PC-Treff 55+

IT-Sicherheit im täglichen Gebrauch

26. SEPTEMBER 2023

EGBERT ZWERSCHKE

RAINER PLUSCHYS

Wer sind wir vom PC-Treff 55+?

(ehrenamtliche Mentoren)

Horst Höfer

Rainer Pluschys

Rainer Kaiser

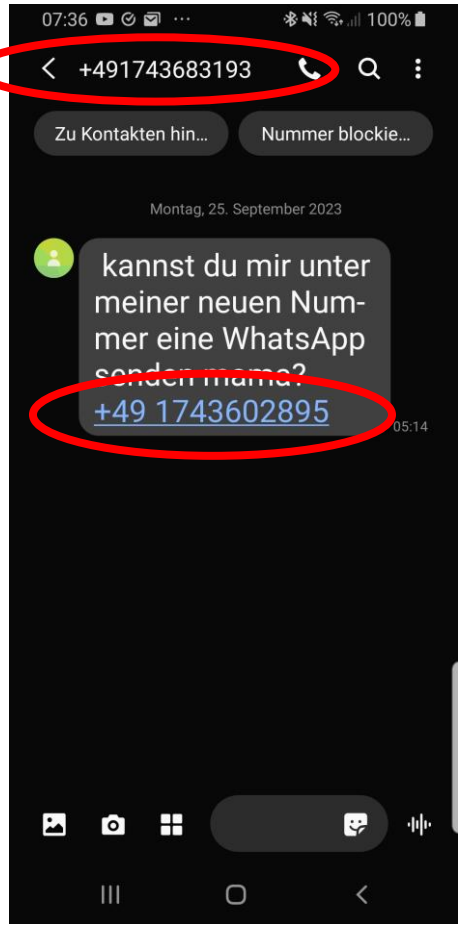
Egbert Zwerschke

Heike Hauß
Leiterin MIT

Worüber wir heute sprechen wollen

- Was gibt’s es für Bedrohungen im Internet und wie kann ich mich schützen?
- Wie sicher ist mein PC, Notebook oder Tablett im Internet?
- Wie kann ich unseriöse E-Mails erkennen?
- Wie schütze ich mich vor unerwünschten Zugriff auf mein Geld und Betrügereien? (Onlinebanking)
- Datenschutz und Datensicherheit

SMS-Nachricht



Informationstechnologie-Sicherheit

Bei Bedrohungen im IT-Umfeld geht es um Angriffe auf die persönlichen Daten und daraus meist resultierenden Daten- und finanzielle-Verluste.

- Ein IT-System wird dann als **sicher** bezeichnet, wenn für den Angreifer der Aufwand für das Eindringen in das System höher ist als der für ihn daraus resultierende Nutzen.
- Ein IT-System ist dann **absolut sicher**, wenn es jedem denkbaren Angriff widerstehen kann.
- Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch anspruchsvolle Sicherheitsmaßnahmen bzw. Abwehr beantwortet werden kann.

Auswirkungen und Ziele einer Bedrohung

- Technischer Systemausfall
- Systemmissbrauch z. B. durch nicht autorisierte Ressourcennutzung, oder Veränderung von Inhalten auf dem Computer
- Sabotage
- Spionage
- Betrug und Diebstahl

Bedrohungen aus dem Internet

- Schadsoftware auch Malware genannt
  - Computerviren, Trojaner, Spyware und Würmer
- Ransomware
  - eine besondere Form von Schadsoftware, die den Zugriff auf Daten und Systeme einschränkt und dessen Ressourcen erst gegen Zahlung eines Lösegelds wieder freigibt
- Social Engineering, das Erschleichen von persönlichen Daten in den sozialen Medien
- Unerwünscht zugesandte E-Mails wie
  - klassischer Spam
  - Schadprogramm-Spam
  - Phishing

