Zugangsdaten sicher und übersichtlich speichern

Passwörter, Benutzernamen, Links, Lizenz Schlüssel, Produkt Key, Netzwerk Schlüssel, SSID, Registrierungsdaten, Kundennummern, Software-Abos, E-Mail-Passwort.

Inhalt

Grundsätzliches

Passwörter, Benutzernamen, Links, Lizenz Schlüssel, Produkt Key, Netzwerk Schlüssel, SSID, Registrierungsdaten, Kundennummern, Software-Abos, E-Mail-Passwort …

- Im Lauf der Zeit kommen immer mehr solcher Daten zusammen und man verliert schnell den Überblick.
- Bei Neuinstallationen, Fehlersuche, und bei Supportanfragen braucht man diese Informationen.
- Eine „Zettelwirtschaft“ hilft auch nicht weiter.
- Eine Möglichkeit diese Daten sicher, dauerhaft und sofort greifbar zu speichern bieten Datenbankprogramme bzw. Passwortdepots.

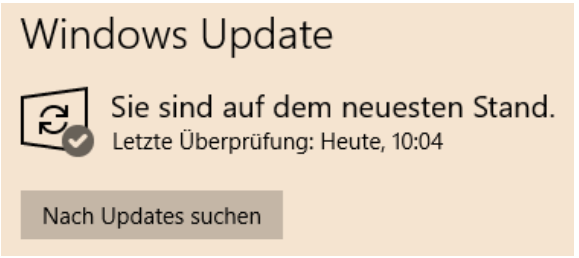
Programmfunktionen

- Eine komfortable Art und Weise, viele PINs, Logins oder Passwörter zu verwalten, sind sogenannte Passwort-Manager. Das sind Programme, die die Daten verschlüsselt speichern und selbst sichere, zufallsgenerierte Kennwörter erstellen können.
- Man muss sich lediglich ein Haupt-Passwort für den Zugang merken oder verschlüsselt auf einem externen Speicher ablegen.
- Es gibt die Manager als Computer-Software oder Smartphone-App. Mobile Anwendungen sind dabei besonders praktisch, da man mit dem Handy seine Zugangsdaten immer griffbereit hat. Einige Apps unterstützen außerdem Fingerabdruckscanner zum Entsperren.
- Neben Passwörtern können in diesem Passwort-Manager z. B. auch Software-Lizenzen, Dokumente, TANs, Benutzernamen, Links, Lizenz Schlüssel, Produkt Key, Netzwerk Schlüssel, SSID, Registrierungsdaten, Kundennummern, Software-Abos, E-Mail-Passwort uvm. Verwaltet werden.

Sicherer PC - Update

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

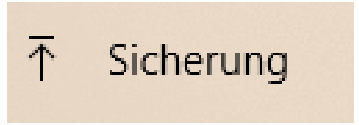
Bei WIN 10 finden sie Update im Startmenü
bei *Einstellungen* und dort bei *Update und Sicherheit*

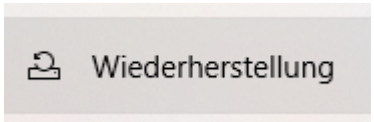


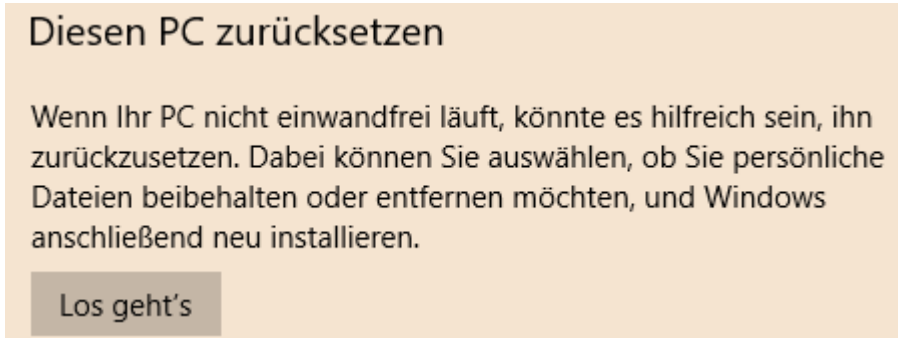
Sicherer PC - Sicherung

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

Bundesministerium des Innern, für Bau und Heimat

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. Verbieten 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.

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.

Zugangsdaten sicher und übersichtlich speichern