

Sicherheit im Internet

Sicherheits-Tipps

Beachte bitte die wichtigsten fünf Regeln, sie bewahren dich vor viel Sorgen und Ärger!

- Behalte deine Passwörter für dich, denn sie sind wie Schlüssel.
- Gib deine E-Mail-Adresse und andere persönliche Angaben nur zurückhaltend weiter.

Tipps für die Praxis

Die Angaben dieses Kapitels beziehen sich vorwiegend auf den Selbstdatenschutz. Anregungen zum  technischen Datenschutz, die vor allem die Kustoden betreffen (Filterprogramme, Selbstdeklaration von Web-Seiten, Privacy Policies, Virenschutzprogramme) werden hier nicht angesprochen.

Ohne spezielle Massnahmen ist die Sicherheit der Kommunikation im Internet nicht gewährleistet. Es kann nicht überprüft werden, wer das Gegenüber im Internet oder E-Mail wirklich ist (keine Authentizität). Ebenso kann nicht mit Sicherheit gesagt werden, ob das, was wir empfangen, tatsächlich von der vermeintlichen Person und in dieser Art abgeschickt wurde (keine Integrität). Versendete E-Mails entsprechen von der Sicherheit her etwa einer versandten Postkarte (keine Vertraulichkeit). Mit speziellen Verschlüsselungsprogrammen lässt sich die abgeschickte Botschaft in eine Zeichenfolge umwandeln, welche nur die Empfängerin oder der Empfänger mit dem entsprechenden Schlüssel wieder in den Ausgangstext zurückübersetzen kann. Ohne den richtigen Code bleibt die Nachricht unverständlich. Verschlüsselungsprogramme werden beispielsweise im E-Banking eingesetzt, können aber auch privat genutzt werden. PGP (Pretty Good Privacy) ist ein Verschlüsselungsprogramm für elektronische Post und Dateien aller Art. Als selbstentschlüsselndes Archiv können auch ganze Verzeichnisse weitergegeben werden, ohne dass der Empfänger PGP haben muss.

Ein «Cookie» ist eine kleine Textdatei, die von einer besuchten Webseite auf dem Computer gespeichert wird und worin alle Aktivitäten auf der entsprechenden Seite festgehalten werden. Es dient hauptsächlich als elektronischer Merkzettel für den Server, worin benutzerspezifische Abfragen oder die Häufigkeit und Dauer der Nutzung bestimmter Seiten festgehalten werden. Somit hinterlässt Surfen im Internet Spuren auf dem Computer, welche rückverfolgt werden können. Der Browser lässt sich entsprechend konfigurieren, dass nur nach aktiver Bestätigung ein «Cookie» gespeichert werden kann. (Oftmals kann man die Speicherung ohne Einschränkung ablehnen.) Den Schülerinnen und Schülern wird damit die Menge der gespeicherten «Cookies» bewusster.

Ohne Kenntnisse der Betroffenen und auch ausserhalb der Kontrolle der Schule können Verknüpfungen und Verbreitungen der Inhalte eigener Seiten geschehen. Dies ist ein weiterer Faktor, den es zu beachten gilt. In einer Suchmaschine kann mit der Eingabe «Link:www.XYZ.ch», nach allen Inhalten gesucht werden, welche auf die entsprechende Seite verweisen.

- Die Schülerinnen und Schüler müssen auf die eingeschränkte Sicherheit der Kommunikation hingewiesen werden. Ein verantwortungsvoller Umgang mit persönlichen Daten ist ein wichtiger Punkt für die zu erreichende, notwendige Medienkompetenz.
- Eigene Angaben sollen nur zurückhaltend erfolgen. Eine Eintragung in Mailinglisten,

Newsgroups wird nicht empfohlen. Wenn im Zusammenhang mit einem Projekt (auf der Oberstufe) eine Eintragung hilfreich und nützlich erscheint, wählt man am besten eine unpersönliche Mail-Adresse eines grossen Anbieters, um Spam-Mails möglichst zu umgehen.

- Bei der Hinterlegung der Schul-E-Mail-Adresse auf der Homepage kann das @-Zeichen durch ein &-Zeichen ersetzt werden. Die Adresse kann so nicht automatisch in Verzeichnisse aufgenommen werden.

Es gibt aber auch die Möglichkeit, mit spezieller Software (Email Protector) die E-Mail-Adressen in JavaScript umzuwandeln und diese so vor Crawlern zu schützen.

