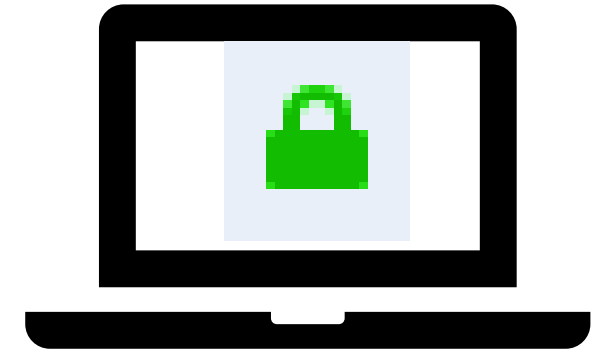


Datenschutz Datensicherheit

Sicheres Arbeiten mit dem PC,
im Internet, beim E-Mail-Verkehr und
beim Online-Banking



Inhalt

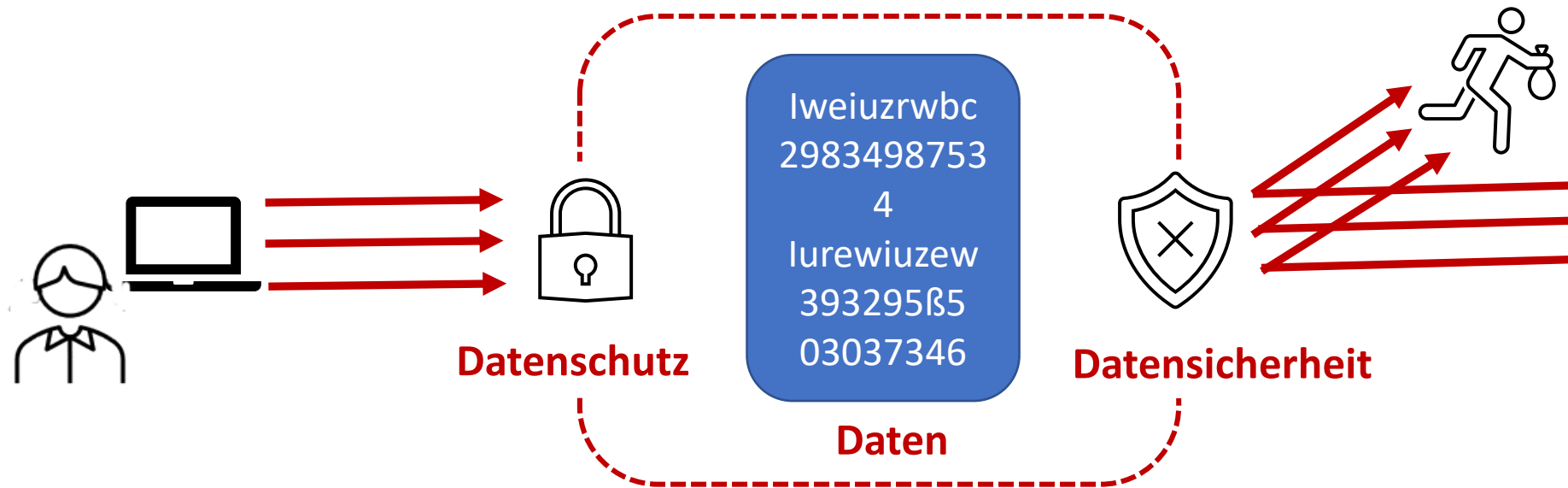
- 3 Datenschutz/Datensicherheit – Definition -
- 4 Sicherer PC - Virenschutz
- 5 Sicherer PC - Update
- 5 Sicherer PC - Sicherung
- 6 Sicherer PC - allgemein
- 7 Sicherer E-Mail Verkehr
- 8 Sicheres Internet
- 9 Sicheres Onlinebanking
- 10 Passwörter
- 11 Haben Sie noch Fragen?

Datenschutz - Datensicherheit

Definition

Beim **Datenschutz** geht es um den Schutz der Menschen, deren Daten erhoben und verarbeitet werden.

Die **Datensicherheit** soll den Schutz vor einem Verlust von Daten ermöglichen. Hier geht es vor allem um technische Maßnahmen.



Sicherer PC - Virenschutz

Das Betriebssystem WIN 10 beinhaltet bereits ein Virenschutzprogramm und eine Firewall, diese sind zuerst zu initialisieren. Bei anderen Betriebssystemen ist ein Virenschutzprogramm zu installieren.

