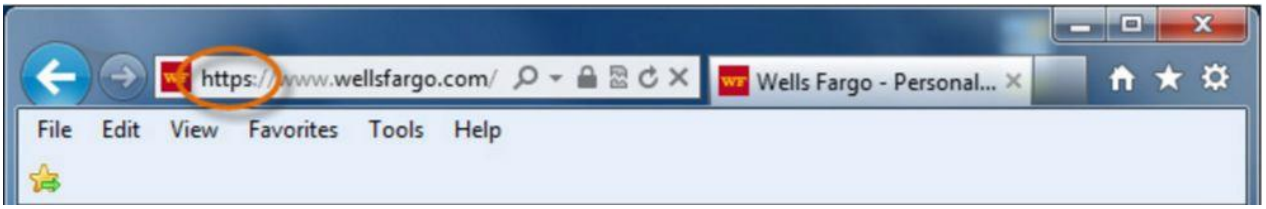
Web-Sicherheit

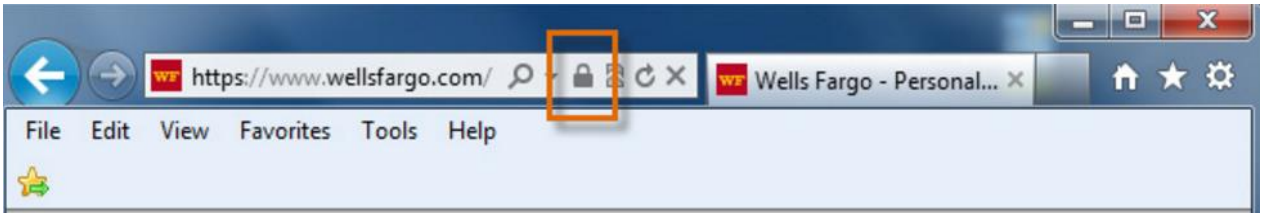
Wenn du browst:

Versichere dich, dass die Verbindung zur Website **sicher** ist und überprüfe das **SSL certificate** z.B., wenn du Bankseiten nutzt.

Verbindungen zu Webadressen beginnen entweder mit „http“ oder“ https“:



Verbindungen nur mit „http“ (also ohne das ‚s‘) sind dabei unsicher und solche mit „https“ sind sicher. Bei unsicheren Verbindungen zeigt der Browser ein offenes Schloss an, bei sicheren Verbindungen ein geschlossenes. Schloss (s.u.)



Klicke auf das Schlosssymbol der Website und versichere dich, dass die Identität der Website **verifiziert** ist:

Virenschutz

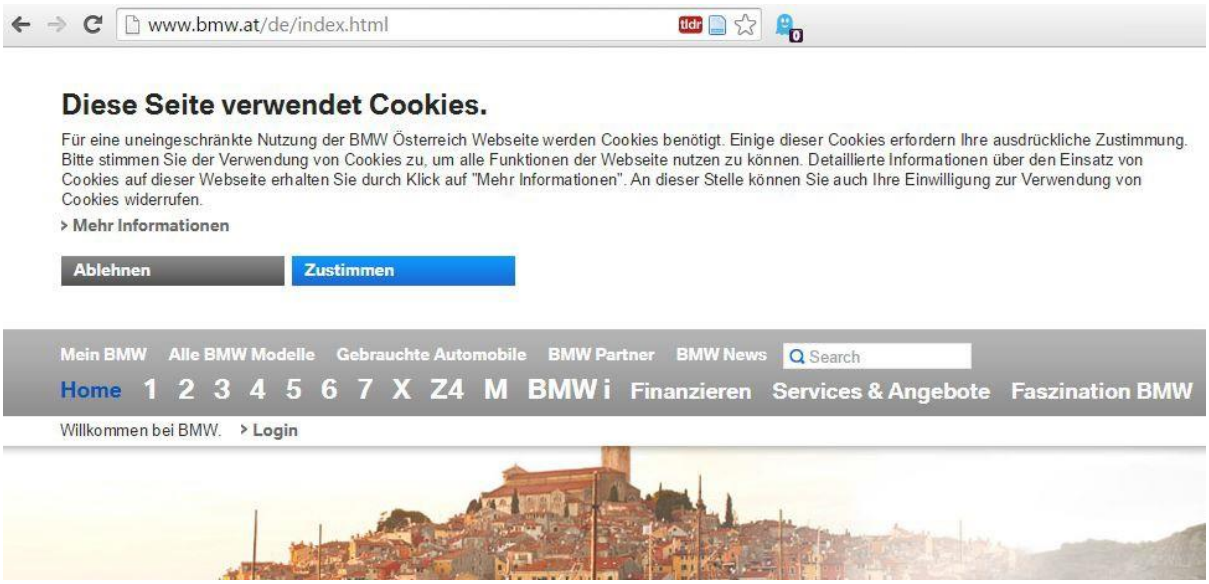
Auf eigenen, privaten Rechnern sollte immer entweder ein Virenscanner installiert, oder – bei Windows 10 - der normale Windows Virenschutz installiert bzw. aktiviert sein.

