# DANGER: Gefahren im Internet

**Vor was einen die Eltern nicht alles warnen. Man soll sich warm anziehen, nicht mit nassen Haaren aus dem Haus, Fremden gegenüber misstrauisch sein, nicht unüberlegt Verträge abschließen und die Haustür abschließen. Aber wie sieht's aus mit dem Internet? Fremde Personen verstecken sich hier zusätzlich noch unter merkwürdigen Pseudonymen. Irgendwelche tollen „Spar"-Verträge sind mit einem Klick abgeschlossen und Internet-Konten, egal ob bei Amazon, Facebook oder Instagram, stehen Hackern offen, wenn man seine Konten nicht richtig „abschließt". Ist erst einmal das E-Mail-Konto gehackt, stehen den Kriminellen fast alle Türen offen. Auf vielen Internetseiten meldet man sich nämlich nur mit seiner E-Mail-Adresse an und nicht mit einem frei erfundenen Namen wie „SweetSugar98". Die Adresse reicht dann aus, um Passwörter anzufordern oder zurücksetzen zu lassen. Ein Verfahren, was sich also der „neue Besitzer" zu nutzen machen kann, um sich Zugang zu weiteren Accounts, und damit zu den dort hinterlegten Daten von euch, zu verschaffen. Das E-Mail-Konto sollte daher mit einem starken Passwort geschützt sein, dass ihr für keine andere Website verwendet. Wie könnte aber jemand euer Kennwort ergaunern und was macht ihr am besten dagegen?**

**Pishing-Mails:** Ihr bekommt z.B. augenscheinlich eine Mail von Blizzard Activision, die euch mitteilen, dass irgendetwas mit eurem World-of-Warcraft-Account sei und man nun eure Anmelde-Daten und das Passwort benötigt. Natürlich will man nur euer Bestes. Folgt ihr dem Link, landet ihr auf einer Seite, die der originalen täuschend ähnlich sein kann, oft aber schon fürchterlich aussieht. Alle Daten, die ihr dort eingebt, landen dann bei irgendwelchen Oberlords. Erschlichene Passwörter müssen nur noch bei anderen Internetdiensten ausprobiert werden.

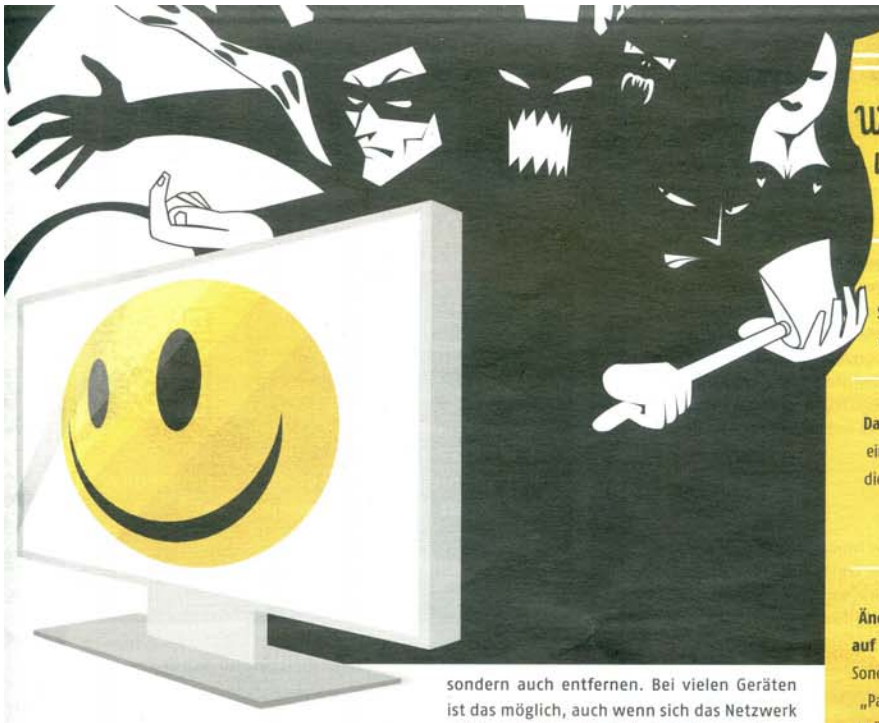
**Was kann ich tun?** Wichtige Schreiben von der Schule, Bank oder Behörden werden grundsätzlich nach alter Schule per Post verschickt. Ruft im Zweifelsfall lieber den Absender der E-Mail unter einer euch bekannten Nummer an. Nicht der, die in der zweifelhaften E-Mail genannt wird. Prüft die Aufmachung der E-Mail genau. Rechtschreib- und Grammatikfehler sowie unvollständige E-Mail-Signaturen und merkwürdige Absender-Adressen können Indizien sein. Am besten ignorieren oder gleich löschen.