Bei WIN 10 finden sie den Schutz im Startmenü bei *Einstellungen* und dort bei *Update und Sicherheit*, hier unter *Windows-Sicherheit*



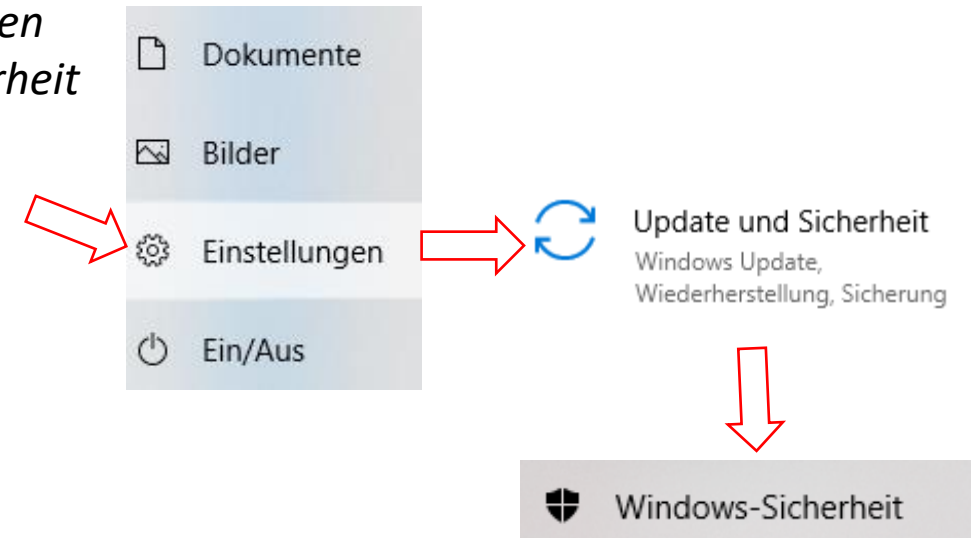
Windows-Sicherheit

Windows-Sicherheit ist Ihr zentraler Anlaufpunkt, über den Sie die Sicherheit und Integrität Ihres Geräts überprüfen und verwalten können.

[Windows-Sicherheit öffnen](#)

Schutzbereiche

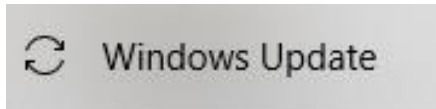
-  **Viren- & Bedrohungsschutz**
Keine Maßnahmen erforderlich.
-  **Kontoschutz**
Keine Maßnahmen erforderlich.
-  **Firewall & Netzwerkschutz**
Keine Maßnahmen erforderlich.



Sicherer PC - Update

Ein vollständiger Schutz besteht nur wenn sie zeitnah Betriebssystem und Programme updaten!

Bei WIN 10 finden sie Update im Startmenü bei *Einstellungen* und dort bei *Update und Sicherheit*

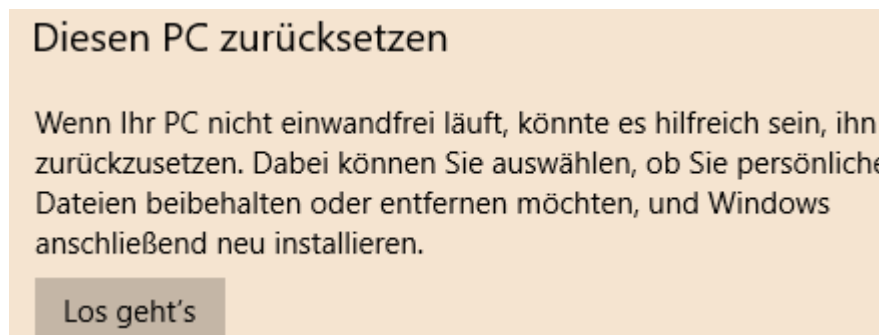
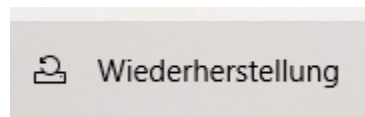
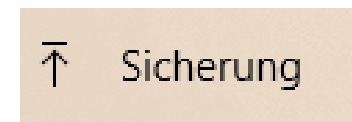


Sicherer PC - Sicherung

a) Datensicherung: Sichern Sie regelmäßig ihre Daten auf einem externen Medium (USB- Stick oder Laufwerk) und entfernen Sie es nach der Sicherung vom PC.



b) Backup: Ebenso notwendig sind regelmäßige Backups des gesamten Systems. Bei WIN 10 finden Sie Backup im Startmenü bei *Einstellungen*, bei *Update und Sicherheit* und dort bei *Sicherung*. Hierbei wird das gesamte System gesichert, dieses können Sie bei Fehlern wieder herstellen.



Sicherer PC- allgemein

Allgemein gilt:

Schließen Sie alle Programme und Konten nach Gebrauch, da sonst Unbefugte an Ihre Daten kommen können. Bei Programmen, bei denen eine Anmeldung erforderlich ist, müssen Sie sich unbedingt abmelden, schließen genügt nicht!



Versehen Sie ihren PC mit einem Gerätepasswort. Das ist wegen Datenklau auch versicherungstechnisch notwendig.

