Adware	Adware (zusammengesetzt aus ***ad***vertisement (Werbung) und Soft***ware***) ist Software, die zu Werbezwecken eingesetzt wird. Oft wird Adware unabsichtlich installiert: Bei vielen kostenlosen Programmen muss die zusätzliche Installation von Adware ausdrücklich abgewählt werden.
Antiviren-Programme	Antiviren-Programme prüfen im Hintergrund alle laufenden Aktivitäten, spüren Computerviren (z.b. Würmer, Trojaner) auf und blockieren oder löschen sie. Verdächtige Dateien können in Quarantäne verschoben und so unschädlich gemacht werden.
Appstore	Apps aus nicht offiziellen Appstores bergen große Risiken: mobile Malware, unnötiger Ressourcenverbrauch, Zugriff auf persönliche Daten, schlechte Qualität, versteckte Kosten. Auch sollte bei Apps aus offiziellen Appstores überprüft werden, ob der Zugriff auf Kontaktdaten, Standortverlauf, Bilder etc. notwendig ist. Eventuell auf das App verzichten.
Attachment	Attachments sind E-Mail-Anhänge. Da Attachments Malware enthalten können, sollte man Anhänge von unbekannten Absendern nicht öffnen.
Auskunftwerber	Das Datenschutzgesetz räumt jedem, dessen Daten verwendet werden, ein Auskunftsrecht über alle zu seiner Person verarbeiteten Daten ein. Die Auskunft verlangende Person wird Auskunftwerber genannt.
Auftraggeber	Unter einem Auftraggeber (im Sinne des Datenschutzgesetzes) versteht man eine Person oder Organisation, die personenbezogenen Daten speichert. Der Auftraggeber muss dem Auskunftwerber Auskunft über die gespeicherten Daten geben.
Authentifizierung	Die Authentifizierung stellt die Identität eines Benutzers sicher. Dies kann z.B. mit Benutzerkennung und Passwort oder einer PIN oder auch per Fingerabdruck erfolgen.
Backdoor	Ein Backdoorprogramm erlaubt es Dritten, einen PC fernzusteuern und auch für kriminelle Zwecke zu verwenden. Backdoorprogramme sind Malware.
Backup	Ein Backup ist eine Datensicherung. Backups sollen regelmäßig erstellt und sicher aufbewahrt werden: z.B. in einem Tresor, in einem anderen Gebäude, auf entfernten Rechnern oder in der Cloud.
Benutzerkonto bzw. Netzwerkkonto	Wird z. B. in einer Familie ein Computer genutzt, sollte für jedes Familienmitglied ein Benutzerkonto eingerichtet werden. So kann jeder Benutzer eigene Einstellungen vornehmen und hat einen von anderen Benutzern getrennten Dateispeicherplatz. Bei der Anmeldung muss sich der Benutzer authentifizieren. **Sicherheitstipp**: Wird der Computer nicht mehr verwendet, sollte man sich abmelden.

Biometrische Verfahren	Biometrische Verfahren werden zur Authentifizierung verwendet: Die Identität eines Benutzers wird durch Gesichtserkennung, Fingerabdruck, Augenhintergrund festgestellt. Biometrische Verfahren ersetzen oder ergänzen in manchen Fällen die Authentifizierung durch Passwörter.
Botnet	Bots sind automatisierte Computerprogramme, die infizierte Computer zu einer Gruppe (Botnet) zusammenschließen. Die Betreiber von Botnets missbrauchen die Computer z.B. für den Versand von Spam- oder Phishingmails.
Cloudspeicher	Das Sichern von Backups auf einen Cloudspeicher haben den Vorteil, dass die Daten zusätzlich an einem anderen Ort aufbewahrt werden, denkt man z. B. an einen Brand oder Hochwasser.
Cloud-Computing	Unternehmen setzen bei Teilen der IT-Infrastruktur auf die Cloud. Dies hat große Vorteile, birgt aber auch Gefahren, da eventuell unbefugte Personen Zugriff auf die Daten erlangen können. Die vollständige Kontrolle über die Daten ist nicht möglich.