**Key-Logger:** Es gibt kleine Programme, die jede eurer Eingaben aufzeichnen, wenn sie auf eurem Rechner landen. Diese Programme sind oft versteckte Prozesse, die auch automatisch gestartet werden, selbst nach dem Beenden oder einem Neustart eures PCs. Die aufgezeichneten Eingaben werden in einer einfachen Datei an den Hacker gesendet. Dort muss er nur nach Eingaben wie „@" oder pseudonym-ähnlichen Begriffen suchen, die ihr oft unmittelbar vor dem Passwort eingebt.

**Was kann ich tun?** Wenn ihr Dateien herunterladet, achtet unbedingt auf die Quellen. Handelt es sich um eine seriöse Seite wie chip.de oder habt ihr den Link auf der fünften Seite der Google-Suche gefunden? Merkwürdige Dateinamen oder Prozesse solltet ihr googeln. Viele Foren und Internetseiten geben Tipps und Infos dazu, u.a. wie ihr die Dateien los werdet.

**Cookies:** Diese kleinen Dateien können äußerst praktisch und gefährlich zu gleich sein. In ihnen lassen sich alle möglichen Benutzer- und Browserdaten speichern. Ein klassisches Beispiel ist das automatische Anmelden auf euren Lieblingsseiten. Besucht ihr eine Seite, prüft der Browser, ob gültige Cookies vorliegen und ruft die gespeicherten Daten ab. So bleiben euch z.B. erneute Eingaben erspart. In Cookies können aber auch Daten gespeichert werden, die Auskunft über einzelne Seitenaufrufe geben und welche Unterseiten oder Links auf einer Website aufgerufen wurden. So nutzen Google Ads Cookies, die von Amazon angelegt wurden, um zielgerichtet Werbung zu schalten. Dass genau das Computerspiel euch auf einer Seite angezeigt wird, dass ihr zuvor bei Amazon gesucht habt, ist kein Zufall. Zwielichtige Seiten können also Cookies speichern, die das Browserverhalten manipulieren können oder bestimmte Cookies auslesen, die von anderen Seiten unbedacht angelegt wurden.

**Was kann ich tun?** Stellt euren Browser so ein, dass Cookies gelöscht werden, wenn der Browser beendet wird oder wenigstens, wenn die Cookies nicht mehr gültig sind (Webseiten, die Cookies anlegen, bestimmen die Gültigkeit). Sie können auch manuell wie der Browserverlauf gelöscht werden. Außerdem gibt es Browser-Erweiterungen, die verhindern, dass generell Cookies angelegt werden. Hier empfehle ich „Ghostery".



**Offenes WLAN-Netzwerk:** Unterwegs und kostenlos im Internet surfen anhand offener WLAN-Netzwerke klingt praktisch. Ob im Café, Hotel oder am Flughafen: jeder geht mal gerne schnell und kostenlos mit dem Laptop, Smartphone oder Tablet ins Internet. Durch das automatische Verbinden mit einem bekannten WLAN-Netz, ohne euch erneut anmelden zu müssen, wird euch das zunehmend leichter gemacht. Sobald euer Gerät jedoch einmal in einem unverschlüsselten WLAN war, sucht es sekündlich nach ihm bekannte Hotspots. Hacker nutzen diese permanente Suche mobiler Geräte nach WLAN-Anschlüssen für kriminelle Zwecke aus. Mit der sogenannten WLAN-Box können Hacker vortäuschen, genau das unverschlüsselte WLAN zu sein, nach dem euer Gerät sucht, obwohl es sich gar nicht in der Nähe befindet. Zum Beispiel gibt sie sich als das Netzwerk des Cafés eures einstigen Urlaubsorts aus, in das ihr damals eingeloggt wart. Wenn ihr im Browser nun Passwörter eingebt oder Daten verschickt, kann das abgefangen werden. Ein geschütztes WLAN, wie z.B. das von zu Hause, könnt ihr ruhig speichern. Die Box kann nämlich nur unverschlüsselte WLANs vortäuschen. Eigentlich sollte die Box Firmennetze und Geräte sicherer machen.