Wenn der Windows 10 Virenschutz (Einstellungen / Update und Sicherheit / Windows-Sicherheit) genutzt wird, sollte auch der automatische Windows Update aktiviert sein (Einstellungen / Update und Sicherheit / Windows- Update), damit der Virenschutz immer aktuell ist. Gerade neue Computer-Viren können besonders verbreitet und gefährlich sein.

Öffentliche oder von mehreren Personen genutzte Rechner sollten natürlich ebenfalls über den gleichen Schutz verfügen.

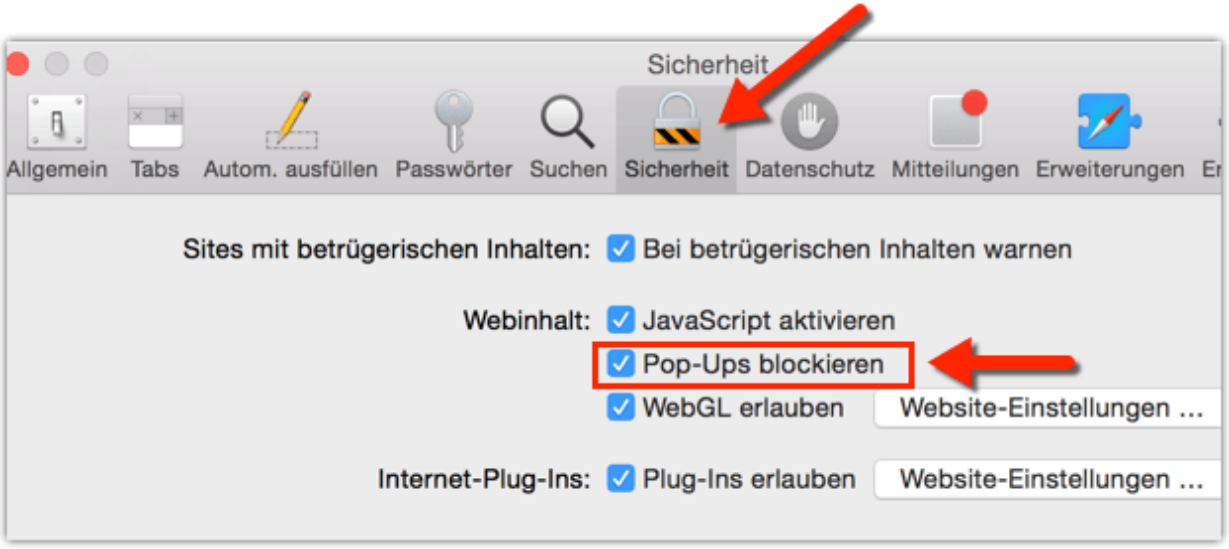
Cookies und Privatsphäre

Viele Webseiten fügen deinem PC kleine Dateien zu, die **Cookies** genannt werden. Cookies können deinem Computer helfen, mit dem **Webserver** und **deinem Browser** zu kommunizieren. Das bedeutet, die Cookies helfen bei der Identifizierung, wer den Computer und den Browser benutzt. Dadurch ist die Information über