Computerviren	Computerviren sind unerwünschte Programme, welche sich in Computerprogramme einschleusen. Durch den Aufruf eines Programms, das ein Virus infiziert hat, wird dieser aktiv und kann sich weiterverbreiten.
Computerwurm	Malware, die sich selbständig über Netze (Internet) verbreitet. Ein Computerwurm nützt sehr oft Sicherheitslücken zum Eindringen in ein System.
Cracker	Cracker (vom englischen crack für „knacken“ oder „[ein]brechen“) umgehen oder brechen Zugriffsbarrieren von Computersystemen und Rechnernetzen. Cracker tun dies aus Böswilligkeit oder für Profit.
Cross Site Scripting-Angriffe	*Übersetzt*: Webseitenübergreifende Scripting-Angriffe. Infizierte Webseiten nützen Sicherheitslücken aus. *Beispiel: die Webseite einer Zeitung infiziert unabsichtlich durch Werbeanzeigen, die automatisch von Werbeanbietern bezogen wird, die Rechner der Besucher.*
Cybercrime	Computerkriminalität bzw. Internetkriminalität
Cyber-Grooming	Gezieltes Ansprechen von Minderjährigen im Internet mit dem Ziel der Anbahnung sexueller Kontakte.
Cyber-Mobbing	Mobbing mit Hilfe von elektronischen Medien: Verbreitung von Unwahrheiten bzw. von bloßstellenden Fotos in sozialen Netzwerken.
Cookies	Cookies sind kleine Textdateien, die Informationen über besuchte Webseiten beinhalten und auf dem PC des Benutzers abspeichert sind. Onlineshops wie Amazon verwenden z.B. Cookies, um Benutzer wiederzuerkennen und den Inhalt des Warenkorbs bei einem wiederholten Besuch wiederherzustellen.

Dateierweiterung	Die Dateierweiterung ist der letzte Teil eines Dateinamens und wird mit einem Punkt abgetrennt. Das Betriebssystem erkennt an der Dateierweiterung das Format einer Datei und kann sie mit einem passenden Programm öffnen. *Dateien mit Erweiterungen wie exe, bat, js, scr oder komprimierte Ordner (Dateierweiterung z.B. zip, rar) können Malware enthalten.*
Daten sicher vernichten	Um Daten sicher zu vernichten, können Datenträger überschrieben, geschreddert (zerstört) oder entmagnetisiert werden.
Datenschutzgesetz	Wichtige Punkte des österreichische Datenschutzgesetzes: • Unternehmen müssen für personenbezogene Daten eine DVR-Nummer haben und auf Schriftstücken angeben, damit die Herkunft der Daten nachvollzogen werden kann. • jede Person kann Einsicht in ihre gespeicherten Daten nehmen und die Richtigstellung von falschen Daten verlangen. • Unternehmen dürfen nur Daten erfassen, die für den Zweck des Unternehmens notwendig sind.
Ablaufplan zur Datensicherung	Unternehmen sollen für die Sicherung ihrer Daten eine Ablaufplanung erstellen. Darin ist unter anderem beschrieben, wann welche Daten wohin gesichert werden und wie im Schadensfall die Daten wiederhergestellt werden können.
Datensicherheit	Die sichere Verarbeitung, Speicherung und Kommunikation der Informationen sollen durch ***Vertraulichkeit***, ***Verfügbarkeit*** und ***Integrität*** gewährleistet werden.
Datenvernichtung	Bei der Entsorgung von Computern oder mobilen Geräten sollten die Daten endgültig gelöscht werden. Festplatten können geschreddert (zerkleinert) werden, entmagnetisiert oder mit einer Software so bearbeitet werden, dass die Daten zu 100 % gelöscht sind. Daten, die nur im Explorer zu gelöscht wurden, können oft wiederhergestellt werden. Auch das Zurücksetzen eines Smartphones könnte zu wenig sein.
Dialer	Dialer-Programme wählen unbemerkt über das Telefonnetz kostenpflichtige Mehrwertnummern und verursachen dadurch finanziellen Schaden.
Digitale Signatur	Eine digitale Signatur stellt sicher, dass eine E-Mail vom angegebenen Absender stammt und bei der Übertragung nicht verändert wurde.