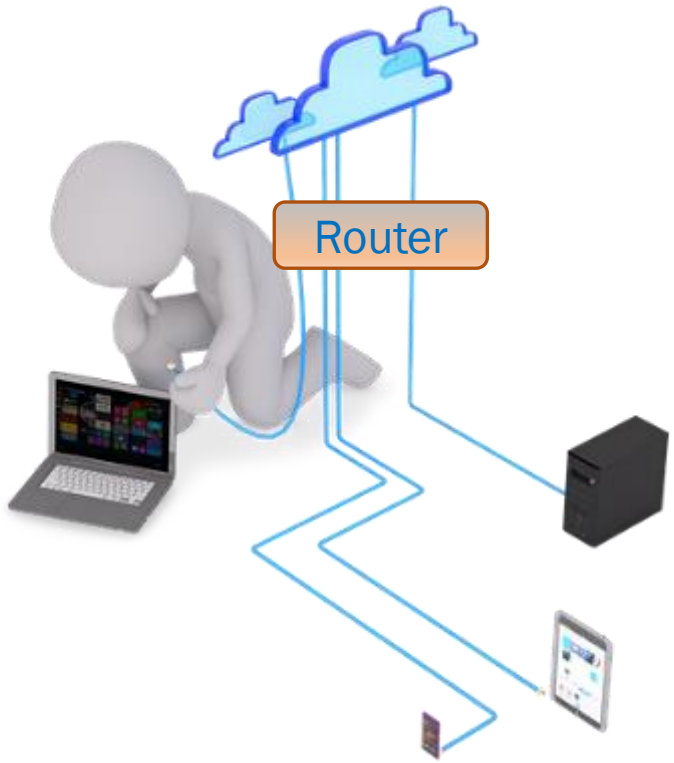
Bedrohungen aus dem Internet

- Botnetze
- Überlastung einer IP-Adresse durch Distributed-Denial-of-Service-(DDoS)-Angriffe
- Ausnutzen von Schwachstellen in Browser, Browser-Plug-ins oder Betriebssystemen
- Identitätsdiebstahl, wie zum Beispiel
  - Spoofing → vortäuschen einer falschen Identität
  - Phishing → sammeln von persönlichen schützenswerten Daten
  - Pharming → umleiten auf eine gefälschte Webseite
- Keylogger

Als Schutzmechanismen dienen u.a. eine Firewall und eine aktuelle Anti-Viren-Software

Basiselemente der IT-Sicherheit
Die Hardware für ein Internetzugang

- Aktiver Internet-Anschluss durch einen Anbieter (Provider)
- Verbindung zwischen Internet und PC (Router)
- PC, Laptop, Tablett
- Smartphone, Smart-TV, X-Box, Cloud Speicher, Network Attached Storage (NAS), Alexa u.v.m.



Basiselemente der IT-Sicherheit
Der Router

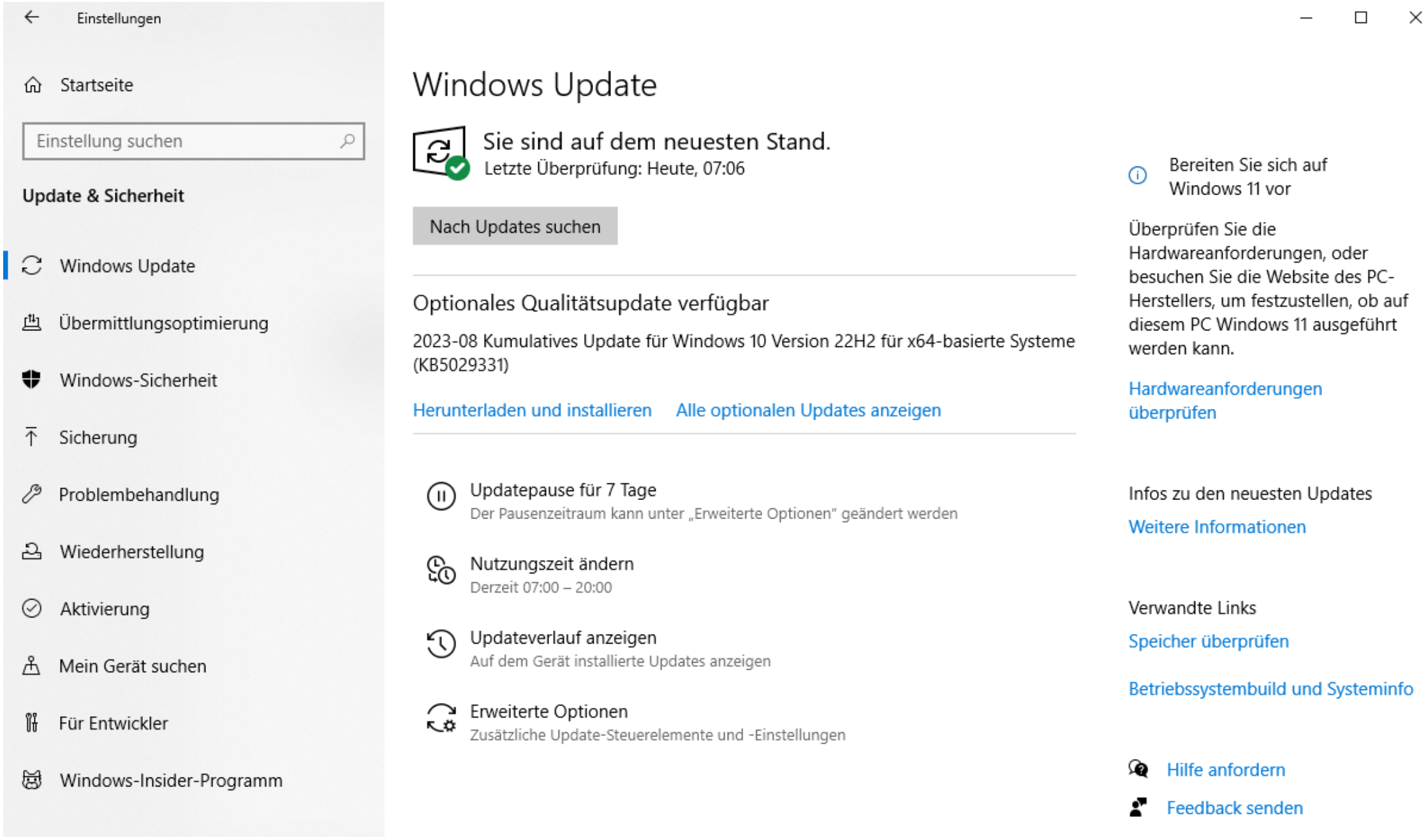
- Stellt die Verbindung zwischen der Außenwelt / Internet und den angeschlossenen Geräten her
- Hardware-Firewall
- LAN (Local Area Network)
- WLAN (Wireless Local Area Network) 2,4 Ghz und 5 Ghz
- SSID (Service Set Identifier), Name des Netzwerks
- WLAN-Netzwerkschlüssel
- IP-Adresse (Internet Protokoll Adresse)
- VPN (virtual privat Network)

