folgende Dinge beachten:

- Play Protect findest Du ebenfalls in Deinem Google-Play-Store-Profil. Hier siehst Du einen Überblick, welche Apps zuletzt gescannt wurden und ob Schadsoftware entdeckt wurde. Überprüfe in den Einstellungen, dass die Haken für Apps scannen und Schadsoftware erkennen aktiviert sind.
- Darüber hinaus solltest Du Drittanbietern das Installieren von Apps untersagen. In Deinen Smartphone-Einstellungen findest Du unter (Geräte-)Sicherheit den Menüpunkt Unbekannte Apps installieren. Hier ist es idealerweise nur dem Google Play Store (meist als Google Chrome aufgeführt) erlaubt, Apps zu installieren.



Google Play



Google Play
Protect

Antiviren-Programme: Beim PC ein Muss, beim Handy auch

Auch wenn Android bereits einige Sicherheiten mitbringt, ist ein Antiviren-Scanner auch auf dem Handy Pflicht. Denn Play Protect bringt nur einen rudimentären Schutz mit sich.

Folgende Beispiele machen Antiviren-Programme zu Sicherheits-Allerwählter:

- **Diebstahlschutz**: Mit solch einer Funktion kannst Du Dein Gerät bei Verlust oder Diebstahl sperren. Mittels GPS-Daten kannst Du Dein Handy dann auch wiederfinden oder die Informationen mit der Polizei teilen.
- **Zugriffsberechtigungen prüfen**: Viele Apps bieten an, zu überprüfen, welche Apps Zugriff auf Dein Gerät hat. Nicht jedes Programm muss auf Deine Kontaktdaten zugreifen können. Diesen Missbrauch kannst Du so unterbinden.
- **Verschlüsselung**: Daten können mit Antiviren-Software verschlüsselt werden. Nutzt Du Dein Smartphone beruflich, kannst Du so sensible Daten verstecken.
- **Backups**: Diese Funktion ist bei fast allen Apps inklusive. Am PC oder Laptop ist das schon längst üblich! die Daten Deines Handys solltest Du auch per Backup sichern.
- **Spam-Blocker**: Seien es Anrufe oder SMS - mit einem Spam-Blocker kannst Du unerwünschte und nervige Bandansagen unterdrücken lassen.



Online-Banking

Worauf muss man beim Online-Banking achten? [1]

Beim Online-Banking ist es wichtig, einige grundlegende Sicherheitsvorkehrungen zu beachten, um persönliche Daten und Konten vor Betrug oder Missbrauch zu schützen. Hier sind die wichtigsten Punkte:

- **Sichere Verbindung nutzen**
 - Achte darauf, dass die URL der Bank mit "**https://**" beginnt und ein Schlosssymbol in der Adressleiste des Browsers angezeigt wird.
 - Vermeide Online-Banking in öffentlichen WLAN-Netzwerken. Nutze stattdessen eine sichere, private Verbindung oder ein VPN.
- **Starke Zugangsdaten**
 - Wähle ein starkes Passwort mit einer Kombination aus Buchstaben, Zahlen und Sonderzeichen.
 - Ändere das Passwort regelmäßig und verwende nicht dasselbe Passwort für andere Dienste.
- **Zwei-Faktor-Authentifizierung (2FA)**
 - Aktiviere, falls möglich, die Zwei-Faktor-Authentifizierung. Dabei wird zusätzlich zum Passwort ein einmaliger Code benötigt, der beispielsweise per SMS oder über eine App generiert wird.
- **Offizielle Banking-Apps und Webseiten**
 - Nutze nur die offiziellen Apps oder Webseiten der Bank.
 - Lade Apps ausschließlich aus vertrauenswürdigen Quellen wie dem Apple App Store oder Google Play Store herunter.



Worauf muss man beim Online-Banking achten? [2]

- **Phishing-Mails vermeiden**
 - Reagiere nicht auf E-Mails oder Nachrichten, die dich auffordern, persönliche Daten einzugeben, Passwörter zu ändern oder Links zu folgen.
 - Banken fragen sensible Daten niemals per E-Mail oder Telefon ab.
- **Software aktuell halten**
 - Halte Betriebssystem, Browser und Banking-App stets auf dem neuesten Stand, um Sicherheitslücken zu vermeiden.
 - Installiere eine zuverlässige Antiviren-Software und aktiviere die Firewall.
- **Konto regelmäßig überprüfen**
 - Kontrolliere deine Kontoauszüge regelmäßig auf ungewöhnliche Transaktionen.
 - Melde verdächtige Aktivitäten sofort der Bank.



Worauf muss man beim Online-Banking achten? [3]

- **Vorsicht bei fremden Geräten**
 - Vermeide Online-Banking auf fremden Geräten oder Computern, da diese mit Schadsoftware infiziert sein könnten.
 - Logge dich nach der Nutzung immer vollständig aus.
- **Zeitbeschränkung für Sitzungen**
 - Einige Banken bieten automatische Sitzungs-Timeouts an. Stelle sicher, dass diese Funktion aktiviert ist, um unbefugten Zugriff zu verhindern.
- **Backups und Notfallmaßnahmen**
 - Speichere wichtige Informationen wie Kontaktdaten der Bank für Notfälle.
 - Melde verlorene Geräte sofort, falls darauf Banking-Apps installiert sind, und lasse das Konto sperren.

Fazit

Eine Kombination aus Vorsicht, der Nutzung aktueller Technologie und dem Bewusstsein für potenzielle Gefahren kann das Risiko beim Online-Banking deutlich minimieren.