dich in deinem Browser für später gespeichert, z.B. beim Einloggen in deinen Email-Account oder Facebook-Konten. Außerdem helfen Cookies Webseiten kundenspezifisch vorzubereiten gemäß deines Browsing-Verlaufs. Cookies können auch benutzt werden, um **Browsing-Aktivität zurückzuverfolgen**.



Pop-up Fenster und Malware

Pop-ups sind kleine Browserfenster, die sich automatisch öffnen, wenn du eine bestimmte Website besuchst. Manchmal sind sie ein Teil des legitimen Funktionierens einer Seite. Oder sie enthalten **Werbung,** die nervig oder unangenehm sein kann. Pop-ups können **Schadsoftwares** enthalten – ein Programm, das deine Daten oder Software zerstören kann.



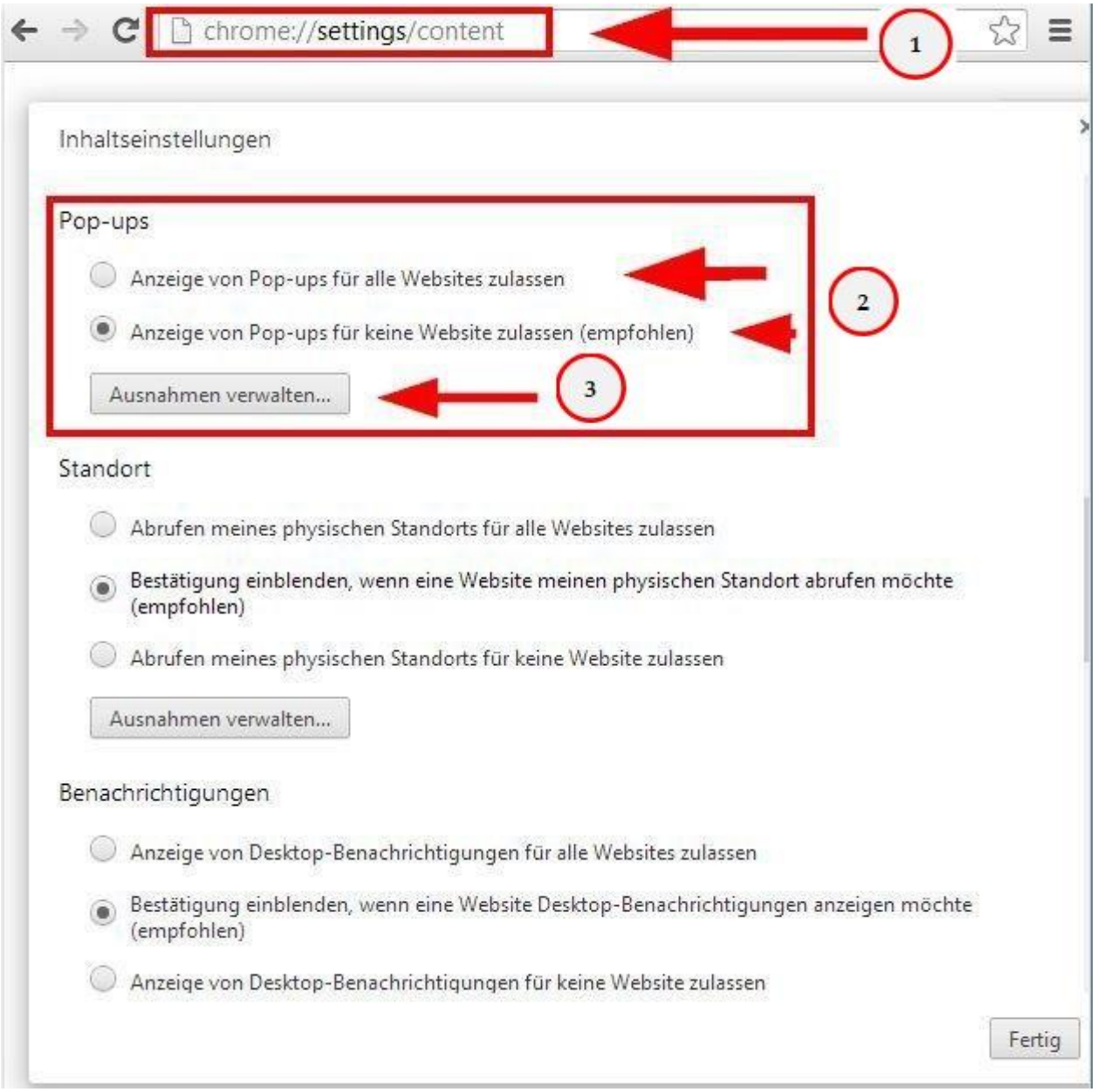
Deswegen ist es gut, den P**op-up Blocker** deines Browsers zu aktivieren. Auf der nächsten Seite zeigen wir dir, wie das geht.