Quelle: Stiftung Warentest

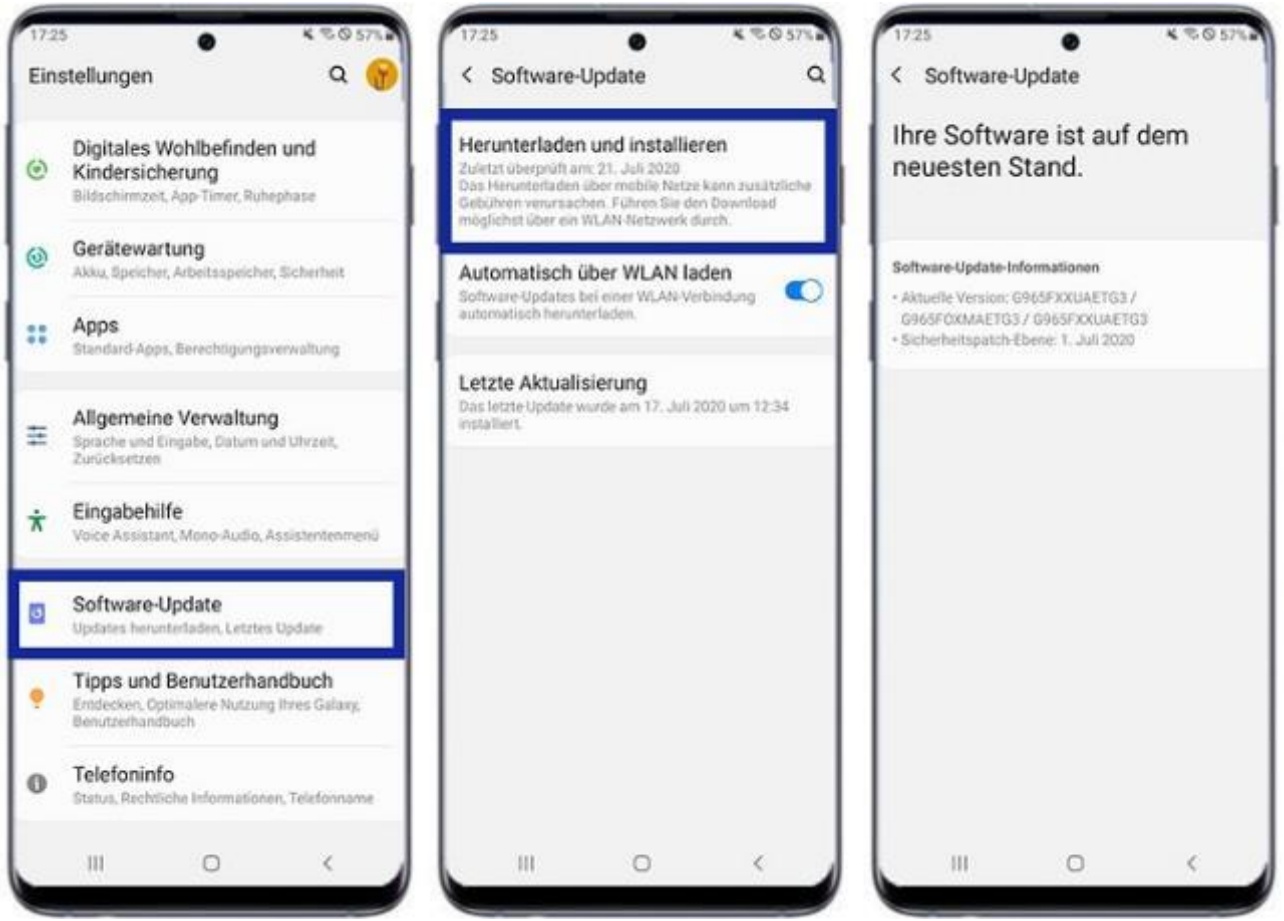
Basiselemente der IT-Sicherheit
Das Betriebssystem