Demo Online-Banking chipTAN [1]

<https://www.sparkasse-karlsruhe.de/de/home/login-online-banking/demo-online-banking-chiptan.html>

Privatkunden Firmenkunden Leichte Sprache Gebärdensprache

Sparkasse Karlsruhe [Online-Abschluss](#) [Produkte](#) [Private Banking](#) [Junge Kundinnen und Kunden](#) [Service-Center](#) [Ihre Sparkasse](#) [Karriere](#)




Demo Online-Banking chipTAN

Ihre Zugangsdaten
Testen Sie selbst. Verwenden Sie dazu bitte folgende Zugangsdaten:

Anmeldename	chipDEMO
Online-Banking-PIN	12345
TAN	beliebige 6-stellige Zahl

Anmeldename
chipDEMO

Online-Banking-PIN
12345 Ausblenden

Demo Online-Banking chipTAN [2]

Privatkunden Firmenkunden

Leichte Sprache Gebärdensprache

Sparkasse Karlsruhe

Online-Abschluss Produkte Private Banking Junge Kundinnen und Kunden Service-Center Mehr > Suche Online-Banking Abmelden

Anmeldename
chipDEMO

Online-Banking-PIN
..... [Anzeigen](#)

Weitere Informationen ⓘ

Anmelden

[Sicherheitshinweise](#) · [Zugangsdaten vergessen](#)

☎
💬
✉

Demo Online-Banking chipTAN [3]

The screenshot displays the Sparkasse Karlsruhe online banking interface. The top navigation bar includes the Sparkasse Karlsruhe logo, account type selection (Privat, Geschäftlich), search, start page, and logout options. The main content area features a 'Finanzübersicht' section with a balance of 1.000 EUR, a notification for pending orders, and a forecast for the account balance by the end of the month (30.09.2025) also at 1.000 EUR. The left sidebar contains navigation links for account overview, planner, offers, and bonus programs, as well as a bottom menu for messages, profile, and help.

Sparkasse Karlsruhe

Privat | Geschäftlich

Suche | Startseite | Abmelden

Finanzübersicht ⓘ

Überweisung + | Favoriten ▾

Guten Morgen Max Mustermann

Offene Aufträge
Sie haben Aufträge zur Freigabe erhalten

1 weiterer Hinweis ▾

Ihre Kontostandprognose für ⓘ
Privatgirokonto - Lebensmittel

heute 1.000 EUR | 30.09.2025 1.000 EUR

Voraussichtliche Entwicklung
Kontostand bis zum Monatsende
[Erwartete Umsätze prüfen](#)

Nachrichten | Profil und Einstellungen | Hilfe und Kontakt


Demo Online-Banking chipTAN [4]

The screenshot displays the Sparkasse Karlsruhe online banking interface. At the top left, the Sparkasse Karlsruhe logo is visible. In the top right corner, there is a button labeled "Abmelden". The main heading is "Überweisung" with an information icon. Below this, the account details for "Privatgirokonto - Lebensmittel" are shown, including the IBAN "DE97 6605 0101 0000 1234 56" and a "Konto wechseln" link. The transfer amount is "1.000,00 EUR". A search bar for "Empfänger oder IBAN eingeben" is present, along with a "Rechnung hochladen" button. Below the search bar, there is a button for "Daten aus der Vorlage übernehmen" with the subtext "Überweisungsdaten aus der Vorlage übernehmen (optional)". The footer contains a language selector set to "Deutsch", a list of links including "AGB", "Cookie-Einstellungen anpassen", "Datenschutz", "Impressum", "Preise und Hinweise", "Kontakt", "Filialen A-Z", "Geldautomaten A-Z", "Barrierefreiheit", and "Barriere melden", and a small icon in the bottom left corner.

Sparkasse
Karlsruhe


Abmelden

Überweisung ⓘ

 **Privatgirokonto - Lebensmittel** ⓘ
DE97 6605 0101 0000 1234 56




[Konto wechseln](#) **1.000,00 EUR** ⓘ

Empfänger oder IBAN eingeben [Rechnung hochladen](#)

 **Daten aus der Vorlage übernehmen** →
Überweisungsdaten aus der Vorlage übernehmen (optional)

Deutsch ▾ | [AGB](#) [Cookie-Einstellungen anpassen](#) [Datenschutz](#) [Impressum](#) [Preise und Hinweise](#) [Kontakt](#)
[Filialen A-Z](#) [Geldautomaten A-Z](#) [Barrierefreiheit](#) [Barriere melden](#)

Demo Online-Banking chipTAN [5]

 **Privatgirokonto - Lebensmittel**  Konto wechseln **1.000,00 EUR** 
DE97 6605 0101 0000 1234 56


IBAN
DE49 8205 6060 3605 0070 57 · Demo-Institut

Empfänger
Haendler 1


Betrag
0,10 EUR


Skontorechner

Verwendungszweck (optional)
A-Nr 24124/12

Zahlungsart (optional)
Keine Angabe 

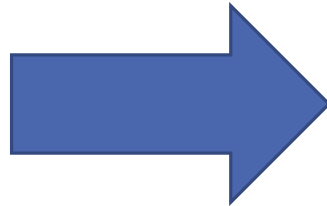
Dauerauftrag als Vorlage speichern


Ausführungsart
Standard 



Ausführungsdatum (Optional)
nächstmöglich 


Buchung auf dem Empfängerkonto spätestens bis Ende übernächster Geschäftstag.

Überweisung prüfen



Überweisung 

 **Privatgirokonto - Lebensmittel** **1.000,00 EUR** 
DE97 6605 0101 0000 1234 56

Zusammenfassung Ihres Auftrags 

Empfänger
Haendler 1
DE49 8205 6060 3605 0070 57
Demo-Institut

Betrag
0,10 EUR

Verwendungszweck
A-Nr 24124/12

Ausführung
29.09.2025 (Standard)


[Bedingungen für den Überweisungsverkehr](#)

Weiter

Demo Online-Banking chipTAN [6]

Zusammenfassung Ihres Auftrags

[chipTAN QR](#) [chipTAN optisch](#) [chipTAN manuell](#)



- Stecken Sie Ihre Karte in den TAN-Generator und drücken Sie ggf. die für den Scan erforderliche Taste.
- Scannen Sie den nebenstehenden QR-Code mit Ihrem TAN-Generator ein.
- Beachten Sie bitte die Anzeige des TAN-Generators.
- Zur Freigabe des Auftrages bitte die im TAN-Generator angezeigte TAN eingeben und absenden.


Jetzt würden Sie normalerweise den TAN-Generator vor den QR-Code halten (dazu können Sie in der Demoanwendung eine beliebige KundenCard Ihres Institutes zur TAN-Erzeugung verwenden). Dabei werden Ihre spezifischen Auftragsdaten an den Leser übergeben und müssen dort von Ihnen kontrolliert werden. Hier im Demokonto werden beispielhaft die Daten für einen Überweisungsauftrag an das Empfängerkonto DE49 8205 6060 3605 0070 57 mit dem Betrag 123,45 dargestellt.

Alternativ können Sie den Demo-Auftrag mit jeder beliebigen 6-stelligen Zahlenkombination absenden, eine Nutzung des TAN-Generators und Ihrer Karte ist nicht notwendig.

