Account

Ein Account ist ein Benutzerkonto und ermöglicht den Zugang zu bestimmten Internetdiensten bzw. allgemein ins Internet. Üblicherweise ist ein Account durch einen Benutzernamen und ein Passwort gesichert. Wenn für den Zugriff auf Benutzerkonten fremde Netzwerke (öffentliches WLAN oder Internetcafes) verwendet und Benutzername oder Kennwort unverschlüsselt übertragen werden, können sie leichter ausspioniert und der Account übernommen werden. Werden bestehende Accounts bei z.B. Google oder Facebook zur Anmeldung auf anderen Webseiten genutzt, ist die dort neu erzeugte Datenspur auch für Google oder Facebook auswertbar.

Altersbegrenzungen bei Computerspielen

Bei Computerspielen sind entsprechende Altersangaben zu finden, welche informieren, ab welchem Alter das Spiel sinnvoll erscheint. Zusätzlich gibt die Bundesstelle für Positivprädikatisierung von Computer- und Konsolenspielen hilfreiche Tipps und Empfehlungen weiter, die bei der passenden Auswahl von Computerspielen helfen. Online zu finden unter: http://bupp.at.

Antivirus-Programme

Virenschutz-Programme haben die Aufgabe, den Computer vor bekannten Viren bzw. Schadsoftware zu schützen. Da ständig neue Varianten in Umlauf gebracht werden, ist es nötig, diese Schutzprogramme immer auf dem neuesten Stand zu halten.

Apps

Unter einer App, der Abkürzung von Applikation, versteht man eine Anwendungssoftware insbesondere für Smartphones und Tablets. Mit dem Einzug der Smartphones hat sich das App-Angebot vervielfacht. Apps werden sowohl kostenfrei als auch kostenpflichtig angeboten. In der Regel finanzieren sich kostenfreie Apps durch Werbeeinschaltungen oder In-App-Käufe. Bei In-App Käufen werden AnwenderInnen meist von Spielen, in denen Guthaben, Punkte oder Zusatzfunktionen gekauft werden können, zu raschem und unüberlegtem Klicken verlockt. Dies kann zu vermehrten und unüberlegten Käufen führen. Unternehmen sind dazu verpflichtet, auf ihrer Website dafür zu sorgen, dass VerbraucherInnen bei Bestellung durch Klick auf eine Schaltfläche ausdrücklich auf die damit verbundene Zahlungsverpflichtung hingewiesen werden. Apps können oft unbemerkt Schadsoftware übertragen. Umfangreiche Zugriffsrechte sowie ungewünschte Übertragung von persönlichen Daten stellen weitere Risiken von Apps dar.

Ballerspiele

Ballerspiele bezeichnen umgangssprachlich Computerspiele, bei denen es darum geht, eine möglichst große Anzahl von Gegnern mit verschiedenen Waffen zu töten. Dass digitale Spiele Kinder und Jugendliche beeinflussen, ist für die Forschung unumstritten. Für die direkte Ausübung von realer Gewalt durch Kinder und Jugendliche scheinen soziale und familiäre Ursachen aber einen größeren Einfluss zu haben als die Nutzung von Gewaltspielen. Jugendschutzsysteme gehen aber von entwicklungsbeeinträchtigenden Wirkungen durch Ballerspiele aus und kennzeichnen deshalb zum Schutz der Kinder und Jugendlichen Spiele mit Gewaltszenen mit Altersempfehlungen.

Bezahlen im Internet

Verschiedene Bezahlsysteme, um online zahlen zu können, sind derzeit möglich und gebräuchlich. So kann z.B. per Kreditkarte, mittels Online-Überweisung oder auch via paybox, paysafecard, PayPal eine Rechnung online beglichen werden. Die Verfahren unterscheiden sich u.a. durch unterschiedlichen Umfang der anzugebenden Daten und unterschiedliche Sicherheitsstufen.