Aktuelle Betriebssysteme benutzen

- Microsoft Windows, IOS, Android, Linux…
- Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken
- Informieren Sie sich regelmäßig über Updates – etwa durch Newsletter der Hersteller oder die Fachpresse
- Installieren Sie Updates möglichst rasch, sobald diese verfügbar sind
- Lassen Sie sich durch gefälschte Updates nicht aufs Glatteis führen
- Achten Sie auf Mitteilungen, die das Auslaufen des Supports für Produkte ankündigen


Einstellungen
Startseite
Einstellung suchen
Update & Sicherheit
Windows Update
Übermittlungsoptimierung
Windows-Sicherheit
Sicherung
Problembehandlung
Wiederherstellung
Aktivierung
Mein Gerät suchen
Für Entwickler
Windows-Insider-Programm
Windows Update
Sie sind auf dem neuesten Stand.
Letzte Überprüfung: Heute, 07:06
Nach Updates suchen
Optionales Qualitätsupdate verfügbar
2023-08 Kumulatives Update für Windows 10 Version 22H2 für x64-basierte Systeme (KB5029331)
Herunterladen und installieren
Alle optionalen Updates anzeigen
Updatepause für 7 Tage
Der Pausenzeitraum kann unter „Erweiterte Optionen" geändert werden
Nutzungszeit ändern
Derzeit 07:00 – 20:00
Updateverlauf anzeigen
Auf dem Gerät installierte Updates anzeigen
Erweiterte Optionen
Zusätzliche Update-Steuerelemente und -Einstellungen
Bereiten Sie sich auf Windows 11 vor
Überprüfen Sie die Hardwareanforderungen, oder besuchen Sie die Website des PC-Herstellers, um festzustellen, ob auf diesem PC Windows 11 ausgeführt werden kann.
Hardwareanforderungen überprüfen
Infos zu den neuesten Updates
Weitere Informationen
Verwandte Links
Speicher überprüfen
Betriebssystembuild und Systeminfo
Hilfe anfordern
Feedback senden

Beispiel Android



Quelle: Samsung

Beispiel Apple hier iOS 12

Quelle: Apple

Basiselemente der IT-Sicherheit
Der Browser

- Welches ist der richtige Browser für Sie?
- Was möchten Sie damit tun?

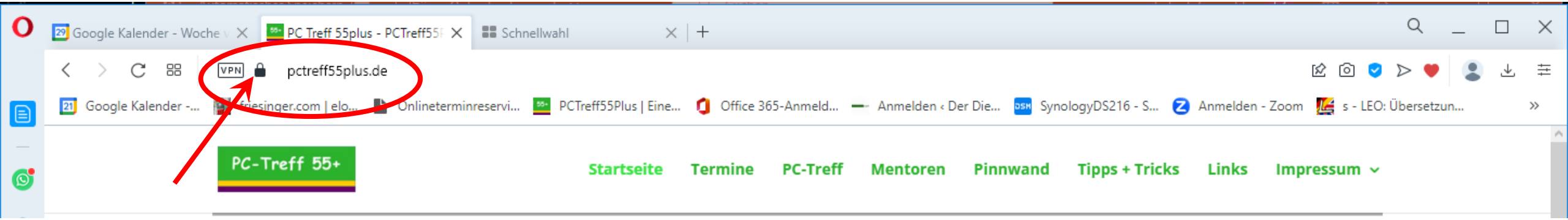
Quelle: Chip

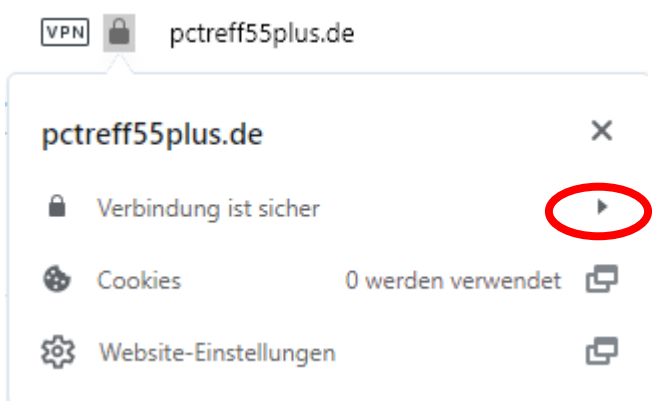
Basiselemente der IT-Sicherheit
Der Browser