**Was kann ich tun?** Ihr solltet offene WLAN-Verbindungen nicht längerfristig speichern, sondern auch entfernen. Bei vielen Geräten ist das möglich, auch wenn sich das Netzwerk nicht in Reichweite befindet. Bei Apple erschreckenderweise nicht.

**Identitätsdiebstahl:** Wer sich nicht mehr in sein Facebook-Account einloggen kann, ist vermutlich Opfer vom Identitätsdiebstahl geworden. Die Folgen sind vielleicht nicht auf Anhieb ersichtlich. Ist ja nur ein Facebook-Profil, richtig? Von den persönlichen Sachen wie Aufenthaltsorte, Freunde, Schule oder Arbeitgeber abgesehen, die man dem Hacker zur Verfügung stellt, gibt es mittlerweile zahlreiche Internetdienste, die das Einloggen durch Google Plus, Twitter oder eben auch Facebook ermöglichen. Der Hacker kann also mit eurem Facebook-Konto sich nicht nur Zugang zu von euch benutzten anderen Diensten verschaffen. Er kann ebenfalls neue Zugänge erstellen und in eurem Namen Beiträge veröffentlichen und Daten verbreiten. Vor allem Pishing-Nachrichten an Freunde schicken. Wenn diese von einer „vertrauten" Person eine Nachricht bekommen, werden sie unter Umständen unvorsichtiger und gehen darauf ein. Facebook- und Google-Plus-Nutzer mit vielen Freunden sind besonders interessant für diese Art von Internetkriminalität.

**Was kann ich tun?** Sichert auch eure Konten in sozialen Netwerken mit sicheren Passwörtern und verbindet eure Accounts nicht achtlos mit jedem Dienst, der diese Möglichkeit anbietet.

## Was kann man noch tun um das Surfverhalten sicherer zu machen?

**Programme sollten von seriösen Software-Portalen** oder direkt von der Seite des Entwicklers legal gedownloadet werden.

**Dateiendungen überprüfen!** Wenn ihr euch z.B. ein Bild oder ein Archiv herunterladen wollt und die Website euch eine Datei mit der Endung *.exe anbietet, solltet ihr misstrauisch sein und sie nicht anrühren.

**Ändert regelmäßig eure Passwörter und achtet auf ihre Sicherheit.** Euer Passwort wird sicherer mit Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben. „Passwort" oder „12345" sind KEINE sicheren Passwörter! Auch keine Namen oder anderen Begriffe, die in einem Wörterbuch vorkommen. Am besten nutzt ihr Kombinationen oder Abkürzungen eines Satzes, den ihr euch leicht merken könnt. So kann man aus dem Satz „Ich surfe gerne auf Facebook. de" das Passwort: „isgaFB.de". Das könnt ihr noch beliebig mit Sonderzeichen erweitern, dessen Muster ihr euch leicht merken könnt. So wird aus dem Passwort: „!§isgaFB.de§!".

**Verlasst euch nicht blind auf Antivirus-Programme,** die ein falsches Sicherheitsgefühl vermitteln können. Diese sind nur so gut wie sie programmiert wurden und lassen auch mal eine schädliche Datei durch und blockieren Dateien, die virenfrei sind (auch „falsch-positiv" genannt).

**Man muss also keine Wissenschaft daraus machen. Denn in erster Linie soll natürlich alles so bequem bleiben wie bisher. Wer aber diese grundlegenden Dinge beachtet, steht bereits deutlich sicherer da. An erster Stelle sollte deshalb immer das eigene Surfverhalten stehen. Ihr habt selbst noch ein paar Tipps oder Fragen? Schreibt uns auf facebook.com/sCHiLLERonline**