Aktiviere den Pop-up-Blocker

1. Um den Pop-up Blocker zu aktivieren, gehe zu deinen Browser-Einstellungen / Optionen (oder Erweiterungen) → Inhaltseinstellungen → finde Pop-up Blocker

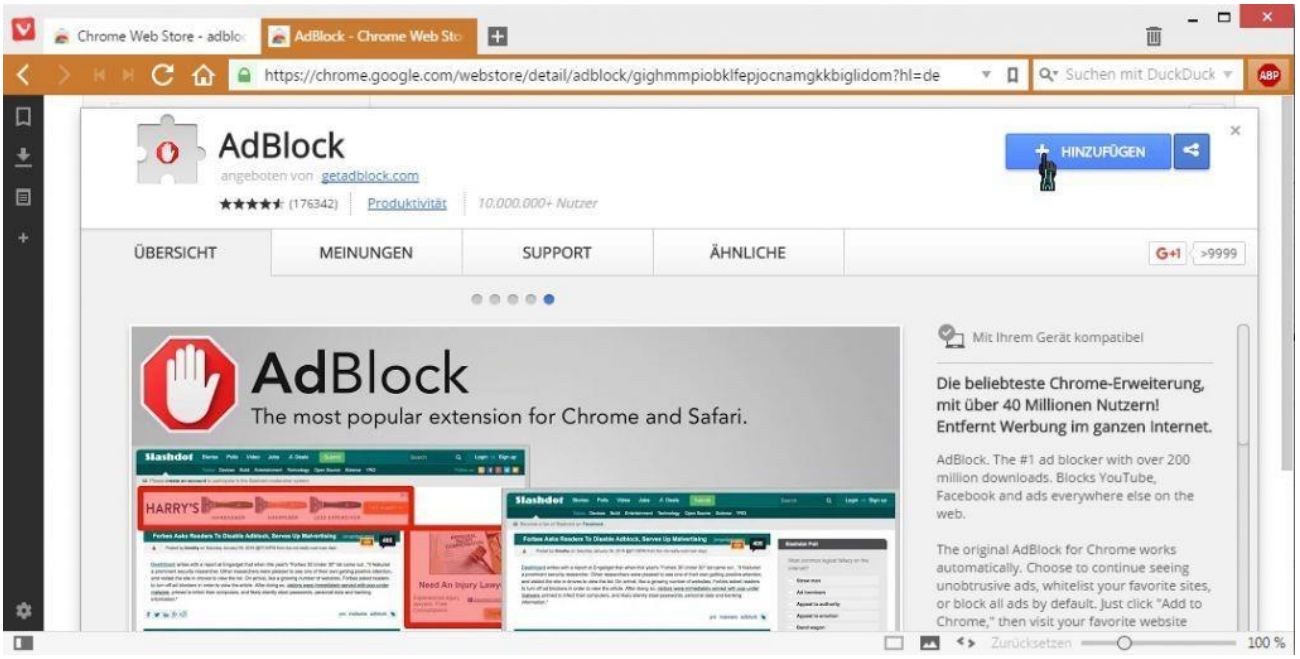
2. Aktiviere Pop-up Blocker: "Pop-ups blockieren". Wenn es sicher ist, dass die Webseiten keine schädigende Datei enthält: Pop-ups-Ausnahmen einstellen.