Geben Sie die TAN ein, um fortzufahren:

• • • • • •

[Bedingungen für den Überweisungsverkehr](#)



- Stecken Sie Ihre Karte in den TAN-Generator und drücken Sie ggf. die für den Scan erforderliche Taste.
- Scannen Sie den nebenstehenden QR-Code mit Ihrem TAN-Generator ein.
- Beachten Sie bitte die Anzeige des TAN-Generators.
- Zur Freigabe des Auftrages bitte die im TAN-Generator angezeigte TAN eingeben und absenden.

Jetzt würden Sie normalerweise den TAN-Generator vor den QR-Code halten (dazu können Sie in der Demoanwendung eine beliebige KundenCard Ihres Institutes zur TAN-Erzeugung verwenden). Dabei werden Ihre spezifischen Auftragsdaten an den Leser übergeben und müssen dort von Ihnen kontrolliert werden. Hier im Demokonto werden beispielhaft die Daten für einen Überweisungsauftrag an das Empfängerkonto DE49 8205 6060 3605 0070 57 mit dem Betrag 123,45 dargestellt.

Alternativ können Sie den Demo-Auftrag mit jeder beliebigen 6-stelligen Zahlenkombination absenden, eine Nutzung des TAN-Generators und Ihrer Karte ist nicht notwendig.

Geben Sie die TAN ein, um fortzufahren:

1 2 3 4 5 6


▲ Bitte befüllen Sie das Feld "TAN".

[Bedingungen für den Überweisungsverkehr](#)




⚠

Der Auftrag wurde entgegengenommen.
Achtung: Der Auftrag wurde nicht ausgeführt (Demo-Zugang).
29. September 2025 um 09:22:42 Uhr

 **Privatgirokonto - Lebensmittel**
DE97 6605 0101 0000 1234 56

Weitere Überweisung **Zur Finanzübersicht**

Zusammenfassung Ihres Auftrags

 [Druckansicht](#)

Demo Online-Banking chipTAN (nach der Anmeldung)

The screenshot displays the Sparkasse Karlsruhe online banking interface. The top navigation bar includes the Sparkasse Karlsruhe logo, a user profile switch between 'Privat' and 'Geschäftlich', search and home icons, and a 'Start' button. A secondary bar contains a red 'Überweisung +' button and a 'Favoriten' dropdown menu. The main content area is titled 'Finanzübersicht' and includes a greeting for 'Max Mustermann'. A notification box indicates 'Offene Aufträge' (open orders) with a sub-message 'Sie haben Aufträge zur Freigabe erhalten'. Below this, a section for 'Ihre Kontostandprognose für Privatgirokonto - Lebensmittel' shows an 'Aktueller Kontostand' of 1.000,00 EUR as of 11.12.2023 and a 'Kontostandprognose' of 2.522 EUR for 31.12.2023. The 'Konten und Karten' section lists three accounts: 'Privatgirokonto - Lebensmittel' (1.000,00 EUR), 'Firmenkonto' (-125,50 EUR), and 'Tagesgeld - Rücklage' (18.235,00 EUR). A left sidebar contains navigation links for 'Finanzübersicht', 'Finanzplaner', 'Nachrichten', 'Einstellungen', and 'Hilfe & Kontakt'.

Sparkasse Karlsruhe

Privat Geschäftlich

Suche Start Abmelden

Finanzübersicht

Überweisung + Favoriten

Guten Tag Max Mustermann

Offene Aufträge
Sie haben Aufträge zur Freigabe erhalten

2 weitere Hinweise

Ihre Kontostandprognose für
Privatgirokonto - Lebensmittel

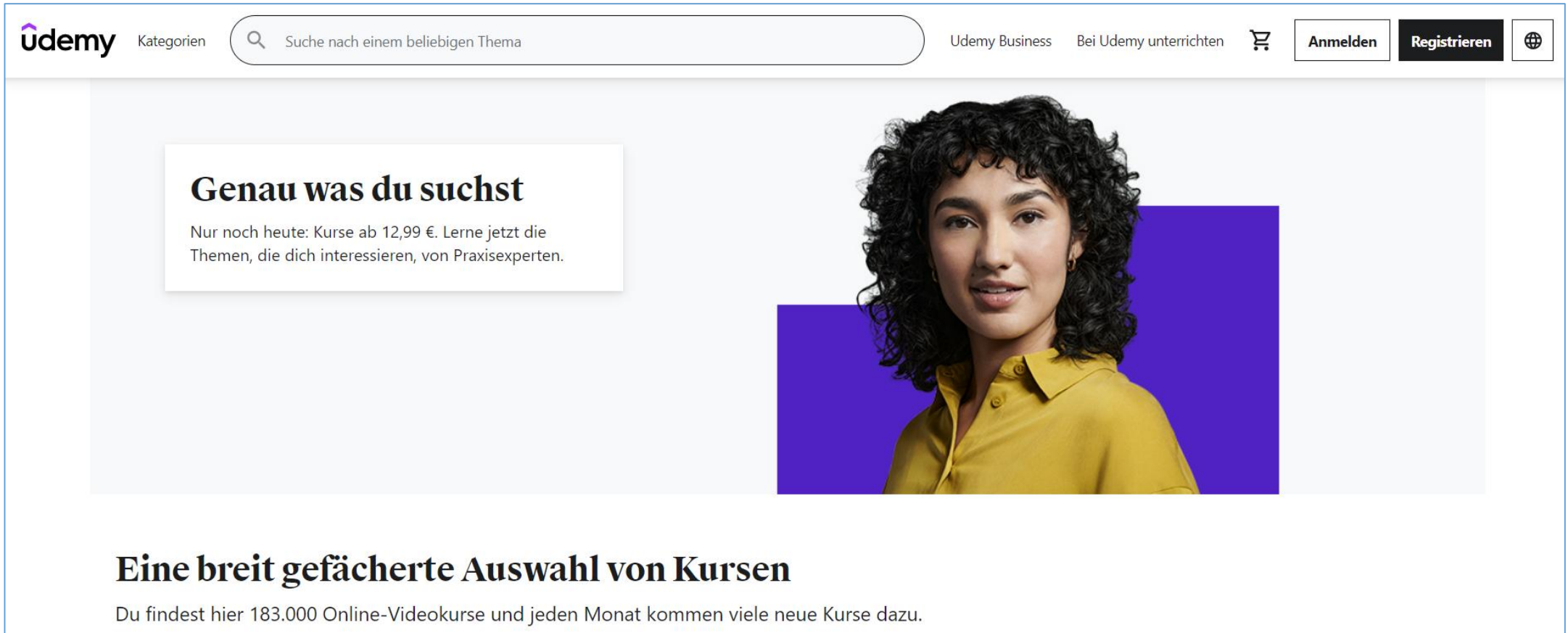
1.000,00 EUR Aktueller Kontostand heute, 11.12.2023	2.522 EUR Kontostandprognose für 31.12.2023
--	--

