Global verbunden

Wir leben in einer Zeit, in der Informationen eine enorm wichtige Rolle spielen. Das Internet macht es möglich, dass uns so viele Informationen und Informationsquellen wie niemals zuvor zur Verfügung stehen. Kinder und Jugendliche wachsen heute ganz selbstverständlich mit digitalen Medien auf und beziehen sie in sämtliche Lebensbereiche mit ein. Das World Wide Web wird für Informationsbeschaffung, für die Vernetzung, für Spiele und auch wesentlich für die Kommunikation eingesetzt.

Den Vorteilen und Annehmlichkeiten globaler Vernetzung stehen allerdings auch zahlreiche Gefahrenquellen gegenüber.

Der gläserne Mensch

Viele Menschen unterschätzen, wie schnell und umfassend persönliche Daten im Internet weitergegeben bzw. überall auf der Welt eingesehen werden können. Wenig versierte User wie Kinder oder ältere Menschen gehen häufig zu leichtfertig mit ihren persönlichen Daten um und sind sich der Konsequenzen nicht bewusst.

Social Media

Social Media ist ein Überbegriff für Technologien, die den NutzerInnen die Vernetzung und Kooperation über das Internet ermöglichen. Durch Social Media können sich die UserInnen als Privatpersonen wie auch beruflich miteinander austauschen. Auch die Kommunikation zwischen Unternehmen und deren KundInnen zum Zweck des Marketing oder der Marktforschung wird durch Social Media gefördert.

Die Datenveröffentlichung von Privatpersonen wird z.B. von Personalmanagern genutzt, um Zusatzinformationen über BewerberInnen zu sammeln. Auch AdresshändlerInnen, die Informationen an Firmen für Werbezwecke oder Ähnliches weiterverkaufen, kommen auf diese Weise einfach zu den begehrten Daten.

Personensuchmaschinen

Welches Ausmaß dieser freizügige Umgang mit personenbezogenen Daten bereits angenommen hat, kann in speziellen Personensuchmaschinen nachvollzogen werden. Hier sind zahlreiche Daten von Menschen gesammelt und wer in Social Media besonders aktiv ist, scheint hier auf vielfältige Weise auf.

Attacken aus dem World Wide Web

Neben dem Datenschutz ist die Sicherung des Computers, aber auch der Smartphones und Tablets ein großes Thema geworden. Sobald eine Verbindung zum Internet hergestellt wird, kann es bereits ab den ersten Minuten zu Attacken von Virenprogrammen aus dem Internet kommen. Da sich auf den Geräten viele (private und/oder berufliche) sensible Daten befinden und z.B. Bankgeschäfte oft von zu Hause aus erledigt werden, ist es nötig, Schutzsysteme (z.B. Firewall und Virenschutz) zu installieren und regelmäßig zu aktualisieren. Hinzu kommt, dass sehr viele dieser schädlichen Programme und Viren versuchen, den Zugang über E-Mails zum Computer und zu den darauf befindlichen Daten zu erlangen.

Ein gesundes Misstrauen bewahren

Unterschiedlichste Computerviren und laufend neue Schadprogramme erschweren es, den Überblick zu behalten. So genannte Trojaner werden sehr häufig in Umlauf gebracht. In diesen Fällen tarnt sich das schädliche Computerprogramm als bekannte und vertrauenswürdige Software. Ist sie erst einmal auf das Gerät gelangt, schädigen die im Programm enthaltenen Viren den Computer, dessen Arbeitsleistung oder vernichten Daten. Manche Virenprogramme sind darauf ausgerichtet, den Virenschutz selbst auszuschalten, damit der PC anschließend allen Attacken schutzlos ausgeliefert ist.

Copyright: Alle Rechte vorbehalten.
Die verwendeten Texte, Bilder und Grafiken sowie das Layout dieser Seiten unterliegen weltweitem Urheberrecht. Die unerlaubte Verwendung, Reproduktion oder Weitergabe einzelner Inhalte oder kompletter Seiten ist untersagt. Dies gilt ebenso für die unerlaubte Einbindung einzelner Inhalte oder kompletter Seiten auf Websites anderer BetreiberInnen. Das Einrichten von Links auf diese Website ist jedoch ausdrücklich gestattet.