Biometrie

Biometrische Verfahren nutzen messbare, individuelle Merkmale zum Zweck der Identifikation einer Person. Diese Verfahren werden u. a. bei Zugriffsberechtigungsprüfungen zum PC, Eintrittskontrollen oder bei der bargeldlosen Zahlungsmöglichkeit eingesetzt. Die biometrischen Verfahren (Gesichtserkennung, Fingerabdruck, Iriserkennung, ...) haben Vor- und Nachteile bezogen auf Erkennungsleistung, Praxistauglichkeit, Fehleranfälligkeit und Überwindungssicherheit. Bei Tests wurde eine Reihe von Mängeln (Überwindungssicherheit, Rate der Falscherkennung) erkannt, die nicht nur unter Datenschutzgesichtspunkten kritisch zu beurteilen sind, sondern auch im Hinblick auf die häufig geforderte (erwartete) Sicherheit.

Blog

Blog ist die Abkürzung für Weblog. Weblog setzt sich zusammen aus den Worten Web (Netz), womit das Internet als Ganzes gemeint ist, und Log, welches von Logbuch (= Journal oder Tagebuch) abgeleitet wird. Somit ist ein Blog ein Journal oder Tagebuch, das im Internet geführt wird und für eine bestimmte Gruppe von Menschen oder für alle sichtbar ist. Einmal im Internet veröffentlichte Daten lassen sich in der Regel nicht mehr vollständig löschen.

Browser

Das Wort Browser kommt vom Englischen „to browse“ und heißt „blättern“. Ein Browser ist ein Computerprogramm, welches für das Aufrufen von Internetseiten benötigt wird. Der Browser ist ein idealer Angriffsort für das Auslesen von Daten. Die meisten Webseiten enthalten Elemente (z.B. Cookies), die Daten sammeln und das Verhalten der User im Internet „aufzeichnen“.

Browser-Sicherheit

Es gibt Programme, die vor potentiell gefährlichen Seiten im Internet warnen. Dazu zählt beispielsweise das Safe Browsing Tool WOT (= Web of Trust), welches in verschiedene Browser integriert werden kann. Allerdings stehen manche Save Browsing Tools aufgrund ihres Umgangs mit personenbezogenen Daten und dem Handel damit auch in der Kritik.

Cloud

Mit Cloud oder Cloud Computing wird eine IT-Infrastruktur bezeichnet, die als Dienstleistung über das Internet zur Verfügung gestellt wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware. Risiken bestehen zum einen bezüglich der Datensicherheit: Zum Beispiel das Risiko bei Übertragung der Daten vom lokalen Rechner auf den entfernten Server, die Möglichkeit von Zugriffen von Cloud-Anbietern auf die eigenen Daten oder die Kontrolle von privaten Anwenderdaten durch marktdominierende Anbieter. Zum anderen besteht bei Cloud basierten Programmen eine physische Abhängigkeit zum Lizenzgeber bzw. Cloudbetreiber. Dadurch können Zugangsberechtigungen relativ einfach beendet oder der Nachkauf von Lizenzen gefordert werden. Darüber hinaus besteht beim Schließen von Cloud-Diensten das Risiko eines Datenverlustes.

Computerspiele

Spiele am Computer können sowohl online, also im Internet, als auch offline, d.h. am PC, aber ohne Internet geschehen. Speziell Online-Glücksspiele bergen neben dem Suchtrisiko das Risiko des Verlustes von Geld sowie fehlende Möglichkeiten zum Spieler- und Jugendschutz.

Cookies

Bei jeder online Computernutzung werden kleine Dateien (Cookies) gespeichert, die für den Austausch zwischen Internet und einzelnen Programmen benötigt werden. Die einzelnen Cookies haben unterschiedliche Aufgaben: Manche sind für die reibungslose Funktion einer Webseite erforderlich, andere, um das Nutzerverhalten zu dokumentieren, Videos ablaufen zu lassen

oder Werbung zu schalten. Seit In Kraft Treten der DSGVO haben NutzerInnen die Möglichkeit, Cookies im Einzelnen zuzustimmen.