- Die Schulleitung oder die Lehrerschaft muss sich mit der Frage auseinandersetzen, ob persönliche E-Mail-Adressen oder eine Adresse für die ganze Klasse eingerichtet werden sollen. Wir empfehlen persönliche E-Mail-Adressen erst ab der Mittelstufe.
- Eine grundsätzliche Entscheidung betrifft auch die Nutzung von Chats. Wird in einer Schule das chatten erlaubt, empfehlen wir, dies nur unter Aufsicht zu ermöglichen, Pseudonyme zu verwenden und die Schülerinnen und Schülern darauf hinzuweisen, auf Angaben zur Person zu verzichten.
- Durch E-Mails können Viren auf die eigenen Computer gelangen! Deshalb empfiehlt sich ein regelmässiges Backup, damit bei einem Schadensfall nicht zu grosse Datenverluste entstehen. Ein aktualisiertes Antivirenprogramm sollte unbedingt auf den Geräten installiert sein.
- Den Browser so konfigurieren, dass «Cookies» nur gespeichert werden, wenn die Schülerin oder der Schüler diese aktiv akzeptiert. Periodisch können sie von der Lehrperson oder dem Systemverantwortlichen gelöscht werden.
- Das Einrichten von Verschlüsselungsprogrammen ist empfehlenswert, wenn via E-Mail auch sensible Daten wie Schülernoten versandt werden. Hier erscheint uns der herkömmliche Weg via Briefpost oder die direkte Übergabe angemessener.
- Mit genauen Nutzungsregelungen (Zeitpunkte, Dauer, Aufsicht und Betreuung), gut strukturierten Arbeitsaufträgen sowie fundierten Informationen können die Schülerinnen und Schüler einen kompetenten Umgang mit dem Internet lernen. Sie wissen, dass ihre Arbeit Spuren hinterlässt und können Sicherheitsrisiken einschränken.

FAQ

Trage ich als Lehrperson die Verantwortung dafür, mit wem und worüber in einem Chat während der Unterrichtszeit gesprochen wird?

Da E-Mails sowie Gespräche in Chaträumen dem absoluten Briefgeheimnis unterliegen, liegt die Verantwortung über deren Inhalte rechtlich gesehen nicht bei der Lehrperson. Die Schule muss sich also überlegen, ob sie das Chatten grundsätzlich erlauben will oder nicht. Dies gilt besonders auch für die unterrichtsfreie Zeit. Wir empfehlen in jedem Fall, das Chatten nur unter Betreuung einer Lehrperson zuzulassen.

Muss ich als Lehrperson die Betreuung beim Zugang zum Internet ausserhalb des Unterrichts gewährleisten (während der Pause, in der Mittagszeit oder nach dem Unterricht)?

Wenn sich eine Schule dafür entscheidet, den Zugang zum Internet auch ausserhalb des Unterrichts für Hausaufgaben oder andere Arbeiten im Zusammenhang mit der Schule zu erlauben, empfehlen wir die Betreuung durch eine Lehrperson. Diese kann bei anfallenden Fragen Hilfestellungen geben und ist berechtigt, Schülerinnen und Schüler, die sich nicht an die Vereinbarung der Schule halten, wegzuweisen und die zuständige Lehrperson zu informieren. Die Betreuung kann durch Lehrkräfte, welche in ihrer unterrichtsfreien Zeit zur Vorbereitung im Schulhaus anwesend bleiben oder beispielsweise durch eine dafür ausgebildete Betreuungsperson (Bibliothekarin, Hauswart) organisiert werden. Das Eintragen in Benutzungslisten hilft bei der Erfassung der anwesenden Schülerinnen und Schüler. Eine technische Betreuung und Hilfestellung kann evtl. auch durch Schülerinnen und Schüler angeboten werden.

Bin ich verpflichtet, die Schülerinnen und Schüler über die Rechtslage zu informieren?

Zur Bildung von Medienkompetenz, welcher im Umgang mit dem Internet eine herausragende Bedeutung zukommt, ist es unerlässlich, vollständig, altersgemäss und angemessen zu informieren. Wichtig ist in diesem Zusammenhang auch, dass die Kinder und Jugendlichen verstehen lernen, aus welchen Überlegungen Gesetzesgrundlagen erstellt wurden, und dass diese nicht aus Willkür entstanden sind.

Wie kann ich unser System vor Viren, welche durch E-Mails ins System gelangen, schützen?

Sie sollten unbedingt ein Antiviren-Programm installiert haben und beachten, dass dieses auch aktualisiert werden muss. Stellen Sie die Sicherheitseinstellungen im Browser auf die höchste Stufe! Machen Sie die Schülerinnen und Schüler darauf aufmerksam, dass sie keine Mails öffnen sollen, deren Absender sie nicht kennen! Besser ist es, solche Mitteilungen ungelesen zu löschen. Attachments mit ausführbaren Programmen (*.com, *.exe) sollten nicht geöffnet werden. Regelmässige Backups schützen vor grossem Datenverlust, falls dennoch ein Virus ins System gelangt.

Wie kann ich vorgehen, wenn eine Schülerin oder ein Schüler beleidigende, anonyme Mails erhält?

Zum Teil ist es leider unmöglich, den Absender oder die Absenderin der unerwünschten Mails zu eruieren. Es besteht jedoch die Möglichkeit, mittels entsprechender Filtersoftware, bestimmte sich wiederholende Adressen zu sperren. Der beste Schutz gegen ungewollte und störende Spam-Mails ist, die Adresse nicht weiterzugeben.

Literatur und Links