Konten und Karten

Privatgirokonto - Lebensmittel	DE97 6605 0101 0000 1234 56 • Mustermann, Max	1.000,00 EUR
Firmenkonto	DE84 6605 0101 0000 1299 95 • Test, Tina	-125,50 EUR
Tagesgeld - Rücklage	DE03 6605 0101 0000 2009 05 • Mustermann, Max	18.235,00 EUR

Nachrichten
Einstellungen
Hilfe & Kontakt

Online-Lernplattform



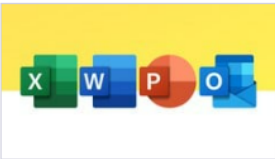




Udeemy Kategorien Udeemy Business Bei Udeemy unterrichten **Anmelden** **Registrieren**

Genau was du suchst
Nur noch heute: Kurse ab 12,99 €. Lerne jetzt die Themen, die dich interessieren, von Praxisexperten.

Eine breit gefächerte Auswahl von Kursen
Du findest hier 183.000 Online-Videokurse und jeden Monat kommen viele neue Kurse dazu.

<https://www.udemy.com/>

Online-Lernplattform

	Microsoft Office 365 - Excel, Word, PowerPoint und Outlook Lerne von den Grundlagen bis zum professionellen Arbeiten alles über Office mit Excel, PowerPoint, Word und Outlook Timothy Meixner, Johannes Ruof 4,5 ★★★★★ (1.906) 40,5 Std. gesamt · 393 Lektionen · Alle Levels Bestseller	22,99 € 149,99 €
	Der Komplette Excel Kurs - Vom Anfänger zum Profi in 50h 11 Kurse in 1: Excel Grundlagen, Diagramme, Pivot, VBA, Power Query, ChatGPT - Vom totalen Anfänger zum Excel Profi Sebastian Glöckner · 275.000+ Teilnehmer, Sebastian Glöckner Karriere-Entwicklung, Sebastian Glöckner... 4,8 ★★★★★ (6.696) 64 Std. gesamt · 470 Lektionen · Alle Levels Bestseller	19,99 € 139,99 €
	Das ganz große Microsoft-Paket - 17 Kurse in einem Paket! Jetzt Windows, Word, PowerPoint, Outlook, Excel, OneNote, OneDrive und weitere 9 Programme noch besser beherrschen! Volker Buntrock 4,3 ★★★★★ (51) 88 Std. gesamt · 658 Lektionen · Alle Levels Bestseller 1 Lektion über „microsoft office“ 👉 1-Klick-Bildschirmaufzeichnung in Microsoft Office-Anwendungen!	14,99 € 89,99 €
	Hol dir Udemy für den Arbeitsplatz Udemy Business ist eine umfassende Weiterbildungsplattform für Unternehmen jeder Größe. Weitere Infos	
	Das ultimative Office 365 Kurs Kompendium für Einsteiger Das ultimative Microsoft Office Kompendium. Lerne alle Grundlagen in Powerpoint, Word, Excel und Outlook! Ben Polland, Sebastian Glöckner · 275.000+ Teilnehmer 4,5 ★★★★★ (351) 28,5 Std. gesamt · 235 Lektionen · Einsteiger:innen	17,99 € 109,99 €

Udemy ist eine große Online-Lernplattform, auf der man Kurse zu fast allen Themenbereichen findet – von Computerkenntnissen bis hin zu Sprachen oder Fotografie.

Als Nutzer kann man dort ganz flexibel lernen, wann und wo man möchte, ohne feste Unterrichtszeiten.

Die meisten Kurse bestehen aus Video-Lektionen, zusätzlichen Materialien wie PDFs oder Tests und sind in verschiedene Schwierigkeitsstufen eingeteilt. Nach dem Kauf eines Kurses hat man lebenslangen Zugriff, also kann man jederzeit erneut darauf zugreifen.

Viele Kurse können auch über die Udemy-App offline angeschaut werden, was besonders praktisch für unterwegs ist.

Am Ende jedes Kurses erhält man ein Teilnahmezertifikat, das sich z. B. bei Bewerbungen oder auf LinkedIn angeben lässt.

Die Preise sind sehr unterschiedlich, aber Udemy bietet regelmäßig starke Rabattaktionen, bei denen viele Kurse nur wenige Euro kosten.

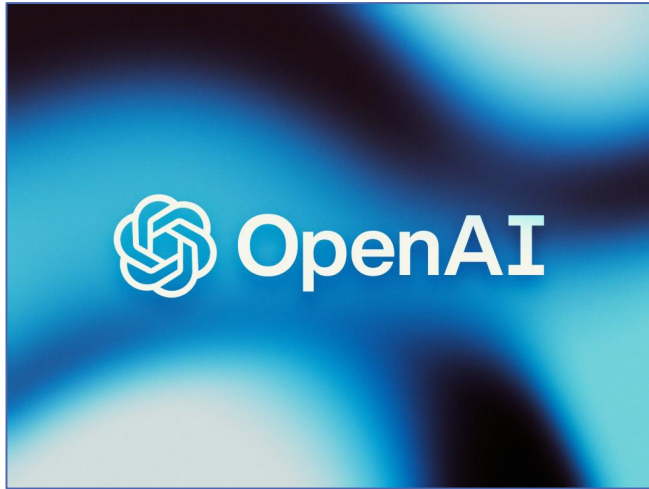
Ein großer Vorteil ist die vielfältige Auswahl und die Möglichkeit, sich ganz individuell weiterzubilden.

Ein Nachteil ist jedoch, dass die Qualität der Kurse schwanken kann, da jeder Trainer Inhalte veröffentlichen darf.