Cyber-Grooming

Als Cyber-Grooming bezeichnet man die Anbahnung sexueller Kontakte über digitale Medien. (Überwiegend männliche) Erwachsene erschleichen sich dabei das Vertrauen von Minderjährigen, um sie sexuell zu belästigen. Der Kontakt beginnt meist harmlos. Groomer geben sich dabei häufig als Gleichaltrige aus, oder sie tarnen sich als Modelagenten, Talentsucher oder professionelle Gamer, die den Jugendlichen angeblich zu mehr Erfolg verhelfen. Besonders gefährdet sind dabei Kinder, die in ihrem sozialen Leben wenig Rückhalt erfahren.

Cyber-Mobbing

Darunter versteht man das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen einer anderen Person über digitale Medien. Das können Chats, Messenger-Dienste wie WhatsApp, E-Mails, Fotos und Videos in sozialen Netzwerken o.ä. sein. In der Regel gehen die Attacken von Personen aus dem persönlichen Umfeld aus, erreichen aber im Internet schnell ein großes Publikum. Cyber-Mobbing findet dort statt, wo digitale Medien genutzt werden: also rund um die Uhr und auch zu Hause. Durch die scheinbare Anonymität der Täter sinkt die Hemmschwelle. Wobei die Opfer/Täterrollen häufig nicht eindeutig sind, da Attacken als Gegenattacken wiederkehren können.

Datenschutz

Laut Datenschutzgesetz haben alle Menschen das Recht auf Privatsphäre und dürfen somit selbst bestimmen, welche persönlichen Daten (z.B. Name, Geburtsdatum, Wohnort, Ausbildung …) weitergegeben werden. Auch im Internet ist darauf zu achten, dass mit den persönlichen Daten sorgsam umgegangen wird, da diese weltweit gefunden und benutzt werden können. Besonders die große Beliebtheit von Social Media (Facebook, Twitter ...) hat in den letzten Jahren zu zahlreichen ungewollten Veröffentlichungen privater Daten geführt. Auf der Website der österreichischen Datenschutzbehörde unter www.dsb.gv.at gibt es zum Thema Datenschutz zahlreiche weiterführende Informationen.

Datenschutz-Grundverordnung

Mit der Datenschutz-Grundverordnung (DSGVO), die mit 25. Mai 2018 in Kraft getreten ist, wird ein einheitliches Datenschutzrecht für alle EU-Mitgliedstaaten geschaffen. Die EU-Verordnung ist grundsätzlich unmittelbar anwendbar. Da aber den Mitgliedstaaten in einzelnen Punkten ein gewisser Regelungsspielraum eingeräumt wird und auch die nationale Zuständigkeit der Behörden festzulegen ist, werden Ergänzungen zu den generellen Bestimmungen der DSGVO mit dem „Datenschutz-Anpassungsgesetz 2018“ geregelt.

Dateiendungen

Es gibt verschiedene Dateiendungen, die festlegen, mit welchem Programm eine Datei geöffnet werden kann. Dadurch erfährt man auch, mit welchem Programm die Datei erstellt wurde. Beispiele: jpg – hierbei handelt es sich um eine Bilddatei, gif – weitere/andere Bilddatei, xls/xlsx – Excel-Dateien, doc/docx – Worddateien, mpg – Videodateien, pdf ein Format von Adobe zur Erleichterung im Datenaustausch, ppt/pps – Powerpointdatei für Präsentationen, u.v.m. Bei Dateiendungen wie z.B. exe ist Vorsicht geboten: Exe steht für executable und bedeutet „ausführbares Programm“. Es besteht die Möglichkeit, dass es Schadsoftware enthält. Ohne Kontrolle durch einen Virenscanner sollen solche Dateien nicht geöffnet werden.

Digitaler Fingerabdruck

Wer Dienstleistungen aus dem Internet nützt, hinterlässt einen sogenannten digitalen Fingerabdruck. Damit ist es möglich, Personen zu

identifizieren und gegebenenfalls bei erneuter Nutzung eines Dienstes wiederzuerkennen. Die dazu eingesetzten Methoden sind das Internet-Protokoll, verschiedene Ausprägungen von Cookies, die historischen Daten in Browsern oder sogenanntes Canvas-Fingerprinting. Canvas Elemente sind auf Webseiten sichtbare oder unsichtbare Elemente. Diese werden abhängig von verschiedensten Elementen (Browsereinstellungen, eingesetzte Hardware, Konfigurationen, etc.) über den Browser interpretiert und ermöglichen die eindeutige Identifikation von Personen.