Aus diesem Grund ist es wichtig, bei unbekannten AbsenderInnen oder verdächtigen Datenanhängen vorsichtig zu sein und diese im Zweifel zu löschen. Besonders Anhänge, die mit dem Kürzel .vbs, .bat, .com, .exe, .pif, .scr oder auch .zip enden, sind mit Vorsicht zu genießen, da diese in der Regel ausführbare Dateien enthalten können.

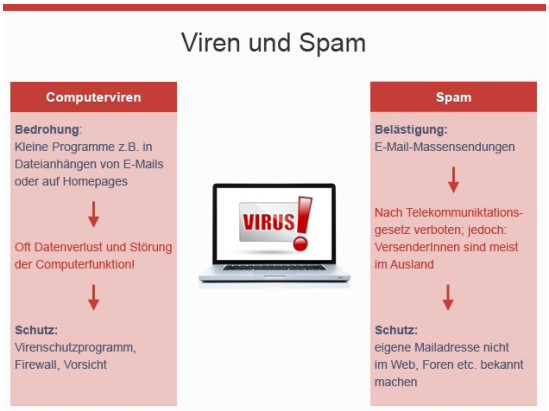

Bild: sozialministerium/fridrich/oegwm

Spam/Junk-Mail – Nutzlose Zusendungen

Ärgerlich und bei zu großem Vertrauen teilweise auch gefährlich sind so genannte Spam- oder Junk-Mails. Diese enthalten oft Werbung für zweifelhafte Produkte, versprechen große Gewinne oder werden als Kettenbriefe versendet. Lästig sind sie, da das Lesen und Aussortieren Zeit kostet, und gefährlich können sie sein, wenn Gewinne oder Geldbeteiligungen angeboten werden und man auf unseriöse Angebote hineinfällt. Jedes Jahr geraten Menschen dadurch in finanzielle Bedrängnis, da sie von BetrügerInnen abgezockt werden.

Im Umgang mit Spam/Junk-Mails ist es wichtig, dass niemals auf diese Art von E-Mails geantwortet wird. Dies würde den Spammern (= SenderInnen von Spams) lediglich bestätigen, dass die Adresse korrekt ist, und so mitunter eine Flut an Spamzusendungen provozieren. Um Spam/Junk-Mails nach Möglichkeit zu verhindern, soll mit der Weitergabe persönlicher Daten zurückhaltend umgegangen werden. Weiters besteht die Möglichkeit, einen Spamfilter einzuschalten, der automatisch bestimmte Zusendungen aussortiert.

Passwörter fischen

Phishing ist ein Kunstwort, das sich aus den beiden englischen Wörtern „password“ und „fishing“ zusammensetzt. Darunter versteht man eine kriminelle Methode, mit der mittels gefälschter Internetseiten oder E-Mails Passwörter und Codes ergaunert werden. Eine häufige Vorgangsweise ist, dass die BetrügerInnen im Namen einer Bank per Mail Sicherheitskontrollen ankündigen und man zur Abklärung die eigenen Kontozugangsdaten übermitteln oder Apps installieren soll.

Wer dieser Aufforderung nachkommt, muss damit rechnen, dass diese Daten dazu verwendet werden, finanziellen Schaden anzurichten. Es ist notwendig zu wissen, dass Banken niemals per Mail zur Installation einer App auffordern oder persönliche Angaben per Mail abfragen, und es ist darauf zu achten, dass die Homepage auch tatsächlich die originale Seite ist (die gefälschten Seiten sehen vielleicht ein bisschen anders aus oder der Name der Internetseite ist nicht genau derselbe). Im Zweifelsfall ist es immer ratsam, Kontakt mit der Bank aufzunehmen und nachzufragen.

Alles nur ein Spiel

Spiele stellen für Kinder und Jugendliche eine wichtige Nutzung des Internets dar. Besondere Vorsicht gilt bei Spielgemeinschaften (so genannten LAN-Partys), da hier die Geräte untereinander verbunden werden und sich so Viren schnell verbreiten können. Grundsätzlich sollten nur legal gekaufte Spiele benutzt werden, da diese sicherstellen, dass neben dem Spielprogramm nicht auch Schadsoftware auf den PC geladen wird.
Bei Online-Spielen wiederum gilt, dass mit der Weitergabe der persönlichen Daten vorsichtig

Copyright: Alle Rechte vorbehalten.
Die verwendeten Texte, Bilder und Grafiken sowie das Layout dieser Seiten unterliegen weltweitem Urheberrecht. Die unerlaubte Verwendung, Reproduktion oder Weitergabe einzelner Inhalte oder kompletter Seiten ist untersagt. Dies gilt ebenso für die unerlaubte Einbindung einzelner Inhalte oder kompletter Seiten auf Websites anderer BetreiberInnen. Das Einrichten von Links auf diese Website ist jedoch ausdrücklich gestattet.

umgegangen und nur auf sicheren und bekannten Seiten gespielt werden soll.