Außerdem sind die Zertifikate nicht staatlich anerkannt, sondern dienen vor allem dem persönlichen oder beruflichen Wissensaufbau.

<https://www.udemy.com/>

Künstliche Intelligenz



<https://chatgpt.com/>



<https://gemini.google.com/>



<https://copilot.microsoft.com/>

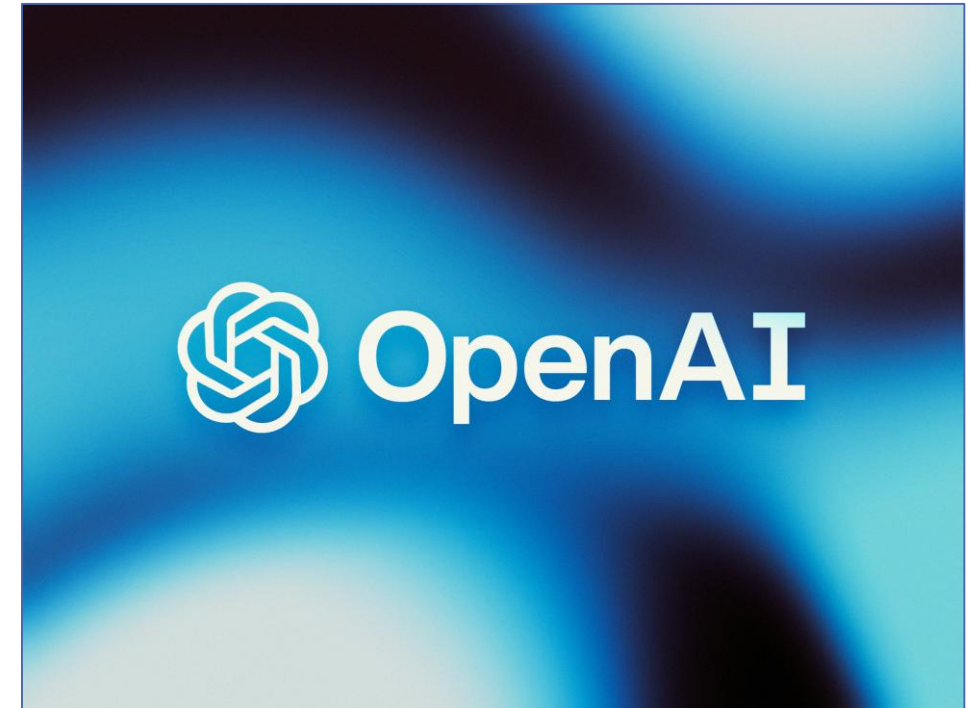
Künstliche Intelligenz im Vergleich ChatGPT, Gemini und Copilot

KI	Internetseite	Wofür gut / Vorteile	Preise	Ohne Account nutzbar?
 ChatGPT (OpenAI)	https://chatgpt.com	Sehr vielseitig, gute Texte & Erklärungen, Lernen, Programmieren, kreative Inhalte	Kostenlos: Ja (Basis) Kostenpflichtig: ChatGPT Plus - 20 €/Monat	 Ja (kostenpflichtig, ohne Login nutzbar)
 Gemini (Google)	https://gemini.google.com	Gute Recherche, Zusammenfassungen, starke Google-Integra-	Kostenlos: Ja (mit Google-Account) Kostenpflichtig: Gemini Advanced ~ 20 € / Monat	 Nein
 Copilot Microsoft Copilot	https://copilot.microsoft.com	Basisfunktionen im Web / Office & Beruf	Kostenlos: Ja (Basis) Kostenpflichtig: Copilot Pro ~ 20 €/Monat Copilot für Microsoft 365 (Business) ~ 30 €/Monat	 Ja, aber... * teilweise ohne Login nutzbar*

Künstliche Intelligenz

Grundverständnis

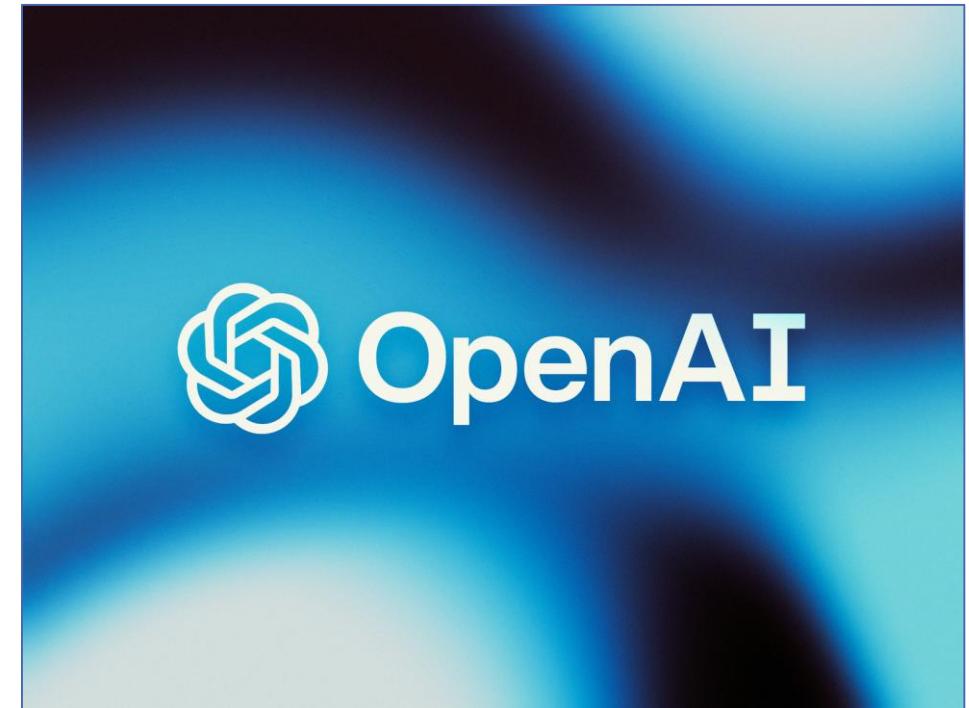
- **Was ist ChatGPT?**
Ein KI-gestützter Chatbot von OpenAI, der Texte versteht und generiert – also antworten, erklären, zusammenfassen, schreiben usw.
- **Was bedeutet GPT?**
„Generative Pre-trained Transformer“ – das Modell ist vortrainiert auf riesige Textmengen und kann dadurch in natürlicher Sprache kommunizieren.
- **Was kann ChatGPT?**
Antworten geben, Texte schreiben, Übersetzen, Zusammenfassen, Programmieren, Brainstorming, Hausaufgabenhilfe, u. v. m.