Digitales Zertifikat	Eine digitales Zertifikat kann man als digitalen Ausweis verstehen, ~~Ein Digitales Zertifikat ist ein digitaler Datensatz~~, der bestimmte Eigenschaften von Personen oder Objekten bestätigt. Digitale Zertifikate werden von unabhängigen Zertifizierungsstellen ausgegeben. Auf Webseiten von Banken kann man sich das Zertifikat mit einem Klick auf das Schlosssymbol anzeigen lassen. Es bestätigt, dass man sich wirklich auf der Webseite der Bank befindet. *Probiere selber: Öffne die Webseite zum Login einer Bank und kontrolliere mit einem Klick auf das Schlüsselsymbol das Zertifikat.*
Dumpster Diving	Der Müll des Opfers wird durchwühlt und nach Hinweisen und Anhaltspunkten über das persönliche Umfeld des Opfers gesucht. Diese Informationen können bei einem darauf folgenden Anruf dazu verwendet werden, das Vertrauen des Opfers zu erschleichen.
DVR-Nummer	Datenverarbeitungsregister-Nummer, damit die Herkunft von Daten nachvollzogen werden kann. *Auch auf Schulzeugnissen ist eine DVR-Nummer angegeben.*
E-Mail	E-Mails können verschlüsselt werden. Erst beim Empfänger wird das E-Mail wieder entschlüsselt und kann gelesen werden.
Ethisches Hacking	Sicherheitsexperten überprüfen Computersysteme auf Sicherheitslücken, indem sie versuchen in das System einzubrechen. Falls dies gelingt, muss die Sicherheit des Netzwerkes verbessert werden.
Firewall	Eine Firewall ist eine Software, die auf dem zu schützenden Rechner installiert ist. Sie bietet einen Schutz vor Angriffen von Rechnern von außen. Alle aktuellen Betriebssysteme haben eine Firewall, die standardmäßig aktiviert ist. Größere Netzwerke werden zusätzlich durch eine Hardware-Firewall geschützt.
Hacker	Hacker dringen in Computersysteme ein, um damit Missstände und Sicherheitslücken aufzeigen wollen. Sie beschäftigen sich mit Sicherheitsmechanismen und deren Schwachstellen. In Massenmedien und in der Öffentlichkeit werden auch Personen, die unerlaubt in fremde Systeme eindringen und Sicherheitslücken ausnutzen als Hacker bezeichnet obwohl dafür der Begriff Cracker besser geeignet wäre.
Höhere Gewalt	Daten können durch höhere Gewalt bedroht werden. Zu höherer Gewalt zählen z. B. Feuer, Hochwasser, Krieg und Erdbeben.
Hijacking	Beim Browser-Hijacking können Einstellungen des Internet Explorers (IE) so verändert werden, dass der Browser beim Start unerwünschte Seiten anzeigt und eingegebene Adressen auf falsche Seiten umleitet. Besonders gefährlich ist es, wenn auf eine gefälschte Bankseite umgeleitet wird.

Identitätsdiebstahl	Als Identitätsdiebstahl bzw. Identitätsmissbrauch wird die missbräuchliche Verwendung personenbezogener Daten bezeichnet. Meist wird ein Identitäts-diebstahl benutzt, um sich betrügerisch zu bereichern. *Beispiel: Ein Betrüger verkauft über eBay mit fremden Anmeldedaten. Die Käufer zahlen und erhalten keine Ware.*
Information Diving	Entwendung von Daten, die unachtsam weggeworfen wurden. In Altpapiercontainern oder auf Festplatten von ausgemusterten Rechnern befinden sich manchmal Daten, die missbraucht werden können. *Maßnahmen gegen Information Diving: Aktenvernichter verwenden, Daten-träger vor dem Wegwerfen sicher löschen*
Inkompatibilität von Software	Veraltete Software (z. B. Windows XP) kann zu neuen Programmen (z. B. Microsoft Office 2016) inkompatibel sein, dass heißt, dass diese Programme nicht funktionieren. Zusätzlich stellt veraltete Software ein Sicherheitsproblem durch Malware für den Computer dar.
