Sicherheit im Netz

THEORIE

T

1. Gefahren im Netz

In den Grundlagen hast du gelernt, wie du deinen Computer schützen kannst.

Wenn du dich auf deinem Computer mit dem Internet verbindest, bist du automatisch zahlreichen Gefahren ausgesetzt. Unbefugte können sich zum Beispiel Zutritt auf deinen Computer verschaffen und Schaden anrichten, auch wenn dieser nicht sofort sichtbar ist.

Umso wichtiger ist es, dass dein Gerät auch hier gut geschützt ist und du dich im Umgang mit dem Internet an bestimmte Regeln hältst.

Zunächst zeigen wir dir die wichtigsten Gefahren im Internet auf.

1.1. Anonymität

Im Internet kann jeder User (= Benutzer) sich als jemand anderes ausgeben als er/sie in Wirklichkeit ist. Oftmals geben sich zum Beispiel Erwachsene als Jugendliche aus und nehmen Kontakt zu anderen Jugendlichen auf.

Stell dir vor, du bist in einem Chatforum angemeldet und plötzlich erhältst du eine Anfrage von einer unbekannten Person. Diese postet freundliche für dich ansprechende Bilder, erzählt von den gleichen Hobbys, schmeichelt dir mit netten, verständnisvollen Worten etc. Zudem schickt sie dir Bilder von angeblich sich selbst. Du findest diese Person auf dem Bild sehr sympathisch oder verliebst dich sogar in sie. Nach und nach gewinnt diese Person dein Vertrauen.

Irgendwann fordert dich diese Person auf, Bilder von dir zu schicken. Vielleicht fordert sie sogar Bilder von dir in Unterwäsche oder Nacktbilder. Es könnte auch sein, dass sich diese Person mit dir treffen möchte.
In Wirklichkeit steckt oftmals eine völlig andere Person dahinter. Die Nachrichten dieser Person sind nicht ernst gemeint, die geposteten Bilder sind gefälscht. Diese Person will dir schaden und du kannst schnell zum Opfer von sexuellem Missbrauch werden.

Tipp:

Sprich dich zuerst mit deinen Eltern ab und informiert euch, welche Chaträume vertrauenswürdig sind und von einem Moderator betreut werden. Verwende im Chat nur «Nicknames», deinen richtigen Namen gibst du nicht bekannt. Gib keine Adressen und Telefonnummern im Internet bekannt. Poste keine unangemessenen Fotos von dir. Triff dich nie alleine mit Personen, die du nicht kennst. Nimm eine erwachsene Person zu einem Treffen mit. Sei immer misstrauisch und hinterfrage.

1.2. Datenmissbrauch

Beim Surfen im Netz oder auf Social Media, wie zum Beispiel Whatsapp, Instagram, Snapchat etc. gibst du viel über dich preis. Diese Informationen können dann missbraucht werden. Zum Teil gibst du auch unwissentlich Daten weiter. Zum Beispiel können Apps auf deine Kontakte greifen, ohne dass du es merkst. Das führt dazu, dass du mit (Spam) Mails überflutet wirst. Im Extremfall führt es auch zu Belästigungen, Verfolgungen, Erpressungen usw.

Tipp:
Überlege gut, welche persönlichen Angaben du über dich (und bei welchem Anbieter) veröffentlichst. Überprüfe in deinem Profil deine Privatsphären-Einstellungen und schränke ein, wer welche Infos einsehen darf. Auch wenn du alles «privat» eingestellt hast, hast du keine Garantie vor Datenmissbrauch. Deshalb überlege gut, was du publizierst!!

1.3. Cybercrime

Cyberkriminelle können mit verschiedenen Methoden versuchen, dich abzuzocken und so an deine Daten zu kommen oder sie können dich erpressen. Mit deinen Daten können Sie zum Teil unglaublichen Schaden anrichten (z.B. Geld von deinem Konto abheben, Reisen buchen, Waren bestellen usw.) Oder du erhältst von «Fake-Firmen» eine eMail mit einem Anhang. Wenn du diesen Anhang öffnest, kann dieser Schaden auf deinem Gerät verursachen.

Tipp:
Auch hier gilt, gib keine persönlichen Angaben (Namen, Adressen, Post- und Bankkonten etc.) von dir preis. Zudem solltest du vorsichtig sein, was du herunterlädst. Mails von unbekannten Absendern solltest du nicht öffnen und schon gar nicht deren Anhänge.