Künstliche Intelligenz

Nutzung & Funktionen

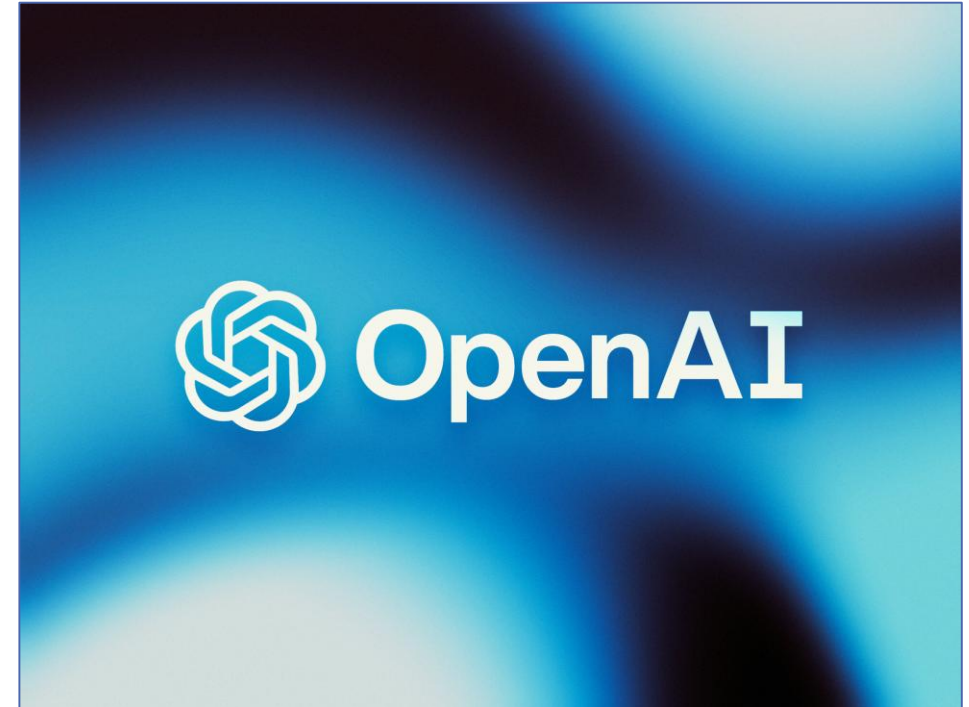
- Benutzeroberfläche ist wie ein Chat
Man schreibt eine Frage oder Aufgabe rein und bekommt direkt eine Antwort.
- Prompt = Eingabe
Alles, was du schreibst, nennt man „Prompt“. Je genauer, desto besser die Antwort.
- Versionsunterschiede (z. B. GPT-3.5 vs. GPT-4)
GPT-4 ist präziser, aktueller und unterstützt oft zusätzliche Funktionen (z. B. Bilderkennung oder Plugins – je nach Abo).
- Chatverlauf speichert Kontexte
Innerhalb eines Chats merkt sich ChatGPT, was ihr vorher besprochen habt – praktisch für tiefergehende Themen.
- Sprache & Ton anpassbar
Man kann ChatGPT bitten, in einfacher Sprache zu antworten, sachlich zu bleiben oder z. B. im Stil einer bestimmten Person zu schreiben.



Künstliche Intelligenz

Was ist (noch) wichtig zu wissen?

- **Nicht immer fehlerfrei**
ChatGPT kann falsche Infos liefern („Halluzination“). Immer kritisch prüfen, vor allem bei Fakten, Zahlen und Quellen!
- **Datenschutz & Privatsphäre**
Persönliche oder sensible Daten sollten nicht eingegeben werden – alles, was du schreibst, kann anonymisiert zur Verbesserung genutzt werden.
- **Offline = Kein aktueller Wissenstand**
Standard-Versionen (ohne Webzugang) haben einen Wissensstand mit einem bestimmten Stand (z. B. GPT-3.5: bis 2021, GPT-4: bis 2023/24, je nach Version).
- **Bezahlversion (ChatGPT Plus)**
Für ca. 20 \$/Monat bekommt man Zugriff auf GPT-4 und zusätzliche Funktionen (z. B. Tools, Dateiupload, Bilderkennung).
- **Gute Prompts = bessere Ergebnisse**
Je klarer und konkreter du bist, desto hilfreicher ist die Antwort. Man kann ChatGPT z. B. auch Rollen geben („Du bist mein Mathelehrer...“).



Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI

1

1. Klarheit & Präzision

Sei so konkret wie möglich: Wer, was, wann, wie, warum

✘ Beispiel: 'Schreib was über Klimawandel'

☑ Beispiel: 'Schreib einen Text (150 Wörter) über die Folgen des Klimawandels in Europa für Schüler der 9. Klasse.'

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



2. Rolle oder Perspektive angeben

Sag der KI, **wer sie sein soll** – das beeinflusst Stil und Tiefe.

„Du bist ein erfahrener Dozent für Erwachsenenbildung. Erkläre einfach, wie KI funktioniert.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



3. Ziel und Zielgruppe definieren

Beschreibe, **wofür** du den Text brauchst und **für wen**.

„Formuliere eine Einladung für Eltern, freundlich, aber professionell.“

„Schreib eine LinkedIn-Post, locker, aber informativ.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



4. Struktur und Format angeben

Wenn du bestimmte Formen brauchst, sag das direkt:

„In Stichpunkten“, „als E-Mail“, „in Tabellenform“, „als Checkliste“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



5. Beispiele oder Stilvorlagen

Wenn du einen bestimmten Stil willst, gib ein Beispiel:

„Schreibe im Stil von Apple-Marketingtexten.“

„Nutze eine ähnliche Tonalität wie in diesem Text: [Beispiel].“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



6. Iterativ vorgehen

Selten ist das erste Ergebnis perfekt.

Nutze Befehle wie:

- „Mach es kürzer / länger / emotionaler / neutraler.“
- „Gib mir drei Varianten.“
- „Fasse die Hauptpunkte zusammen.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



7. Kontext geben

Je mehr Hintergrund du gibst, desto relevanter die Antwort.