3. Gehe zu deinen Browser Einstellungen / Optionen (oder Erweiterungen) → Inhaltseinstellungen→ finde Pop-ups → Ausnahmen verwalten. Danach wirst du aufgefordert, die Links zu den Webseiten hinzuzufügen.



AdBlock

AdBlock ist eine externe und sehr zu empfehlende **Browser Erweiterung**, um Werbung während der Internetnutzung zu blockieren.



Private Informationen im Internet

Internetnutzung erfordert manchmal, persönliche Informationen mitzuteilen. Z.B. bei:

- E-Mail-Konten
- Soziale Netzwerke, z.B. Facebook
- Jobs Netzwerke, z.B. LinkedIn, XING
- Einkaufen, z.B. bei Amazone, eBay und anderen Online-Shops
- Cloud-Services für Unternehmen, z.B. SAP, Salesforce, etc.
- Geld-Transaktionen, z.B. Online-Banking;

Viele Menschen wissen nicht, dass die Webbrowser die persönlichen Daten, sowie **persönliche Aufzeichnungen, Telefonnummern** und auch manchmal **Bilder** abspeichern. Deswegen ist es möglich, diese Informationen abzufragen. Private Informationen im Internet können verschiedene Nachteile für dich haben.

Wenn du dich zum Beispiel bei einer Firma bewirbst, kann es sein, dass der Arbeitgeber ins Internet geht, um etwas über dich herauszufinden.

Wenn du dich bewirbst, achte also auf…

- … die Bilder und Informationen, die jeder auf deiner Facebook-Seite sehen kann

- … die privaten Informationen, die du im Internet (zum Beispiel auf Facebook) eingibst (Telefonnummer, Emailadresse…)

Übung:

Google deinen Namen und überprüfe, welche Informationen über dich online verfügbar sind.

Passwort-Sicherheit

Wenn Du ein starkes Kennwort erstellst, wird das Risiko reduziert, dass es jemand „knackt". Falls jemand dein Passwort „knackt":

1) …hast du unter Umständen anschließend keinen Zugang mehr zu deinen eigenen Daten wie E-Mail etc., da der Dieb als erstes ein neues Passwort vergeben wird, das du natürlich nicht kennst. Dein Passwort ist dann nicht mehr gültig.
2) …kann er alle deine Daten sehen, möglicherweise auch alle deine Kontakte
3) …kann er in deinem Namen auch E-Mails oder WhatsApp Messages versenden
4) Wenn du Online Banking machst oder ein PayPal Konto hast, kann der Dieb unter Umständen auch darauf zugreifen über dein Geld/deine Konten verfügen.

Als Kennwort nutzen viele Menschen ihr Geburtsdatum, die Namen der Eltern oder Ehegatten, Hobbies oder sehr einfache Muster. Dies solltest Du unbedingt vermeiden!