Instant Messaging (IM) = Chat	Instant Messaging *(deutsch: sofortige Nachrichtenübermittlung)* ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Text-nachrichten in Echtzeit unterhalten (Chatten). Mittels IM können auch Dateien übermittelt werden. *Achtung: Keine Dateien von unbekannten Personen annehmen, da diese **Malware** enthalten können.*
Integrität von Daten	Begriff zur Datensicherheit: Daten enthalten den ***korrekten Inhalt***, stehen ***voll-ständig*** zur Verfügung und ***wurden nicht unbefugt verändert.***
Keylogger	Programme, die Tastatureingaben mitprotokollieren. So können Hacker an Passwörter gelangen.
Krypto-/Erpressungs-trojaner	Wird auch **Ransomware** genannt. Daten werden auf dem PC verschlüsselt. Die Daten werden angeblich entschlüsselt oder wieder zurückgegeben, wenn ein Geldbetrag an die Kriminellen überwiesen wird.
Kindersicherung	Kindersicherungsprogramme schützen Kinder vor ungeeigneten Webinhalten und unkontrollierter Internetnutzung und schränken die zeitliche Nutzung von Computern ein. Das Betriebssystem Microsoft Windows besitzt eine Kindersicherung, die in den Internetoptionen bzw. in der Systemsteuerung aktiviert werden kann.
LAN	**L**ocal **A**rea **N**etwork: Ein **LAN** ist lokales Netzwerk z. B. in einem Schul- oder Firmengebäude. Computer werden über LAN-Kabel oder drahtlos mit dem Netzwerk verbunden und haben so Zugriff auf gemeinsame Ressourcen wie Drucker, Speicher und Internet.
Man-in-the-Middle-An-griff	Ein Hacker platziert sich bzw. seine Software zwischen dem Opfer und und einer aufgerufenen Internetseite, wie z.B. eine Bank oder Webmail. So können z.B. Überweisungen abgeändert oder Rechnungen gefälscht werden.

Netzwerk bzw. Netzwerktypen	**LAN:** **L**ocal **A**rea **N**etwork, *z.B. Firmennetzwerk* **WLAN:** **W**ireless **L**ocal **A**rea **N**etwork, *drahtloses Netzwerk bzw. Funknetzwerk* **VPN:** **V**irtuell **P**rivate **N**etwork, *verschlüsselte Verbindung, die Netzwerke über das Internet verbindet.*
MAC-Filter	Die **MAC-Adresse** (**M**edia-**A**ccess-**C**ontrol-Adresse) dient dazu, einen Computer im Netzwerk eindeutig zu identifizieren. Ein **MAC-Filter** gibt den Zugang zu einem Netzwerk nur für bestimmte MAC-Adressen frei - allen anderen ist der Zugang verwehrt. So können sich nur bestimmte Computer mit dem WLAN verbinden. *So sieht z.B. eine MAC-Adresse aus:* ***CC-52-AF-40-A0-1FA*** Ein MAC-Filter bietet wenig Sicherheit, weil MAC-Adressen mit Software beliebig geändert werden können.
Makro, Makroviren	Makroviren sind Viren, die als Programm in ein Dokument (z.B. Word oder Excel) eingebettet sind. Sie werden aktiv, wenn das schädliche Makro ausgeführt wird. Beim Öffnen z.B. eines Excel-Dokuments mit Makros wird nachgefragt, ob vorhandene **Makros aktiviert** werden sollen. In den Programmeinstellungen kann festgelegt werden, ob die Ausführung von Makros erlaubt wird.
Malware	Überbegriff für unerwünschte, schädliche Software. Malware kann einen Schaden am Computer (Software, gespeicherte Daten) anrichten. Mit einer **aktuellen Antivirensoftware** und dem Installieren von **Software-Updates** gegen **Sicherheitslücken** kann der Computer gegen Malware gesichert werden.
Mitarbeiter	IT-Systeme und Daten können auch durch die eigenen Mitarbeiter einer Firma bedroht werden: unabsichtlich wie durch Unaufmerksamkeit, absichtlich durch Weitergabe von Daten, Datenverfälschungen oder Sabotage durch unzufriedene oder ehemalige Mitarbeiter.