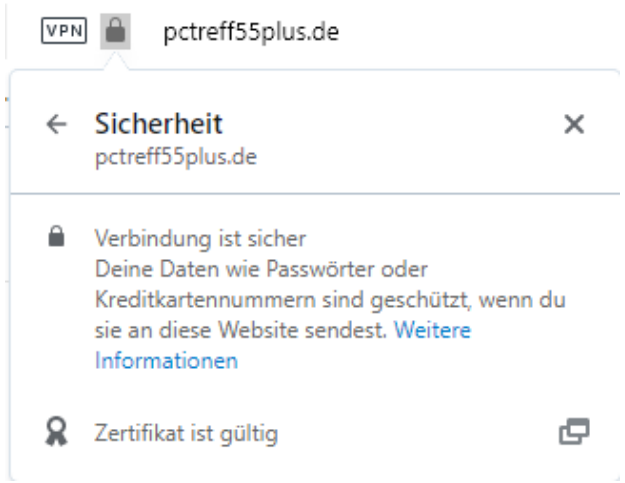
- Automatische Updates, die sich selbsttätig und zeitnah installieren
- Verschlüsselte Verbindung nutzen (siehe Beispiel)
- Kritisches Beobachten der Fenster z.B. unbekannte Popups, wie Gewinninformationen oder Viruswarnungen **nicht** aktivieren
- Werbeblocker im Browser unter Einstellungen einschalten
- Unnötige Plugins wie **Java, ActivX** oder **Flash** ausschalten
- Nicht als Administrator Surfen evtl. mit dem Gast-Konto (eingeschränkte Rechte)
- Wichtige Web-Adressen als Lesezeichen speichern
- Cookies automatisch löschen, Cookies von Drittanbietern sperren

Infografik Sicherheitscheck für Ihren Web-Browser
Quelle: Bundesamt für Sicherheit in der Informationstechnik

Beispiel einer sicheren Verbindung



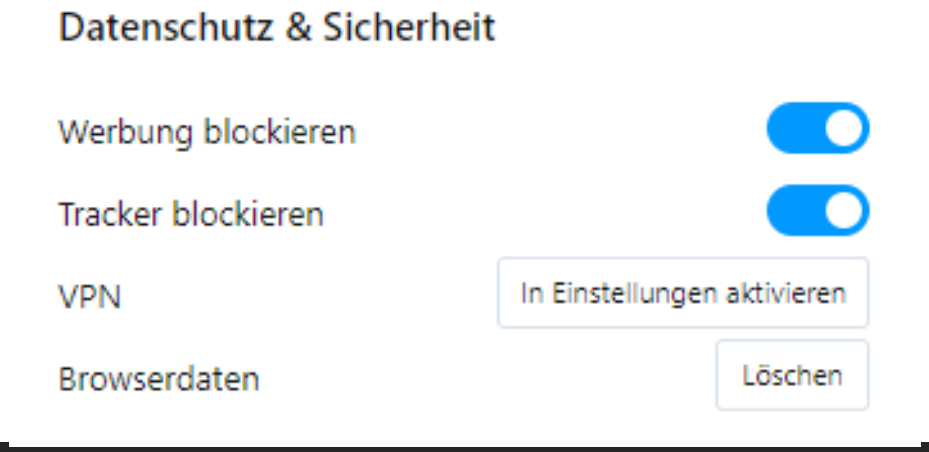


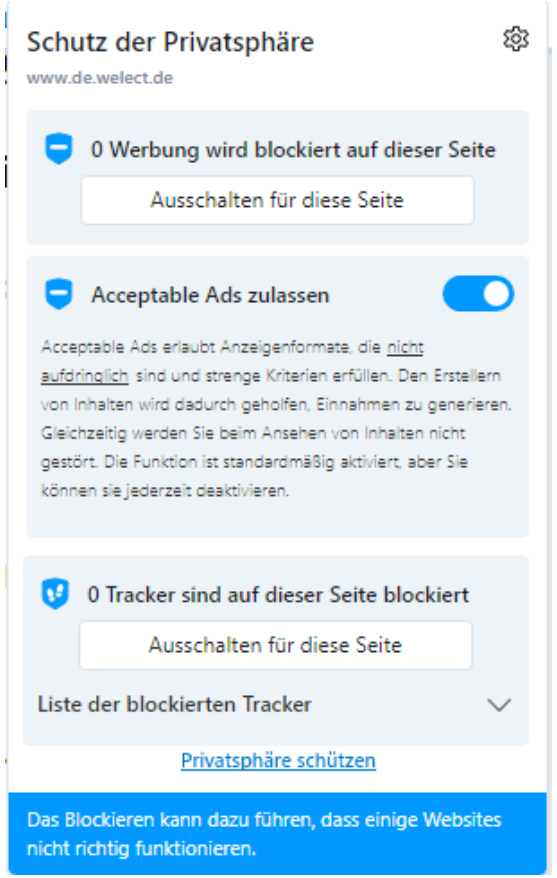


Browser Ad-Blocker und Tracker

Quelle: Chip

- Was sind Ad-Blocker?
- Was sind Tracker?
- Wie können Sie ein- / ausgeschaltet werden?
- Wie können Ausnahmen zugelassen werden?