1.3.1 Von Viren, Würmern und Trojanern

Es gibt verschiede Arten von Schadsoftware. In der Fachsprache heisst diese Malware, was so gut wie schädliche Software bedeutet. Diese zielen darauf ab, dein Gerät auszuspionieren oder es sogar zu zerstören.

Solche Programme werden von sogenannten Hackern programmiert. To hack bedeutet: in etwas eindringen.

Hier erhältst du einen kurzen Überblick der bekanntesten Malware-Arten:

Viren:	befallen Dateien oder Datenträger und können sich nur auf anderen Geräten verbreiten, wenn diese infizierten Dateien von den Benutzern an weitere Geräte weitergegeben werden (z.B. via USB-Stick).
Würmer:	Würmer verbreiten sich selbständig von Computer zu Computer über ein Netzwerk oder die Internetverbindung (z.B. über eMails).
Trojaner:	sind getarnt als harmloses oder sogar nützliches Programm oder Dokument. Wenn du die Datei dann öffnest, kann diese Schadsoftware unbemerkt dein Gerät ausspionieren und kommt so an sensible Daten wie zum Beispiel an Passwörter und anderes. Besonders gefährlich sind die Backdoor-Trojaner. Das sind Hilfsprogramme, mit welchen ein Hacker auf fremde Computer zugreifen kann.

Spyware: spioniert persönliche Daten und Surfgewohnheiten eines Users aus und überträgt sie über das Internet. Dadurch können sie gezielt Werbung auf deinem PC machen, was dich zum Kaufen, Buchen etc. animiert.

Hoax: ist ein «schlechter Scherz» und wird für eine Falschmeldung verwendet. Meistens wird man gebeten, die Nachricht an Freunde und Bekannte weiterzuleiten.

Adware: sind kostenlose Software-Angebote und Apps, die Werbung einblenden. In der Regel sind diese nicht gefährlich.

Scareware: haben die Absicht, User zu verunsichern und werben damit, dass du deinen PC schützen sollst, da er scheinbar von Viren etc. befallen sei. Sie verleiten dich zum Kauf einer Software, die dieses Problem angeblich beseitigen soll.

Ransomware: sperrt den Zugriff auf die Benutzeroberfläche und fordert den Benutzer zur Zahlung.

Phishing: sind betrügerische Emails. Das sind zwar keine Schadprogramme, aber trotzdem höchst gefährlich. Sie locken dich auf gefälschte Internetseiten. Sie sehen zwar genauso professionell aus wie die Originale (z.B. von der Post oder einer Bank). Wenn du dich dann dort mit deinen Konto-Zugangsdaten anmeldest, können sie dein Post- bzw. Bankkonto plündern.

1.3.2 Woran erkennst du, ob dein PC mit Malware infiziert ist?

- Beim Surfen tauchen Popups für Antivirenprodukte auf
- Programme starten von alleine auf
- Du hast plötzlich eine neue Toolbar auf deinem Browser oder deine Einstellungen sind verändert
- Der PC und/oder das Internet sind langsamer als gewohnt
- Du erhältst viele Systemfehlermeldungen von Windows

1.4. Cybermobbing/ Cyberbullying

Über Social Medias und Chats werden Opfer bedroht, gedemütigt, beleidigt, schikaniert und erpresst. Oftmals werden anonyme oder Fake-Profile erstellt, so dass unbekannt ist, wer dahinter steckt. Ihnen ist es oftmals egal, wie es dem Opfer geht. Für das Opfer ist das sehr schlimm, weil viele andere das mitbekommen und mitmachen und es dann auch noch weitergeht (z.B. in der Schule, Pausenplatz usw.)

Tipp:
Wenn du merkst, dass du oder jemand anderes ein Mobbing-Opfer ist, melde dies den entsprechenden Social Medias (= Spam melden) und blockiere diese Profile. Erstelle allenfalls Screenshots, damit du Beweise hast. Melde dies dann deinen Eltern und Lehrpersonen. Cybermobbing ist strafbar.

1.5. Fake News/Hate Speech

Fake News sind bewusst verbreitete Falschmeldungen. Hate Speech ist Hass und schlimme Beleidigungen, welche in Beiträgen oder Kommentaren verbreitet werden. Dieser Hass richtet sich

in der Regel gegen Personen oder bestimmte Personengruppen. Diese werden oftmals auch von anonymen Absendern veröffentlicht.