Multi-Faktor-Authentifizierung	Der Benutzer muss sich mehrfach identifizieren: • Etwas, das er weiß: Passwort oder Pin • Etwas, das er hat: Token (kann mit USB angesteckt werden und erzeugt ein Einmalpasswort) • Etwas, das er ist: Biometrie wie Fingerabdruck, Augenscan, Handscan
Netzwerk-Administrator	Ein Netzwerk-Administrator konfiguriert, betreibt und überwacht Datennetze für Computer. Aufgaben: Authentifizierung der Benutzer, Benutzerrechte verwalten, Nutzung dokumentieren, Updates (Sicherheitsaktualisierungen) durchführen, Netzverkehr überwachen, Malware bekämpfen.
Passwörter	Sichere Passwörter haben mindestens acht Buchstaben, Zahlen und Sonderzeichen. Für jeden Zugang sollte ein eigenes Passwort verwendet werden.

Passwort-Manager	Passwort-Manager speichern sensible Daten wie Benutzernamen und Kennwörter verschlüsselt an einem Ort auf der Festplatte des Computers. Statt sich viele Passwörter merken zu müssen, genügt jetzt ein Master-Passwort. Die Eingabe des Master-Passwortes gibt alle anderen frei.
Persönlicher Hotspot Tethering	Steht kein WLAN zur Verfügung, kann mit einem Smartphone ein persönlicher Hotspot (ein eigenes WLAN) zur Verfügung gestellt werden. Damit wird die mobile Datenverbindung des Smartphones für andere Geräte (Computer, Tablets, weitere Smartphones) freigegeben. Für den Hotspot sollte ein sicheres Passwort vergeben werden.
Phishing	***Phishing**: Kunstwort abgeleitet von **fishing** (Angeln, Fischen), meint das Angeln nach Passwörtern mit Ködern. Die Schreibweise mit -ph entstammt dem Hacker-Jargon.* Unter Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden. Bei dieser Form des Social Engineering wird die Gutgläubigkeit des Opfers ausgenutzt.
PIN	**P**ersönliche **I**dentifikations**n**ummer (PIN) oder Geheimzahl mit der sich Personen authentifizieren können.
Personenbezogene Daten	Personenbezogene Daten sind z. B. Geburtsdatum, Adresse, E-Mailadresse, Telefonnummer, Einkommen und Beruf. Besonders schutzwürdig (sensibel) sind Daten wie Religionsbekenntnis, rassische und ethnische Herkunft, politische Meinung, Gesundheit oder das Sexualleben.
Pharming	Betrugsmethode, bei der Anwender auf eine gefälschte Seite umgeleitet wird.
Pretexting	Daten eines Dritten (unter Vorgabe einer fremden Identität) besorgen. Pretexting ist ein anderer Begriff für Identitätsdiebstahl. Pretexting ist eine im Social Engineering angewandte Methode.
Quarantäne	Speicherort für verdächtige Dateien. Virenprogramme, die vom Antivirenprogramm in die Quarantäne verschoben wurden, können keinen Schaden mehr anrichten.
Ransomware	Krypto-/Erpressungstrojaner. Daten werden auf dem PC verschlüsselt. Die Daten werden angeblich entschlüsselt oder wieder zurückgegeben, wenn ein Geldbetrag an die Kriminellen überwiesen wird.
Rootkit	Programm, das Viren im Betriebssystem so versteckt, dass sie von Antivirenprogramme nicht entdeckt werden.
Shoulder Surfing	Informationsbeschaffung durch Beobachtung bei der Eingabe von Daten wie PINs oder Passwörtern.

Sichere Webseiten	Erkennbar an: ***https*** (***s***=secure) und dem Vorhangschloss. Sichere Webseiten haben ein digitales Zertifikat. Die Datenübertragung von gesicherten Webseiten erfolgt verschlüsselt. *Online-Banking und E-Commerce verwenden sichere Webseiten.*
Skimming	Ein Kartenlesegerät wird von Kriminellen vor dem Karteneinschubschacht der Geldautomaten montiert. Dieses Gerät liest die den Magnetstreifen von Bankomatkarten aus. Zusammen mit der erspähten PIN kann ein Betrüger mit einer kopierten Karte Beträge abheben.