Sicherer E-Mail-Verkehr

E-Mail- Anhänge:

Öffnen Sie keine E-Mail-Anhänge ohne den Absender zu kennen. Klicken Sie keine Links an, deren Herkunft und Ziel unbekannt sind.

Zum Beispiel: <http://chtico.zenesk.com/hc/requests/2052658>

E- Mail- Programme:

Verwenden Sie möglichst E-Mail-Programme und nicht die Web-Seite ihres E-Mail-Anbieters.
Vorteil: keine Werbung und offline- Betrieb möglich, gestaltbare Oberfläche.

Beispiele:



Thunderbird



Outlook 2010

Teilen Sie NIEMALS Ihre Konten und Zugänge (Accounts) auf Anfrage per E-Mail mit!

Provider (Anbieter):

Es gibt kleinere Anbieter, die gegen kleines Geld den elektronischen Postverkehr anonymisieren und die Ihre Privatsphäre schützen.

Beispiele: **aikQ; Posteo; mailbox;**

Sicheres Internet

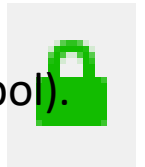


Internet Explorer, Edge, Firefox, Chrome oder Safari gehören zu den meistgenutzten Webbrowsern: Viele erreichen heute schon ein ordentliches Sicherheitsniveau. Doch nicht jede Website ist vertrauenswürdig und nicht jeder Onlineshop echt. Auch Webbrowser selbst können angegriffen werden und Schadsoftware ausführen. Über die Einstellungsmöglichkeiten in der Menüleiste lässt sich das Sicherheitsniveau weiter verbessern.

Einstellungen wie „privater Modus“, „Verlauf löschen“, „Cookies nicht für Drittanbieter zulassen“ verringern die Speicherung von vertraulichen Informationen.

Verwenden Sie einen aktuellen Browser (Updates).

Prüfen Sie ob „https“ vorne in der WEB- Adresse steht und ob die WEB- Seite verifiziert ist (Schlosssymbol). Nutzen Sie ein Programm zum Blockieren von Werbung, um sich vor Verbreitung von Malware über Werbeeinblendungen, zu schützen.



Vermeiden Sie unnötige Datenspuren. *Cookies* und Ihren Browserverlauf löschen Sie über die Browsereinstellungen. Verboten Sie ein sogenanntes Tracking oder bevorzugen Sie von vornherein Suchmaschinen, die keine Informationen über Nutzer speichern.

Sicheres Onlinebanking

Öffnen Sie Online Banking nur durch WEB Adresseneingabe oder durch einen selbst gespeicherten Link.

Teilen Sie NIEMALS Ihre Konten und Zugänge (Accounts) auf Anfrage per E-Mail mit.

Derzeit sehr sichere Onlinebanking-Verfahren sind ChipTan, BestSign, PhotoTan und QR-Tan. SMS-Tan hat nur eine mittlere Sicherheit.

Vorsicht! Kommt Ihnen beim Onlinebanking etwas komisch vor, brechen Sie den Vorgang ab.

Bevorzugen Sie Online- Banking- Programme. Diese sind gegenüber dem Web-Seiten-Zugang sicherer, da sie, offline arbeiten und nur während des kurzzeitigen Sendens von Aufträgen online gehen.

Sicherheitsrelevante Passwörter sollten regelmäßig geändert werden.

Passwörter

Passwörter sind erst sicher, wenn Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten sind (möglichst acht oder mehr Zeichen).

Hier zwei Beispiele:

Bn#350\$Sodi ; geschätzte Zeit zu knacken: 442 Jahre

12AbX0 ; geschätzte Zeit zu knacken: 1 Sekunde

Passwörter sind leichter zu merken, wenn sie an persönliche Themen anknüpfen.

Sicherheitsrelevante Passwörter sollten regelmäßig geändert werden.

Wenn Sie sehr viele Passwörter verwenden müssen, ist ein Passwortmanager sehr hilfreich. Dann brauchen Sie sich nur das Zugangspasswort des Passwortmanagers zu merken.



Was hat Ihr Passwort mit Pizza zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:

„Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“

Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

AleIPm4Z+eK!

© Bundesamt für Sicherheit in der Informationstechnik (BSI) www.bsi-fuer-buerger.de

Datenschutz Datensicherheit

Haben Sie noch Fragen ?

Kontaktieren Sie uns:

cafeschoeckingen@gmx.de oder Tel. 07156-3071972 (AB).

Wir sind persönlich für Sie da: Jeden Dienstag
von 15:00 bis 18:00 Uhr, im Alten Rathaus in Schöckingen,
bitte melden Sie sich an.

Weitere Tipps zur Nutzung von Medienangeboten und Onlinediensten

https://www.lmz-bw.de/fileadmin/user_upload/Downloads/Handouts/2019-01-treffpunkt-internet.pdf