„Ich schreibe einen Kursflyer für Senioren, die Anfänger sind.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



8. Negatives Prompten (was du *nicht* willst)

Hilfreich, um Fehlinterpretationen zu vermeiden.

„Vermeide Fachbegriffe und komplizierte Sätze.“

„Bitte ohne Emoji und ohne Du-Ansprache.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI



9. Schritt-für-Schritt-Anweisungen

Gerade bei komplexen Aufgaben:

„Erstelle zuerst eine Gliederung. Warte dann auf mein OK, bevor du den Text schreibst.“

Worauf sollte man beim Prompten achten?

Eine kompakte Übersicht für effektives Prompten mit KI

10

10. Feinschliff durch gezieltes Nachfragen

Wenn du etwas bekommst, das fast passt:

„Mach den Ton etwas motivierender, aber nicht zu werblich.“

„Kürze den Mittelteil um 30 %, behalte aber die wichtigsten Fakten.“

ChatGPT – Beispiel 1

Prompt

Wie kann ich dir helfen?

Ich möchte meine Mietwohnung kündigen, weiß aber nicht, wie ich das Schreiben formulieren soll. Es ist eine normale Kündigung, keine Sonderkündigung. Kannst du mir bitte ein einfaches Kündigungsschreiben erstellen, das ich meinem Vermieter schicken kann? Die Kündigungsfrist soll eingehalten werden, und ich möchte auch um eine schriftliche Bestätigung bitten. Meine Adresse ist [deine Adresse], die des Vermieters ist [Adresse Vermieter], und ich möchte zum [Datum] kündigen. Danke :-)

+ 🌐 Suche 🔍 Deep Research ⋮



Antwort ChatGPT

Klar, hier ist ein einfaches, sachliches Kündigungsschreiben, das du verwenden kannst. Du brauchst nur die eckigen Platzhalter durch die passenden Daten zu ersetzen:

[Dein Vor- und Nachname]

[Deine Adresse]

[PLZ Ort]

An:

[Name des Vermieters / der Vermieterin]

[Adresse Vermieter]

[PLZ Ort]

Ort, Datum

Kündigung des Mietvertrags für die Wohnung in [Straße, Hausnummer, PLZ Ort]

Sehr geehrte Damen und Herren,

hiermit kündige ich den Mietvertrag für die oben genannte Wohnung fristgerecht zum [Datum].

Ich bitte Sie, mir den Erhalt dieses Schreibens sowie das Beendigungsdatum des Mietverhältnisses schriftlich zu bestätigen.

Bitte teilen Sie mir auch mit, wann die Wohnungsübergabe stattfinden kann.

Mit freundlichen Grüßen

[Dein Vor- und Nachname]

(Unterschrift – wenn du das Schreiben postalisch versendest)

ChatGPT – Beispiel 2

Prompt

Wie kann ich dir helfen?

Ich bin neu in Deutschland und möchte so schnell wie möglich Deutsch lernen, damit ich mich im Alltag besser verständigen kann. Kannst du mir bitte Tipps und eine einfache Lernstrategie empfehlen, die mir wirklich hilft? Danke :-)

+ 🌐 Suche 🔍 Deep Research ⋮



Antwort ChatGPT

Willkommen in Deutschland! 😊 Es ist super, dass du motiviert bist, schnell Deutsch zu lernen – das ist der wichtigste Schritt! Ich gebe dir gern eine einfache, effektive Lernstrategie mit konkreten Tipps, die dir im Alltag wirklich helfen können.

🎯 Ziel: Alltagsdeutsch so schnell wie möglich lernen

✅ 1. Jeden Tag 30 Minuten aktiv Deutsch lernen

Nutze kurze, regelmäßige Lerneinheiten – das ist besser als einmal pro Woche stundenlang.

Apps:

- 📱 *Duolingo, Babbel, DeutschAkademie, Mondly* – sehr gut für den Einstieg.
- 🎧 *Anki oder Quizlet* für Karteikarten – so lernst du Vokabeln spielerisch.

✅ 2. Höre jeden Tag Deutsch – passiv

Auch wenn du nicht alles verstehst: Dein Gehirn gewöhnt sich an die Sprache.

Empfehlungen:

- 🎧 Podcasts: z. B. *„Deutsch – warum nicht?“* oder *„Slow German“*
- 📺 Serien mit deutschem Untertitel: z. B. *„Extra auf Deutsch“* (lustige Lernserie auf YouTube)

ChatGPT – Beispiel 2

Prompt

Wie kann ich dir helfen?

Ich bin neu in Deutschland und möchte so schnell wie möglich Deutsch lernen, damit ich mich im Alltag besser verständigen kann. Kannst du mir bitte Tipps und eine einfache Lernstrategie empfehlen, die mir wirklich hilft? Danke :-)

+ 🌐 Suche 🔍 Deep Research ⋮



Antwort ChatGPT

✅ 3. Sprich von Anfang an – keine Angst vor Fehlern

Fehler sind Teil des Lernprozesses. Sprich mit Menschen – auch wenn du nur wenige Wörter kennst.

Ideen:

- 🗣️ Sprich mit Nachbarn, im Supermarkt, beim Arzt: „Ich lerne Deutsch. Können Sie langsam sprechen?“
- 🤝 Sprach-Tandem (z.B. über die App *Tandem* oder *HelloTalk*) – du hilfst mit deiner Sprache, andere helfen dir mit Deutsch.
- 📺 Deutschkurse beim VHS (Volkshochschule) oder in deiner Stadt – oft günstig oder kostenlos.

✅ 4. Lerne zuerst das, was du im Alltag brauchst

Keine langen Grammatiklisten! Lerne Sätze, die du täglich brauchst:

Deutsch

Bedeutung

Wie heißt du?

What's your name?

Ich komme aus ...

I'm from ...

Ich hätte gern einen Kaffee, bitte

I would like a coffee, please

Wo ist die Toilette?

Where is the bathroom?

Was kostet das?

How much is this?

ChatGPT – Beispiel 2

Prompt

Wie kann ich dir helfen?

Ich bin neu in Deutschland und möchte so schnell wie möglich Deutsch lernen, damit ich mich im Alltag besser verständigen kann. Kannst du mir bitte Tipps und eine einfache Lernstrategie empfehlen, die mir wirklich hilft? Danke :-)

+  Suche  Deep Research ...