Sicherheitseinstellungen der gängigen Browser

Firefox:
•Sicherheitseinstellungen: https://support.mozilla.org/de/products/firefox/privacy-and-security
Empfehlung: Verwenden Sie die Standard-Einstellungen von Firefox. Deaktivieren Sie die Option "Passwörter speichern". Falls Sie Passwörter im Browser speichern wollen, verwenden Sie unbedingt ein Master-Passwort (Beachten Sie die Hinweise für ein sicheres Passwort).

Internet Explorer / MS Edge:
•Sicherheitseinstellungen: https://support.microsoft.com/de-de/help/17479/windows-internet-explorer-11-change-security-privacy-settings
Empfehlung: Blockieren Sie die ActiveX-Steuerelemente. Verwenden Sie die neueste Version des Internet Explorers, die für Ihre Windows-Version verfügbar ist.

Chrome:
•Sicherheitseinstellungen: https://google.com/intl/de_ALL/chrome/security/
•Blockieren Aktiver Inhalte in Google Chrome: http://support.google.com/chrome/bin/answer.py?hl=de&answer=142064
Empfehlung: Wählen Sie unter "Plugins blockieren" die Funktion "Click-to-Play".

Opera:
•Sicherheitseinstellungen https://help.opera.com/
•Guide to security and privacy in Opera https://de.opera.com/browser/tutorials/security/

Safari:
Auf der Internetseite von Apple gibt es Zusatzinformationen zu den Sicherheitseinstellungen des Browsers im Benutzerhandbuch.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

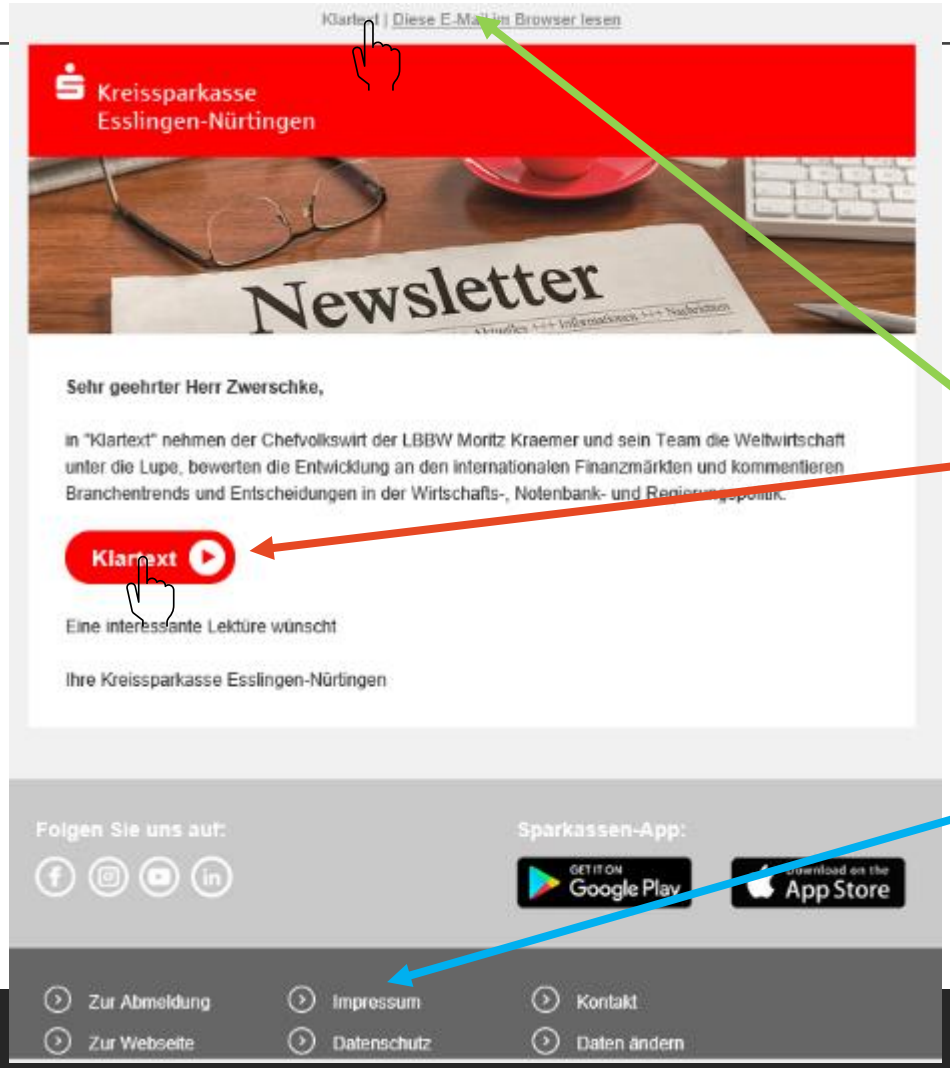
Achtung, E-Mail-Betrüger!

Wenn Sie eine E-Mail erhalten, die sensible Daten abfragt, wie z.B. Kreditkartennummer, PIN, TAN, Passwörter o.ä. abfragt, geben Sie diese Information auf keinen Fall weiter. Ihre Bank wird solche Daten nie per E-Mail oder am Telefon abfragen.