E-Mail

E-Mails gelten in der weltweiten schriftlichen Kommunikation als Standard. Herkömmliche E-Mails sind in der Regel nicht verschlüsselt und verfügen damit – vergleichbar mit einer Postkarte – über einen sehr geringen Sicherheitsstandard.
Anbieter kostenfreier E-Mail-Adressen wie z.b. web.de, gmail oder gmx finanzieren sich über Werbung und bieten oft wenig Datenschutz. Durch kostenpflichtige und werbefreie Accounts lässt sich die Privatsphäre erhöhen.

Fake

Im Medienkontext werden Fälschungen als Fake bezeichnet. Mit Fake-Shops (gefälschte Webshops) werden Onlineshops bezeichnet, die erstellt wurden, um zu betrügen. In der Regel wird eine Zahlung mittels Vorkasse gefordert, die bestellte Ware wird jedoch nie geliefert. Fake News verbreiten Falsch- oder Fehlinformationen. Fake Videos verwenden z.B. reale Gesichter und erstellen mit Hilfe von selbstlernenden Algorithmen Fälschungen, auch deepfakes genannt, die als solche kaum oder nicht mehr zu erkennen sind. Neben dem Erhaschen von Aufmerksamkeit werden mit diesen Aktivitäten auch handfeste Geschäftsinteressen verfolgt sowie politischer und gesellschaftlicher Einfluss genommen.

Firewall

Übersetzt aus dem Englischen bedeutet Firewall Brandschutzmauer. Im technischen Bereich wird damit ein dem PC vorgelagertes Sicherheitssystem bezeichnet, das den laufenden Datenverkehr überwacht und so z.B. Eindringversuche von Computerviren vereiteln kann. Es ist wichtig, die Firewall regelmäßig auf den neuesten Stand zu bringen, da ständig neue Schadsoftware entwickelt wird. Firewalls gibt es als Softwarelösung oder sie ist hardware-seitig, z.b. im Internetrouter, eingebaut.

Forum

Als Forum wird eine Diskussionsmöglichkeit im Internet bezeichnet. Dabei erscheinen die einzelnen Gesprächsbeiträge auf einer Website, auf die andere TeilnehmerInnen reagieren können. Mitunter ist die Teilnahme nur für registrierte BenutzerInnen möglich und durch Passwörter geschützt. Neben dem Risiko durch Schadsoftware sollte man sich bei der Beteiligung an Foren bewusst sein, dass Aussagen auch strafbar sein können. In manchen Foren werden überhaupt illegale Themen abgehandelt. Darüber hinaus können Verabredungen mit Menschen, die man nur aus dem Internet kennt, heikel sein.

Happy Slapping

Happy Slapping bedeutet übersetzt „lustiges Draufschlagen“. Bei den auch als „Smack Cam“ oder „Slap Cam“ genannten Gewaltvideos filmen sich Jugendliche dabei, wie sie andere schlagen, und stellen diesen Clip dann ins Internet. Diese Videos, in denen sich neben gestellten Szenen auch reale Gewalttaten finden, erzielen in den sozialen Netzwerken hohe Aufmerksamkeit. Unter Jugendlichen sind sie beliebtes Tauschgut und sie überbieten sich darin, wer ärgere Szenen am Handy hat.
Das Versenden von gewaltverherrlichenden Bildern oder Videos an Minderjährige kann aber ebenso strafbar sein wie die Verletzung des Rechts am eigenen Bild. Die Aktionen werden

von den Tätern z.T. unterschätzt. Sie können Straftaten wie Körperverletzung oder Nötigung entsprechen.