Antwort ChatGPT

✅ 5. Starte ein kleines Lern-Tagebuch

Schreib jeden Tag 2–3 Sätze auf Deutsch – z. B. „Heute war ich einkaufen. Ich habe Brot gekauft.“
Das hilft beim Denken in der Sprache.

📅 Vorschlag für deine erste Lern-Woche

Tag	Aktiv lernen	Passiv hören	Sprechen / Schreiben
Montag	Duolingo 15 Min + 10 Vokabeln	Podcast „Slow German“ (15 Min)	Begrüßung auf Deutsch üben
Dienstag	App + Karteikarten (Essen/Wohnen)	YouTube-Serie (z. B. „Extra“)	Im Laden „Ich hätte gern ...“ sagen
Mittwoch	Kurzer Text lesen (Kinderbuch-Niveau)	Musik auf Deutsch hören	3 Sätze im Tagebuch schreiben
Donnerstag	Grammatik: Personalpronomen „ich/du“	Film mit deutschem Untertitel	Tandem-App ausprobieren
Freitag	Neue Wörter aus dem Alltag notieren	Podcast beim Spazieren	Fragen üben: „Wo ist ...?“
Weekende	Wiederholen + Spaß mit Spiel/App	Lieblingslied auf Deutsch hören	Mit jemandem über dein Wochenende reden

ChatGPT – Beispiel 2

Prompt

Wie kann ich dir helfen?

Ich bin neu in Deutschland und möchte so schnell wie möglich Deutsch lernen, damit ich mich im Alltag besser verständigen kann. Kannst du mir bitte Tipps und eine einfache Lernstrategie empfehlen, die mir wirklich hilft? Danke :-)

+ 🌐 Suche 🔍 Deep Research ⋮



Antwort ChatGPT

Wenn du möchtest, kann ich dir auch:

- eine **persönliche Lernkarte** (PDF oder PowerPoint) erstellen
- **alltägliche Dialoge** schreiben
- oder dich bei bestimmten Themen begleiten (z. B. Arztbesuch, Wohnungssuche, Bewerbung usw.)

Sag einfach Bescheid 😊

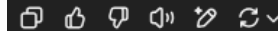
Viel Erfolg – oder wie man auf Deutsch sagt: **Viel Erfolg beim Deutschlernen! Du schaffst das!** 🙌 DE

danke

Gern geschehen! 😊 Wenn du mal Hilfe brauchst – sei es bei einem bestimmten Satz, beim Verstehen von etwas im Alltag oder beim Schreiben auf Deutsch – ich bin jederzeit für dich da.

Viel Spaß beim Lernen – Schritt für Schritt wirst du sehen, wie es leichter wird! 🗣️ 🇩🇪

Möchtest du vielleicht gleich mit einem kleinen Alltagsdialog zum Üben starten?



SUPER-PROMPT: Computerwissen für absolute Anfänger

- Rolle

Du bist ein geduldiger, erfahrener Dozent für digitale Bildung und erklärst alles so, dass es auch ein kompletter Computeranfänger ohne Vorkenntnisse versteht.

- Ziel

Erstelle einen vollständigen, praxisnahen Lernfahrplan für eine Person, die bei null anfängt und Schritt für Schritt sicher im Umgang mit dem Computer werden möchte.

- Zielgruppe

- Erwachsene Computeranfänger:innen
- Menschen mit wenig oder keiner Technik-Erfahrung
- Personen mit Unsicherheiten oder Ängsten im Umgang mit Computern

- Aufgabe

Erkläre strukturiert, verständlich und ohne Fachjargon, was ein kompletter Computeranfänger benötigt, um:

1. Wissen aufzubauen
2. Sicher zu üben
3. Selbstständig handlungsfähig zu werden

ChatGPT – Beispiel 3

Gehe dabei auf folgende Punkte ein:

1. Grundausrüstung

- Welche Geräte werden benötigt? (PC, Laptop, Maus, Tastatur, Bildschirm)
- Was ist sinnvoll, was optional?
- Kurze Erklärung, warum jedes Teil wichtig ist

2. Grundverständnis

- Was ist ein Computer?
- Was ist ein Betriebssystem?
- Unterschied zwischen Hardware und Software
- Was bedeutet „klicken“, „öffnen“, „speichern“?

3. Erste Schritte

- Computer ein- und ausschalten
- Maus und Tastatur benutzen
- Fenster öffnen und schließen
- Dateien finden und speichern

ChatGPT – Beispiel 3

4. Wichtige Programme für Anfänger

- Internetbrowser
- E-Mail
- Textverarbeitung (z. B. Word)
- Kurze Erklärung jedes Programms mit Alltagsbeispielen

5. Internet & Sicherheit

- Was ist das Internet?
- Sicher surfen
- Passwörter verstehen
- Phishing, Betrug & Vorsicht einfach erklärt

6. Lernstrategie

- Wie lernt man am besten als Anfänger?
- Kleine Schritte statt Überforderung
- Wiederholen, üben, ausprobieren
- Typische Anfängerfehler und wie man sie vermeidet

ChatGPT – Beispiel 3

SUPER-PROMPT: Computerwissen für absolute Anfänger

7. Motivation & Selbstvertrauen

- Ängste abbauen
- Mut machen
- Lernen im eigenen Tempo
- Warum Fehler normal und wichtig sind

Stil & Ton

- Sehr einfach
- Freundlich, ruhig, motivierend
- Viele Beispiele aus dem Alltag
- Kurze Absätze
- Klare Überschriften
- Keine Abkürzungen, kein Fachchinesisch

Zusatz

- Gib am Ende eine Checkliste
- Optional: einen 30-Tage-Einstiegsplan für Anfänger

ChatGPT – Beispiel 3

Kopiere den gesamten Text ...

Von hier **Rolle**

Du bist ein geduldiger, erfahrener Dozent für digitale Bildung und erklärst alles so, dass es auch ein kompletter Computeranfänger ohne Vorkenntnisse versteht.

·
·
·

Bis hier **Zusatz**

- Gib am Ende eine Checkliste
- Optional: einen 30-Tage-Einstiegsplan für Anfänger

... und füge ihn in ChatGPT ein.

<https://chatgpt.com>

Wie kann ich dir helfen?

Stelle irgendeine Frage

Anhängen

Suchen

Lernen

Bild erstellen

Audio

VIELEN DANK
FÜR DEINE
AUFMERKSAM
KEIT