Tipp:
Glaube nicht alles, was im Internet verbreitet wird und mach bei solchen Dingen nicht mit. Nutze die Funktionen «Spam melden» oder «Blockieren».

1.6. Cybergrooming

Unter Cybergrooming versteht man das gezielte Ansprechen von Kindern und Teenagern, um sie zu schockieren, zu motivieren von sich sexuelle Fotos oder Videos zu machen, sie zu sexuellen Handlungen zu überreden, sie zu treffen oder einfach sie sexuell zu belästigen.

Dazu nehmen Erwachsene in Chatrooms eine falsche Identität an und geben sich als Gleichaltrige aus. So können sie den Kontakt zu den Jugendlichen aufbauen und sich unbemerkt über das Leben, den Tagesablauf, den Wohnort usw. informieren. So kann es also sein, dass ein erwachsener Mann sich als 13 jähriges Mädchen im Chat ausgibt. Am Anfang sind diese sehr aufmerksam, einfühlsam, freundlich und verständnisvoll. Sie zeigen Interesse an den Jugendlichen, kennen ihre Wünsche und Bedürfnisse und gewinnen nach und nach ihr Vertrauen. Ihr Ziel ist es aber, sexuelle Unterhaltungen im Chat zu führen und die Teenager zu motivieren, sexuelle Fotos oder Videos von sich zu machen und diese dann zu veröffentlichen. Cybergrooming-Täter sind meistens Männer, welche den Kontakt sowohl zu Mädchen wie auch zu Jungs suchen.

Tipp

Häufig sind Cybergrooming-Täter für Jugendliche schwer zu erkennen. Sei in Chats immer misstrauisch und vorsichtig, wem du was mitteilst. Wenn du ein komisches Gefühl hast oder dein Chatpartner versucht dich zu überreden das Gespräch fortzusetzen, informiere deine Eltern. Ebenfalls bei komischen Fragen wie zum Beispiel, «Kannst du mir ein Foto von dir schicken? Kann ich dich per Webcam sehen? Wo wohnst du? Bist du alleine? Was trägst du für Kleider?» handelt es sich voraussichtlich um einen Cybergrooming-Täter.

1.7. Sexting

Beim Sexting geht es um das Versenden und das Verbreiten von anzüglichen Inhalten, also zum Beispiel das Versenden von Nacktfotos, Fotos in Unterwäsche, usw.

Ein Beispiel dazu: Du hast gerade jemanden kennengelernt und flirtest über Social Media. Weil du dieser Person imponieren möchtest, versendest du ein erotisches Bild von dir (z.B. posierst du sexy in Unterwäsche oder nackt). Diese Person ist vielleicht stolz oder prahlt damit und sendet es an weitere Bekannte. So wird dein Bild, welches ursprünglich nur für eine Person gedacht war, innert kürzester Zeit rasant verbreitet. Im schlimmsten Fall kann dies sogar bis zum psychischen Terror und zu Mobbing führen.

Tipp:
Auch wenn du grosses Vertrauen zu dieser Person hast, sende niemals intime Fotos. Was du

einmal ins Netz gestellt hast, kannst du praktisch nicht mehr entfernen. Deshalb überlege zuerst, bevor du handelst!

1.8. Happy Slapping

Unter Happy Slapping – zu Deutsch «fröhliches Schlagen» - wird das Filmen von Schlägereien, Hänseleien, Demütigungen usw. verstanden. Bereits eine kleine Schlägerei oder Hänselei auf dem Pausenplatz kann für das Opfer sehr verletzend sein. Ganz zu schweigen, wenn dies noch gefilmt und verbreitet wird. Happy Slapping ist strafbar. Gemäss Strafgesetzbuch ist bereits der Besitz von solchen Gewaltvideos gegen Menschen und Tiere verboten und kann strafrechtlich verfolgt werden.

2. Regeln

Im oberen Kapitel hast du verschiedene Gefahren kennengelernt und weisst, wie du dich verhalten solltest.

Wie überall gibt es auch im Internet Regeln, an welche du dich halten musst.