Hoax

Hoax ist der englische Begriff für Scherz oder Jux und wird für Falschmeldungen verwendet, die bewusst verbreitet werden. Da diese Meldungen meist für wahr gehalten werden, werden sie in großer Zahl per E-Mail, Handy oder anderen Kommunikationsformen an Bekannte, Freunde und Verwandte weitergeleitet (Spam-Mail). Beispiele: Sowohl Nachrichten, die angeben, dass beim Weiterleiten der E-Mail ein bestimmter Betrag für einen karitativen Zweck gesammelt wird, als auch absichtlich veröffentlichte Falschmeldungen über bestimmte Menschengruppen, Aprilscherze oder Kettenbriefe, die Glück o.ä. versprechen, fallen in die Kategorie eines Hoax.

Influencer

Als Influencer (engl. to influence = beeinflussen) werden Personen bezeichnet, die Inhalte zu verschiedenen Themengebieten in sozialen Netzwerken veröffentlichen und damit eine Interaktion mit den ZuseherInnen hervorrufen. Aufgrund des hohen Ansehens und ihrer Präsenz im Web werden Influencer auch als Werbeträger herangezogen (= Influencer-Marketing).

Junk-Mail

Junk-Mail ist ein weiterer Begriff für Spam-Mails. Die Bezeichnung „Junk“ kommt aus dem Englischen und bedeutet so viel wie „wertloser Mist“.

Kleinanzeigenbetrug

Bei der Kaufabwicklung von (privaten) Waren ist Vorsicht geboten: Kriminelle erstellen Kleinanzeigen, um KäuferInnen abzuzocken. Für den Austausch von Geld und Ware wird ein fiktives Unternehmen als Treuhänder ins Spiel gebracht. Als Begründung wird z.B. ein Wohnsitz im Ausland genannt. Deshalb soll das Treuhandunternehmen Geld und Ware erhalten und, wenn beides eingelangt ist, den Vertragsparteien Ware und Geld weiterleiten. Die BetrügerInnen erhalten so das Geld oder die Ware ohne Gegenleistung. Erkennbar ist dieser Betrug u.a. auch durch auffällig günstige oder teure Ware.

Markenfälschung

Besonders günstige Markenware ist meist gefälscht. Wer die Ware bestellt, erhält zum Teil mangelhafte und/oder nicht zu gebrauchende Produkte. Die gefälschte Ware kann auch vom Zoll beschlagnahmt werden. KäuferInnen drohen hohe Zusatzkosten und rechtliche Konsequenzen. Hinweise auf Markenfälscher sind hohe Rabatte, Produkte, die in anderen Geschäften vergriffen sind, negative Kundenkritiken, fehlende Angaben zum Webseitenbetreiber, schlecht ins Deutsche übersetzte Texte und unverschlüsselte Internetverbindungen (http:// anstelle von https://).

Messengerdienste

Mit Hilfe von Apps kann mit den darin gespeicherten Kontakten kommuniziert werden. Wird diese Kommunikation nicht verschlüsselt, kann sie leicht ausspioniert werden. Über Messengerdienste werden auch private Daten geteilt bzw. veröffentlicht. Diese können auch für kriminelle Zwecke wie Phishing oder Stalking genutzt werden.

Onlinebanking

„Online“ bezeichnet die aktuelle Verbindung zum Internet und der Begriff Onlinebanking wird somit für alle Bankgeschäfte verwendet, die über das Internet abgewickelt werden. Andere Begriffe hierfür sind E-Banking oder Homebanking. Zur Bestätigung von Überweisungen werden sogenannte TANs (Transaktionsnummern) verwendet. Diese dienen ausschließlich der Unterzeichnung von Aufträgen; beim Anmeldevorgang sind sie niemals erforderlich. Onlinebanking gilt als sicher, wenn einige Grundregeln eingehalten

werden. Dazu gehören unter anderem das Geheimhalten von Zugangsdaten, die Verwendung sicherer Netzwerke und die Anwendung auf eigenen Geräten.