Weitere Gefahren im Internet

Zu den bereits erwähnten Risiken wie Viren, Spams oder dem Diebstahl von persönlichen Daten gibt es noch weitere Risiken, die besonders auf Kinder und Jugendliche abzielen. Um sich davor zu schützen, ist es besonders wichtig, dass bereits die jüngeren NutzerInnen lernen, Inhalte kritisch zu beurteilen und mögliche Gefahren zu erkennen. Dazu gehören vor allem Happy Slapping, Cyber-Mobbing, Extremismus, Fake News und Manipulation, Sexting und Pornografie. Nähere Informationen und Hilfestellungen finden sich z.B. bei www.saferinternet.at.

Internet und Smartphone

Für Kinder und Jugendliche ist vor allem das eigene Smartphone der Einstieg in das World Wide Web. Studien belegen, dass in Deutschland und Österreich so gut wie alle Jugendlichen ab 12 Jahren ein eigenes Smartphone besitzen. (vgl. JIM-Studie 2020, S. 8)

Es ist auch das am häufigsten eingesetzte Gerät zur Internetnutzung. „73 Prozent derjenigen, die zumindest alle 14 Tage das Internet nutzen, nennen das Smartphone als häufigstes Zugangsgerät. Mit deutlichem Abstand folgen mit jeweils zehn Prozent der stationäre Computer und der Laptop. Danach folgen das Tablet mit vier Prozent, die Spielekonsole mit zwei Prozent und der Fernseher mit einem Prozent.“ (JIM-Studie 2020, S. 30)

Gängige Apps wie z.B. YouTube, WhatsApp, Instagram oder Snapchat können ebenfalls programmabhängige Risiken bergen. Auch in Apps finden sich z.B. Inhalte, die für Kinder und Jugendliche nicht geeignet sind. Viele Apps greifen auch auf Dateien oder Programme des Gerätes zu. Diese Einstellungen lassen sich aber in der Regel am Gerät ändern.

10 Gebote der digitalen Ethik

Für ein gutes und gelingendes Leben in der digitalen Gesellschaft wurden an der Hochschule der Medien in Stuttgart Leitlinien formuliert. Diese sollen helfen, die Würde des Einzelnen, seine Selbstbestimmung und Handlungsfreiheit wertzuschätzen:

1. Erzähle und zeige möglichst wenig von dir.
2. Akzeptiere nicht, dass du beobachtet wirst und deine Daten gesammelt werden.
3. Glaube nicht alles, was du online siehst, und informiere dich aus verschiedenen Quellen.
4. Lasse nicht zu, dass jemand verletzt und gemobbt wird.
5. Respektiere die Würde anderer Menschen und bedenke, dass auch online Regeln gelten.
6. Vertraue nicht jedem, mit dem du online Kontakt hast.
7. Schütze dich und andere vor drastischen Inhalten.
8. Miss deinen Wert nicht an Likes und Posts.
9. Bewerte dich und deinen Körper nicht anhand von Zahlen und Statistiken.
10. Schalte hin und wieder ab und gönne dir auch mal eine Auszeit.

www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Jugendliche/ZehnGebote_DigitaleEthik_Infokarte.pdf (2021-06-28)

Regelmäßige und aktuelle Informationen, Tipps und Tricks zu Apps und deren Risiken findet man z.B. unter www.saferinternet.at oder www.klicksafe.de.

Anmerkungen

Copyright: Alle Rechte vorbehalten.
Die verwendeten Texte, Bilder und Grafiken sowie das Layout dieser Seiten unterliegen weltweitem Urheberrecht. Die unerlaubte Verwendung, Reproduktion oder Weitergabe einzelner Inhalte oder kompletter Seiten ist untersagt. Dies gilt ebenso für die unerlaubte Einbindung einzelner Inhalte oder kompletter Seiten auf Websites anderer BetreiberInnen. Das Einrichten von Links auf diese Website ist jedoch ausdrücklich gestattet.