Auch wenn die E-Mail einen offiziellen Eindruck macht, ist wahrscheinlich eine betrügerische Absicht dahinter. Solche SPAM-Nachrichten bitte sofort löschen **…und keinenfalls einen Link im E-Mail anklicken!**

Wenn Sie unsicher sind, können Sie natürlich jederzeit Ihre Bankoder den Anbieter kontaktieren.

Beispiel einer seriösen E-Mail



https://emailing.ksk-es.de/-link2/6516/8619/5/7/1375/SsrEP3DP/CRE9uekX0J/0

Ein Blick im Impressum kann auch hilfreich sein.

Beispiel E-Mail E.Zwerschke

Beispiele typischer Phishing E-Mails

Wir benötigen von Ihnen die Aktualisierung Ihrer Informationen

Kundenservice

An: dienstagstreff@t-online.de

Postbank

Ihr Konto Wurde Aus Sicherheitsgründen Gesperrt

Sehr geehrter Kunde,
Kürzlich haben unsere Aufzeichnungen ergeben, dass möglicherweise ein Dritter auf Ihr Postbank-Konto zugegriffen hat. Die Sicherheit Ihres Kontos ist unser Hauptanliegen, daher haben wir uns entschieden, den Zugriff auf Ihr Konto vorübergehend einzuschränken.

Um den vollen Zugriff auf Ihr Konto wiederherzustellen, müssen Sie Ihre Angaben bestätigen.

Mein Login

Nachdem Ihre Angaben von uns geprüft und bestätigt wurden, erhalten Sie schnellstmöglich eine telefonische Nachricht von uns und der Zugang zu Ihrem Konto wird vollständig wiederhergestellt. Wir danken Ihnen für Ihre Mitarbeit.
Freundliche Grüße,

Daniel Schneider Braun
Kundenservice | Postbank AG

© 2023 Postbank – eine Niederlassung der Deutsche Bank AG

Beispiel E-Mail E.Zwerschke

Ihr [Netflix Konto] ist abgelaufen...

N etflix <adidas@fr-news.adidas.com>

NETFLIX

Achtung!!! Netflix Mitgliedschaft

Sehr geehrter Kunde,
Ihre Mitgliedschaft ist abgelaufen!

aber im Rahmen unseres Treueprogramms konnen Sie jetzt kostenlos fur 90 Tage verlangern.

Kostenlos verlangern

* Nach der Anmeldung mussen Sie Ihre Kreditkartendaten zur Validierung Ihres Kontos eingeben.
Wir werden keine Betrage abheben.

Wenn Sie diese E-Mails nicht mehr erhalten mochten, konnen Sie sich per E-Mail abmelden Klicken Sie hier

https://hycnothize-coinctide-quazified.s3.dualstack.us-east-1.amazonaws.com/partnetru/conesultation/index.html?utm_source=1559&pompa=c&utm_medium=76208324

Beispiel E-Mail E.Zwerschke

Sie haben eine ausstehende Lieferung - Verwenden Sie Ihren Code für die Verfolgung und `Entgegennahme`!

PT P0ST TRACKING <no-reply@nls.la-selection-privee.fr>

Antworten

http://unbouncepages.com/zeigt-buchidee/?torrefera=76208324&serema=1615&kamp=c

Beispiel E-Mail E.Zwerschke

Weitere Elemente der IT-Sicherheit

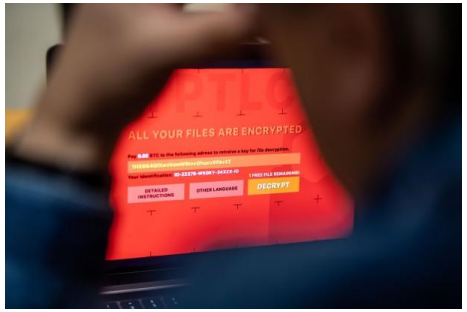
- Automatische Software-Updates einrichten bzw. zulassen
- Veraltete, unsichere und unbenutzte Software deinstallieren
- Verschlüsselungen aktivieren z.B. MS-Bitlocker
- Passwort Manager benutzen
- Open Source Software einsetzen z.B. Libre Office benutzen
- Sicherungskopien erstellen → Datensicherheit
- Persönliche Weiterbildung → bleiben Sie informiert

Virenschutzprogramme

Aufgaben einer Virenschutz-Software

- Ein Antivirenprogramm, Virenscanner oder Virenschutz-Programm ist eine Software, die Schadprogramme wie z. B.
  - Computerviren
  - Computerwürmer
  - Trojanische Pferde
- aufspüren, blockieren, gegebenenfalls betroffene Anwender informieren und die Schadsoftware beseitigen soll.