Online-Shopping

Shopping ist der englische Begriff für Einkaufen. Mit Online-Shopping ist also das Einkaufen im Internet gemeint. Dies kann mit dem Bestellen von Waren aus einem Katalog verglichen werden, wobei die Geschäftsbedingungen für Online-Käufe zu berücksichtigen sind. Neben dem Sofortkauf gibt es auch die Möglichkeit von Versteigerungen. Folgende Grafik gibt einen kurzen Vergleich von Online-Shopping mit Internet-Versteigerungen:

Bild: sozialministerium/fridrich/oegwm

Einige Online-Marktplätze bieten neben dem Einkauf bei Gewerbetreibenden auch Möglichkeiten zum Handel unter VerbraucherInnen. Trotz etablierter Schutzmaßnahmen wie z.B. einem 14-tägigen Rückgaberecht bestehen für die KonsumentInnen Risiken wie z.B. Fake-Shops. Darüber hinaus kommen durch Konzernstrukturen globaler Onlineshops regionale Händler stark unter Druck, soziale Errungenschaften werden häufig ausgehebelt und durch die Zunahme von Transportwegen entstehen ökologische Belastungen.

Passwort

Ein Passwort ist ein Code, der bestimmte Bereiche auf dem PC oder im Internet vor fremden Zugriffen schützt. Passwörter verhindern z.B., dass sich jemand, der nur den Usernamen einer anderen Person kennt, sich bei dessen Konto anmeldet und so etwa E-Mails lesen bzw. schreiben oder Geschäfte unter falschem Namen abschließen kann. Es ist wichtig, Passwörter geheim zu halten. Auf keinen Fall sollten reale Namen oder Begriffe, die in Wörterbüchern zu finden sind, als Passwort verwendet werden. Passwörter gelten dann als relativ sicher, wenn sie aus einer Kombination von verschiedenen Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen bestehen. Eine Mindestlänge von acht Zeichen ist sinnvoll, zwölf oder 16 Zeichen erhöhen die Sicherheit deutlich. Passwörter sollten nicht mehrfach verwendet werden. Auf der Website www.passwortcheck.ch/passwortcheck/passwortcheck können Passwörter einem Sicherheitscheck unterzogen werden.

Phishingmails

Der Begriff Phishing setzt sich aus „Password" und „Fishing" zusammen und bezeichnet damit eine Betrugspraktik, bei der per E-Mail versucht wird, durch arglistige Täuschung Passwörter und Codes abzufragen. In den meisten Fällen zielen Phishingmails darauf ab, Bankverbindungen auszuspionieren und somit finanziellen Schaden anzurichten.

Sexting

Kombination aus „sex" und „texting". Damit ist das Verschicken von Bildern und Videos mit erotischen Selbstaufnahmen über Handy bzw. Internet gemeint. Die Gefahr ist, dass solche Inhalte sich über das Internet schnell verbreiten und nur schwer gelöscht werden können.

Social Media

In den letzten Jahren hat sich die Nutzung des

Internets immer mehr verändert. Besonderer Beliebtheit erfreuen sich dabei Social Media, die es ermöglichen, einfach und schnell Inhalte ins Internet zu stellen. Die NutzerInnen legen ein eigenes Profil mit persönlichen Angaben wie beispielsweise zu Interessen, Hobbys u. ä. an. Beispiele: Facebook, Twitter, Instagram, Snapchat. Neben den Risiken durch bzw. über die Software (Phishing, Schadsoftware, Hacken von Profilen) sind durch Social Media auch Cyberformen von Mobbing oder Stalking entstanden. Darüber hinaus ist es riskant, Unbekannte in das eigene Netzwerk aufzunehmen, da diesen manchmal auch Zugriff auf persönliche Informationen und Kontakte gewährt wird.

Spam-Mail

Spam-Mail ist die Bezeichnung für E-Mails, die wahllos an möglichst viele Menschen geschickt werden. Ständige Spam-Attacken verringern nicht nur die Arbeitsleistung des Computers; zum Teil enthalten diese auch Schadsoftware, die zusätzlich Schaden anrichtet. Als Spam können z.B. auch unnütze massenhafte Beiträge in einem Forum bezeichnet werden. Im ursprünglichen Sprachgebrauch ist Spam der englische Ausdruck für Dosenfleisch, das als unnützes und ungewolltes Produkt verstanden wird.