Hinweise zu starken Passwörtern:

➢ Verwende **niemals** personenbezogene Daten (z.B. Geburtsdatum, dein Name)
➢ Erstelle ein langes Passwort mit mindestens 8 Stellen
➢ Eine gute Regel für ein starkes Passwort ist folgende:

- Du denkst dir ein Wort oder einen kurzen Satz bzw. eine Folge von Worten aus, der für dich eine große Bedeutung hat und den du deshalb nie vergessen kannst, z.B. den Namen deines ersten Lehrers

„Abdulrahman“, oder einen Satz aus der Bibel oder dem Koran, der dir viel bedeutet und den du nie vergessen wirst, z.B. „Du sollst dankbar sein für das Geringste“, oder die Namen deiner Geschwister.

- Dann nimmst du dieses Wort, oder diese Worte, oder diesen Satz und veränderst es/ihn nach einer sehr einfachen Regel:
  - z.B. von dem Wort „Abdulrahman“ nimmst du jeden zweiten Buchstaben: „Abdulrahman“ = „burha“ und dann die übrigen Buchstaben „Adlamn“ und fügst beides zusammen: „burhaAdlamn“. Obwohl es nur ein einfaches Wort und eine einfache Regel sind, wird niemand so schnell auf ein Passwort wie „burhaAdlamn“ kommen. Du musst dir natürlich das Wort und die Regel selber ausdenken und gut merken. Es ist auch gut ein Sonderzeichen wie „-„ oder „%“ oder „?“ einzubauen („burha%Adlamn“).
  - Bei einem Satz oder einer Folge von Worten ist es vielleicht noch einfacher, hier nimmst du einfach den ersten Buchstaben von jedem Wort: „Du sollst dankbar sein für das Geringste.“ = “DsdsfdG“, oder „Peter, Hans, Sabine, Klaus, Ahmed“ = „PHSKA“, oder „PeHaSaKlAh“ und schon hast du ein kompliziertes Passwort, das es als normales Wort gar nicht gibt.
  - Wenn du das Wort bzw. den Satz und die Regel sehr einfach hältst, wirst du ich immer schnell erinnern können, obwohl das Passwort sehr stark ist.

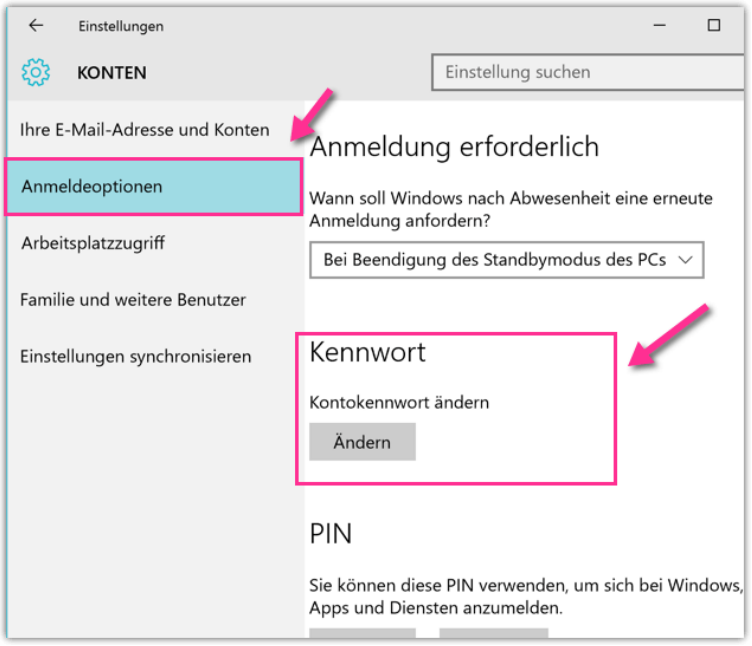
➢ Wenn du deine Passwörter notieren musst, bewahre sie an einem sicheren Ort auf. Schreibe sie aber niemals ganz auf, sondern nur einen Teil, der dir hilft, dich an das ganze Passwort zu erinnern.
  - Es gibt einfache, kostenfreie Programme und Apps, um Passwörter auf dem Smartphone oder PC zu speichern, ohne dass sie jemand anderes finden kann. Z.B.: Password-Safe

➢ Gib niemals deine Passwörter an andere weiter.