Social Engineering	Zwischenmenschliche Beeinflussung mit dem Ziel, Personen zum Beispiel zur Herausgabe von vertraulichen Informationen zu bewegen. Betrüger spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Freundlichkeit, Hilfsbereitschaft oder Autoritätshörigkeit aus, um an geheime Informationen zu gelangen. Pretexting ist eine im Social Engineering angewandte Methode, mit der versucht wird, an persönliche Daten des Opfers zu kommen.
Spam oder Junk E-Mails	sind unerwünschte Werbemails. Das Aussortieren dieser E-Mails kostet Zeit und Geld. Mailprogramme versuchen, Spam zu erkennen und auszusortieren.
SSID	**S**ervice **S**et **I**dentifier: Die **SSID** ist der Name eines WLAN. Der voreingestellte Name für die SSID kann beliebig geändert werden. Dies erleichtert die Erkennung des eigenen WLANS. Die Anzeige der SSID kann in den Einstellungen versteckt werden. Damit wird Sie in der Liste der vorhandenen WLANs nicht angezeigt.
Spyware	Diese Malware forscht das Nutzerverhalten aus und sendet die Daten an Hersteller der Malware.
Sicherungskabel	Computer und mobile Geräte können entwendet werden. Sicherungskabel verhindern das Entwenden von mobilen Geräten.
Soziale Netzwerke und Daten	Das Löschen von Daten in sozialen Netzwerken ist bei manchen Diensten nicht endgültig. Dies sollte schon bei dem Hochladen von Informationen berücksichtigt werden.
Trojaner	Diese Malware ist in einem scheinbar nützlichen Programm versteckt und kann z. B. Passwörter auslesen oder auf Daten im Netzwerk zugreifen und diese an den Auftraggeber der Malware übermitteln.
Verfügbarkeit	Begriff zur Datensicherheit: Daten müssen ***jederzeit zur Verfügung stehen***. Daher müssen Maßnahmen getroffen werden, um Serverausfälle, Probleme mit der Internetverbindung etc. zu verhindern.
Vertraulichkeit	Begriff zur Datensicherheit: Informationen sollen ***vertraulich behandelt*** werden und ***vor Missbrauch geschützt*** werden. Nur befugte Personen dürfen Zugang zu vertraulichen Informationen haben.

Vertrauenswürdigkeit einer Website	Der Benutzer sollte die Vertrauenswürdigkeit an Hand folgender Punkte eine Website überprüfen können: URL, Impressum, Kontaktdaten, Sicherheitszertifikat, Domain-Inhaberschaft.
WLAN	***WLAN*** (eng. von ***W***ireless ***L***ocal ***A***rea ***N***etwork) bezeichnet ein lokales Funknetzwerk. Viele mobile Geräte wie Smartphones, Tabletts oder Notebooks werden über WLAN mit dem Internet verbunden.
VPN	**V**irtual **P**rivate **N**etwork: Ein VPN ist eine *v*erschlüsselte Verbindung, die Netzwerke über das Internet verbindet. *Ein Außendienstmitarbeiter verbindet sich per VPN über das Internet mit dem firmeneigenen Netzwerk.*
WEP	Veraltetes, unsicheres Verfahren zur Verschlüsselung von WLAN-Netzwerken.
WPA bzw. WPA2	Abkürzung für **W**i-Fi **P**rotected **A**ccess. Sicheres Verfahren zur Verschlüsselung von drahtlosen Netzwerken (WLAN).
Zugriff auf Daten	Auf Daten sollen nur befugte Benutzer zugreifen können. • Benutzerauthentifizierung durch Eingabe von Benutzername und Passwort/Kennwort • Schutz von Dateien durch ein Passwort: z. B. Word, Excel oder PowerPoint möglich. • Die Verschlüsselung von Daten verhindert unberechtigten Zugriff: z. B. Daten auf einem USB-Stick oder Notebook.
Zugriffskontrolle zum Internet	Für Kinder sollte der Zugriff zum Internet eingeschränkt werden: • Zeitliche Einschränkung: **Kindersicherung** (Software) oder Einstellung am Modem (wird vom Provider zur Verfügung gestellt). • Inhaltliche Einschränkung: Ein **Inhaltefilter** verhindert den Zugriff auf Webseiten mit ungeeignete Inhalten.