Spyware

Spyware setzt sich zusammen aus „spy“, was übersetzt „ausspionieren“ heißt, und „ware“ (Ware oder Programm). Damit sind Computerprogramme gemeint, die bestimmte Daten wie z.B. Passwörter und Codes ausspionieren wollen. In der Regel handelt es sich dabei um Passwörter und Codes. Es ist auch möglich, dass die Spyware über einen Trojaner auf einen Computer gelangt, sich dann auf dem PC selbstständig macht und gewisse Daten an Fremde weiterleitet.

Suchmaschine

Suchmaschinen sind spezielle Webangebote, die dabei helfen, das Internet gezielt nach bestimmten Inhalten zu durchsuchen. Die Rangordnung der Ergebnisse wird vom Suchmaschinenbetreiber festgelegt. Webseiten können für das Auffinden von bestimmten Inhalten durch Suchmaschinen optimiert werden. Bekannte Suchmaschinen sind z.B. Google, Yahoo oder bing. Diese Suchmaschinen sammeln zusätzlich auch Daten über NutzerInnen (etwa Speichern der IP-Adresse oder des Suchverhaltens), um ein möglichst genaues Benutzerprofil erstellen zu können. Eine Alternative stellen sogenannte anonyme Suchmaschinen wie z.B. StartPage dar.

Trojaner

Trojaner sind Programme, die sich als bekannte bzw. vertrauenswürdige Programme tarnen und dabei im Hintergrund Schaden auf dem PC anrichten können. Die schädlichen Computerprogramme laufen oft heimlich und ohne Wissen der betroffenen Person. Anhänge von E-Mails können Trojaner enthalten und sollten deshalb keinesfalls geöffnet werden, wenn der Absender oder die Dateiendung unbekannt ist.

Update

Update ist die englische Bezeichnung für die Aktualisierung von Betriebssystemen, Antivirensoftware und Computerprogrammen. Regelmäßige Updates sind besonders wichtig, um sich wirksam gegen Schadprogramme und Viren zu schützen.

Virus

Im Computerbereich versteht man unter einem Virus ein Computerprogramm, welches das Ziel hat, Schaden auf dem jeweiligen PC oder im Netzwerk anzurichten oder diesen als Wirt für weitere Attacken zu nutzen. Es gibt zahlreiche, unterschiedlich arbeitende Computerviren.

Wurm

Ein Wurm ist eine bestimmte Art von Schadsoftware. Diesen zeichnet aus, dass er sich ohne weiteres Zutun eines Users von einem Computer

auf den nächsten fortpflanzen und verschiedene Programme auf dem PC schädigen kann. Wird der Virenschutz deaktiviert, ist der Computer schutzlos gegenüber verschiedensten Angriffen.

Zwei-Faktor-Authentifizierung

Für den erhöhten Schutz eines Benutzerkontos wird zusätzlich zum Passwort eine weitere Sicherheitskomponente verlangt, für die ein eigener Übertragungskanal verwendet wird. Bei Zahlungsvorgängen im Internet ist dieser Vorgang verpflichtend, er wird aber auch von Behörden mittels Handysignatur oder Bürgerkarte oder von großen Internetdiensten eingesetzt. Für die zweite Sicherheitskomponente gibt es verschiedene Methoden: SMS-Code an eine hinterlegte Handynummer, automatisch generierter Sprachanruf an eine hinterlegte Handynummer, Sicherheitscode über eine Codegenerator-App, E-Mail an eine hinterlegte E-Mail-Adresse, physischer Sicherheitsschlüssel wie z.B. ein USB-Stick, Sicherheitscodes zum Ausdrucken, etc. Mit dieser Methode besteht aber auch die Gefahr, sich vom eigenen Konto auszusperren. Verwendet man z.B. eine Codegenerator-App und muss diese bei einem Handywechsel neu installieren, hat man danach keine Verknüpfung mehr zu Online-Plattformen und kann deshalb keine Bestätigungscodes mehr erzeugen. Deshalb wird empfohlen, wo möglich, mehrere Methoden zur Zwei-Faktor-Authentifizierung anzuwenden bzw. Codes auch auszudrucken.

Anmerkungen