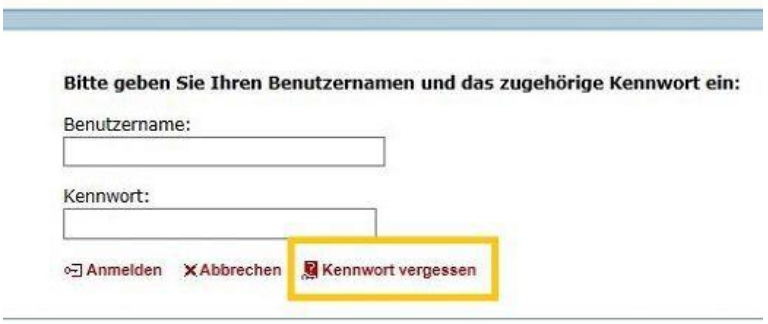
➢ Verwende unbedingt verschiedene Kennwörter für verschiedene Online-Konten, also niemals ein Passwort für mehrere oder gar alle wichtigen Konten. Sonst hat ein Dieb, der dieses eine Passwort findet, sofort Zugriff auf alle deine Konten/Websites, E-Mail etc. Besonders wichtig sind alle Konten, die irgendwie

mit Geld/Kaufen oder mit deinen persönlichen Daten wie E-Mail etc. zu tun haben.

- ➢ Deine Kennwörter sollten nicht nur Buchstaben, sondern auch Zahlen, Symbole, Groß- und Kleinbuchstaben enthalten
- ➢ Vermeide die Verwendung von oft verwendeten Wörtern und einfachen Mustern, z.B. 123456789
- ➢ Zufällige Passwörter sind sehr sicher, zum Beispiel H=jNp2#xhuon/h (leider sind sie schwer zu merken)



Du kannst dein Kennwort über **Kontoeinstellungen des Kontos** (Facebook, Email u.ä.) **immer ändern.** Normalerweise wird dabei nach deiner Telefon-Nummer oder alternativen E-Mail-Adresse gefragt. Bei der Kennwort-Änderung solltest du die Einstellungs-Anweisungen befolgen: Wenn du dein Kennwort vergessen hast, kannst du es **zurücksetzen**. Sende eine **Aufforderung** und folge den Anleitungen der Webseite. **Klicke auf "Passwort vergessen"**



Datensicherheit / Backup

Für alle eigenen Daten wie Kontakte, Adressen, E-Mails, Dokumente, Fotos – egal ob auf Computer oder Handy - ist es wichtig, dass sie **gesichert** werden!

Jedes technische Gerät kann immer plötzlich kaputt gehen. Wenn ein Computer kaputt geht, liegt das oft an der Festplatte, also dem Speicher des Computers. Wenn der Speicher erst einmal kaputt ist, sind die Daten in aller Regel verloren und können nicht mehr, oder nur mit sehr viel und teurem Aufwand wieder gerettet werden. Gleiches gilt auch für Handys, wobei hier zusätzlich die Gefahr des Verlierens oder eines Diebstahls sehr hoch ist.

Es ist also sehr wichtig, immer alle wichtigen Daten, die du auf dem Computer und dem Handy hast, zu sichern!