Virenschutzprogramme



Quelle: DPA

1. Bitdefender Total Security
2. Avira Prime
3. Kaspersky Premium
4. AVG Internet Security
5. F-Secure Total
6. Avast Free Antivirus
7. AVG Anti-Virus Free
8. Trend Micro Maximum Security
9. McAfee Total Protection
10. Norton 360 Advanced
11. ESET Smart Security Premium
12. Microsoft Windows Defender

Internet Security-Suiten im Vergleich September 2023
Quelle: Bundespolizei

Sicherheit beim Online-Banking

- ✓ **Sicheres Gerät**
- ✓ **Sichere Internetverbindung**
- ✓ **Sichere Internetseite**

Wie sicher ist Online-Banking?

Grundlegende Sicherheitstipps:

- ✓ **Installieren und nutzen Sie ein aktuelles Virenschutzprogramm.**
- ✓ **Installieren Sie Software-Updates am PC, um Sicherheitslücken zu schließen.**
- ✓ **Aktivieren Sie den Phishing-Schutz in Ihrem Internet-Browser, um verdächtige Seiten sofort zu blockieren. (unter Grundeinstellungen, Datenschutz & Sicherheit)**
- ✓ **Wählen Sie starke, sichere Passwörter, die nur Sie kennen. (z.B. adTs1SE#)**
- ✓ **Achten Sie darauf, nur Webseiten mit einer sicheren Verbindung zu nutzen („https“ am Anfang der Internetadresse).**

Tipps für sicheres Online-Banking

- ✓ Geben Sie sensible Daten wie Geheimzahlen oder Transaktionsnummern nie heraus.
- ✓ Öffentliche WLAN-Netze sind meist unverschlüsselt und somit **nicht sicher**. Für das Online-Banking sollten Sie daher besser Ihr sicheres Heimnetzwerk benutzen.
- ✓ Nutzen Sie keine fremden Geräte für das Online-Banking, da sich nicht ausschließen lässt, dass Ihre eingegebenen Daten aufgezeichnet und weiterverwendet werden.

Tipps für sicheres Online-Banking

- ✓ melden Sie sich aus der App oder dem Browserfenster stets ab
- ✓ setzen Sie ein Tages-Überweisungslimit
- ✓ Wenn Ihnen sensible Daten gestohlen wurden oder Sie verdächtige Kontobewegungen bemerken, lassen Sie den Zugang zu Ihrem Online-Banking-Konto **sofort sperren**. Rufen Sie dazu den Sperrnotruf 116 116 oder die Online-Banking-Hotline Ihrer Bank an.

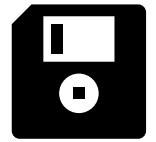
Datenschutz

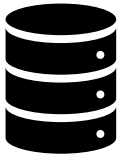
Quelle: Wikipedia

- Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten.
- Der Begriff wurde auch verwendet für Schutz wissenschaftlicher und technischer Daten gegen Verlust oder Veränderung – und Schutz gegen Diebstahl dieser Daten
- Heute bezieht sich der Begriff meist auf den Schutz personenbezogener Daten (Schutz der Privatsphäre).
- Datenschutz ist das Recht des Einzelnen auf informationelle Selbstbestimmung. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen.
- Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Datensicherheit

- Wiederherstellungspunkte im Windows Betriebssystem anlegen
- Dokumente, Bilder und alle wichtigen Daten auf externe Datenträger speichern (USB-Stick, externe Platten etc.)
- Regelmäßig ein Backup durchführen (z.B. mit Acronis Software)
  - gesichert werden sollen Betriebssystem und alle Daten
  - z. B. in einer NAS
  - oder in einer Cloud (z.B. DropBox, Microsoft OneDrive, Google Drive, auch div. Virenscanner wie Norton 360





Bundesamt
für Sicherheit in der
Informationstechnik

Weitere hilfreiche Informationen rund um das Thema „Sicherheit im Internet“ finden Sie auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik.

Digitaler Verbraucherschutz

Aktuelle Themen und Vorfälle | Sicher im digitalen Alltag | Kooperationen und Forschung

Verbraucherschutz-Newsletter "Sicher informiert"

Bericht zum Digitalen Verbraucherschutz

IT-Sicherheitskennzeichen

Sie haben einen IT-Sicherheitsvorfall?

Internet der Dinge / Smart Home / vernetztes Fahren

Wie Sie eine Cloud für Ihre Daten sicher nutzen

5G, Blockchain und Co. sicher gestalten

Identitätsdiebstahl und seine Folgen

Fazit

Auch wenn Sie technische Hilfsmittel zum Schutz in der Internetnutzung einsetzen,

bleiben Sie kritisch und wachsam!

Vielen Dank für Ihre Aufmerksamkeit

Quellen

Internet:
https://www.senioren-computerkurs24.de/online-banking-mit-sicherheit/
(abgerufen am 12.02.2021)

Bildquellen:
iStock.com/Extreme Media
Pixabay
Wikibanking.net
BMI
MicroSoft 360
wie unter dem Bild angegeben