2.1. Urheberrecht

Im Internet kannst du unglaublich viele tolle Dinge tun. Unter anderem kannst du coole Spiele, Filme, Songs, Bilder etc. herunterladen. Allerdings ist das Herunterladen häufig illegal, da diese Dateien urheberrechtlich geschützt sind. Illegale Downloads sind strafbar und können verfolgt werden.

Tipp:
Sei dir bewusst, dass viele kostenlose Downloads illegal und strafbar sind. Surfe nur auf geprüften Download-Seiten und lade nur Dateien herunter, die wirklich legal sind. Häufig musst du eine kleine Gebühr bezahlen. Frage immer zuerst deine Eltern.

Wenn du Bilder herunterlädst, darfst du diese nur für deinen privaten Gebrauch verwenden.

2.2. Das Internet macht süchtig

Wenn du täglich mehrere Stunden im Internet surfst und kein Interesse hast, dich mit deinen Freundinnen und Freunden zu treffen, kannst du abhängig werden. Du verlierst dich in deiner eigenen Cyberwelt und somit den Bezug zur Realität. Zudem wirst du einsam, weil du den Kontakt zu deinen Freunden nicht mehr pflegst.

Tipp:
Vereinbare mit deinen Eltern feste Internetzeiten. Pflege den Kontakt zu deinen Freunden, denn sie sind wichtig. Verbringe Zeit draussen an der frischen Luft. Dies ist gesund und gibt dir neue Energie. Denk daran, das Internet läuft dir nicht davon, Freunde können das aber!

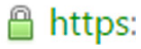
2.3. Das Internet vergisst nie

Wenn du einmal ein Bild oder ein Video im Netz hochgeladen hast, wird es irgendwo immer gespeichert bleiben. Damit kann man je nachdem grossen Schaden anrichten. Häufig informieren sich Arbeitgeber über Bewerber im Netz. Stell dir vor, sie finden dort unangebrachte Inhalte über dich!

Tipp:
Überlege lieber **dreimal**, was du wirklich ins Netz oder in Chats stellen willst. Frage lieber einmal mehr nach der Meinung der Eltern, auch wenn es peinlich sein könnte. Teilweise erachtest du einen Text, ein Bild oder ein Video als nicht schlimm – für andere wirkt es aber unpassend. Ebenfalls solltest du vorsichtig mit Inhalten von Freunden und Bekannten umgehen. Stelle keine Inhalte ins Netz, wenn du diese Person vorher nicht um Erlaubnis gefragt hast. Auch das ist strafbar.

2.4. Tipps im Überblick

Das Internet hat auch viele Vorteile und es kann dir beim Lernen, Recherchieren usw. nützlich sein. Hier erhältst du einige Tipps, die du beim sicheren Surfen beachten solltest. Natürlich können wir dir keine 100%ige Garantie geben.

- Speichere deine Passwörter (z.B. Mailkonto, etc.) nie auf fremden Computern ab.
- Verwende nur komplizierte Passwörter. Diese sollten aus einer Kombination von grossen und kleinen Buchstaben, Zahlen und Sonderzeichen zusammengesetzt sein.
- Achte darauf, dass dir bei der Eingabe des Passwortes niemand zuschaut. Passwörter sagst du auch keinen weiteren Freunden und Bekannten weiter.
- Hast du dich auf einer Webseite angemeldet, melde dich immer wieder ab (Abmelden, Logout, verlassen usw.).
- Persönliche Daten wie Name, Adresse, Telefonnummer usw. gibst du nur an Personen weiter, die du wirklich kennst.
- Sei misstrauisch beim Angeben deiner persönlichen Daten auf Webseiten. Nicht immer sind diese zwingend erforderlich.
- Registriere dich nur bei sicheren und seriösen Webseiten. Diese erkennst du am Schloss-Symbol in der Adressleiste 

- Klicke nie zu schnell auf einen Link oder auf einen Button. Lies vorher immer alles genau durch.
- Sei misstrauisch bei Mitteilungen wie zum Beispiel «du hast gewonnen» oder weiteren Angeboten. Oft stecken nicht die Firmen dahinter, auch wenn die Dateien oder Webseiten noch so professionell aussehen.
- Lade keine Dateien von unbekannten und unseriösen Seiten herunter. Gefahren verbergen sich oft in diesen Dateien.
- Mails und deren Anhänge von unbekannten fremden Absendern löschst du immer ohne sie zu öffnen.

Wir wünschen dir viel Spass beim Erkunden und Erforschen des Internets!