Zum Sichern gibt es grundsätzlich mehrere Wege:

1) Eine **physische Sicherung der Daten** machen, ein sogenanntes Back-Up. Hierzu nimmt man normalerweise einen externen Speicher (z.B. USB-Stick oder externe Festplatte), auf der die Daten gespeichert werden. Dies ist vor allem bei PCs üblich. Bei Handys ist dies kaum eine Alternative, da man die wichtigen Dateien nur schwierig (Android) oder gar nicht (iOS/iPhone) finden und kopieren kann.
2) Man kann solche Daten aber auch **im Internet (Cloud) sichern**, indem man die entsprechenden Dateien in eine Cloud kopiert. Besser ist es aber noch, ein sogenanntes Back-Up System zu nutzen, das diese Arbeit systematisch unterstützt und durchführt. Ein solches Back-Up System kann dann auch entweder auf einen externen Speicher (USB-Stick) oder in eine Cloud speichern. Ein solcher Cloud Speicher muss natürlich vorher angemeldet und eingerichtet werden.
3) Einige Anbieter wie Google haben aber auch komplette Lösungen, die praktisch alle Daten, die man im Alltag benötigt, in ihrer Cloud speichern. Der Vorteil ist hierbei, dass alle Daten von vorneherein und unabhängig vom jeweiligen Endgerät (PC oder Handy) immer nur im Internet gespeichert und zugänglich sind. Wenn ein Gerät (PC oder Handy) kaputt geht, oder gestohlen wird, ist das für die Daten ganz egal, weil man mit Hilfe des eigenen Login/Passwort mit jedem anderen Gerät wieder auf die eigenen Daten zugreifen kann. Der Nachteil an dieser Lösung ist natürlich, dass man immer nur etwas speichern oder abfragen kann, wenn man mit dem Internet verbunden, also Online ist. Google mit gmail und „Google

Drive“ ist hier eine komfortable und kostenlose Möglichkeit für praktisch alle Daten.

Ausloggen / Beenden der Arbeit am Computer

Wenn man die Arbeit am Computer beendet, ist es wichtig, sich auszuloggen (= abmelden). Dies gilt insbesondere für öffentliche Computer in Bibliotheken, Heimen oder Wohngemeinschaften oder in Firmen und Büros. Wenn man sich am Ende der Arbeit nicht ausloggt und den Computer ausschaltet, kann jeder, der Zugang zu diesem Computer hat, mit dem noch bestehenden Login von dir weiterarbeiten und deine Daten sehen, bzw. allgemein deinen Zugang für irgendwelche Dinge nutzen und es wird später immer so aussehen, als hättest du diese Dinge getan.

Wenn man sich irgendwo einloggt, meldet man sich dort an und wenn man sich ausloggt, meldet man sich wieder ab. Ausloggen muss man sich also immer genau so oft, wie man sich vorher eingeloggt hat:

1) Auf der Ebene von Programmen wie z.B. des E-Mailprogramms, oder Google, oder Facebook
2) Und am Ende immer auch auf der Ebene des Computers selbst.
3) Hinweis: Es wird in der Regel so sein, dass das Ausloggen aus dem Computer auch alle anderen vorher bestandenen Logins schließt und insofern alleine ausreicht.

NÜTZLICHE LINKS FÜR WEITERES LERNEN:

- https://www.digitalunite.com/guides
- https://www.gcflearnfree.org/basic-computer-skills/
- https://support.microsoft.com/en-us/products/windows?os=windows-7
- http://ecomputernotes.com/fundamental
- http://www.diffen.com/difference/Hardware_vs_Software
- Using windows help and support services
- https://guernseyhelp.sure.com/
- http://www.wikihow.com
- http://wikipedia.org/
- http://www.computerseite.net/computer-grundlagen/

QUELLENVERZEICHNIS:

- http://www.gcflearnfree.org
- https://www.digitalunite.com/guides
- http://www.fremontne.gov/DocumentCenter/View/1687
- http://www.diffen.com/difference/Hardware_vs_Software
- howcast.com youtube channel
- https://support.microsoft.com/en-us/products/windows?os=windows-7
- http://ecomputernotes.com/fundamental
- WINDOWS HELP AND SUPPORT CENTRE
- https://guernseyhelp.sure.com/
- http://www.wikihow.com
- http://wikipedia.org/
- https://gsuite.google.com/learning-center/products/calendar/get-started/
- GSuite YouTube Channel Tutorials
- https://www.howtogeek.com