

**Add-on:** Eine Funktionserweiterung für ein Programm. Mithilfe eines Add-ons können Sie bspw. Ihrem Browser individuell Funktionen hinzufügen.

**App:** Kurzform des englischen Wortes „Application“. Damit ist ein Anwendungsprogramm gemeint, welches spezifisch auf das jeweilige Betriebssystem ausgelegt ist. Eine App, die auf das Betriebssystem Android zugreift, kann daher z. B. nicht auf einem iPhone verwendet werden und umgekehrt. Eine Web-App wiederum bezeichnet eine Webseite, die für Smartphones und Tablets angepasst worden ist – quasi als eine mobile Version der Seite.

**Backup:** Bei einem Backup speichern Sie eine Kopie einer Datei an einem zusätzlichen Ort. So beugen Sie den Verlust dieser Dateien vor. Backups sind besonders für Fotos und Dokumente von hohem finanziellen und emotionalen Wert wichtig.

**Blog:** Ein regelmäßig erscheinendes Online-Journal, in dem Unternehmen oder Privatpersonen Texte, Videos oder Bilder zu verschiedenen Themen veröffentlichen. Zumeist dienen diese dazu, Fachwissen oder Erfahrungen zu teilen.

**Browser:** Ein Computerprogramm, welches speziell zur Wiedergabe und Abbilden von Inhalten aus dem Internet (Text, Bilder, Videos) entwickelt wurde. Jeder Browser (ob bspw. Chrome, Firefox oder Edge) zeigt dieselben Inhalte in einer anderen Darstellung an.

**Brute-Force-Angriff:** Hacker nutzen diese Methode, um schwache Passwörter zu knacken. Das gelingt mithilfe von Algorithmen, die systematisch Zahlen- und Buchstabenkombinationen austesten.

**Cache:** Dieses digitale Kurzzeitgedächtnis eines Browsers ermöglicht das Zwischenspeichern von größeren Daten (bspw. Bilder) beim Besuchen einer Webseite. Somit können die Webseiten schneller geladen werden.

**Catfishing** ist eine Betrugsmasche, bei der sich die Kriminellen auf Dating-Plattformen oder in den sozialen Medien als jemand anderes ausgeben, um andere auszunutzen oder zu täuschen.

**CC/BCC:** Damit Sie die gleiche E-Mail nicht mehrfach versenden müssen, um mehrere Personen zu erreichen, können Sie die Nachricht per Kopie an weitere Empfänger weiterleiten. Personen in „CC“ sind hierbei für alle anderen Leser sichtbar, Empfänger in „BCC“ sind verborgen.

**ChatGPT** ist ein Prototyp eines Chatbots des amerikanischen Unternehmens OpenAI. Mithilfe von künstlicher Intelligenz ist es dem Bot möglich, jede Frage in Textform zu beantworten. Er wird für wissenschaftliche und allgemeine Fragen verwendet, lässt sich aber auch für einfache Dinge wie das Schreiben eines Valentinsgrußes nutzen.

**Cloud:** In einer Cloud lassen sich jegliche Inhalte digital auf einem Server sichern. Somit haben Sie von jedem internetfähigen Gerät auf der ganzen Welt Zugriff auf Ihre Daten. Praktisch: Bei Verlust Ihres Smartphones finden Sie z. B. Bilder in der Cloud vor – vorausgesetzt, Sie führen regelmäßige Backups durch.



**Cookies** sind kleine Datenpakete, die beim Aufruf einer Webseite automatisch auf Ihrem Gerät gespeichert werden. Sie beinhalten Informationen, die Rückschlüsse auf Ihr Nutzungsverhalten möglich machen (z. B. besuchte Unterseiten, Verweildauer oder Ihre gewählten Spracheinstellungen). Diese Informationen kann die Webseite bei erneutem Besuch wiederverwenden, um bspw. personalisierte Werbung zu schalten oder den letzten Warenkorb anzuzeigen.

**Cryptojacking:** Cyberkriminelle versuchen die Rechenleistung eines fremden Computers zu nutzen, um heimlich Kryptowährungen zu schürfen.

**Cybergrooming:** Sexuell motivierte Täter versuchen sich im Internet als Gleichaltrige auszugeben, um Minderjährige zu manipulieren.

**Cyberstalking** bezeichnet das digitale Nachstellen und auch Überwachen einer Person. Dies geschieht insbesondere in Beziehungen und kann sowohl aktuelle als auch ehemalige Partnerinnen und Partner betreffen.

**Darknet:** Das Darknet ist ein verschlüsselter Bereich des Internets, dessen Betreibende und Besuchende anonym sind. Es hat keinen offiziellen Zugang, sondern benötigt spezielle Darknet-Suchmaschinen oder eine exakte URL.

**Deepfakes** sind täuschend echt aussehende, aber künstlich hergestellte oder veränderte Foto-, Video- oder Sprachaufnahmen. Dabei kann es sich um einzelne Bilder realer Personen oder um vollständig neu geschaffene Bilder handeln. Stimmen können nachgeahmt oder neu geschaffen werden. Es können aber auch bestehende Reden verändert und Worte lippensynchron in den Mund gelegt werden.

**Digital Detox** ist eine beliebte Methode, um Stress abzubauen. In dem Sie sich bewusst für eine temporäre Auszeit von digitalen Geräten und dem Internet entscheiden, können Sie Ihr Wohlbefinden steigern.

**Domain** bezeichnet den eindeutigen Namen einer Webseite und ist somit ein Bestandteil der URL. So handelt es sich im Beispiel „<https://www.gmx.net>“ bei dem fettgedruckten Teil um die Domain. Bei einer E-Mail dagegen liegt sie hinter dem @-Zeichen – also „@gmx.de“.

**Doxing** bezeichnet die unbefugte Weitergabe oder das Veröffentlichen von persönlichen Daten einer Person im Internet.

**Emojis** sind Piktogramme oder Symbole, die in der digitalen Kommunikation zum Einsatz kommen (auch Smileys). Sie geben dem schriftlichen Austausch eine emotionale Tiefe und können in vielen Messenger-Diensten aus spezifischen Tastenkombinationen gebildet werden.

**Firewall** bezeichnet eine Schutztechnologie und dient der Sicherheit eines Computers. Mit dem Überprüfen des ein- und ausgehenden Datenverkehrs wehrt sie unbefugte Zugriffe ab, sodass schädliche Dateien erst gar nicht in das Computersystem gelangen.



**GIF** ist ein bestimmtes Grafikformat, bei dem eine kurze Bildsequenz tonlos animiert wird. GIFs dienen zur Unterhaltung und sind daher oftmals mit einem lustigen Spruch untermalt. Sie werden gerne über die sozialen Medien und über Messenger-Dienste verbreitet. Die Abkürzung steht für „Graphics Interchange Format“.

**GPS** ist die Abkürzung von „Global Positioning System“. Mithilfe von Satelliten wird eine bestimmte Position übertragen – bspw. den eigenen Standort im Auto, auf dessen Grundlage das Navi funktioniert.

**Hacker:** jemand, der Schwachstellen in Computersystemen und Netzwerken sucht und ausnutzt. Hacker können sowohl gute als auch böse Absichten haben.

**Homepage:** Diese spezielle HTML-Seite dient als Start- und Ausgangsseite einer Webseite. Über diese sind alle dazugehörigen Seiten via Hyperlinks erreichbar.

**Hoax:** Falschmeldungen, die über alle möglichen Medien verbreitet werden – auch via E-Mail oder Messenger.

**HTML:** Die „Hypertext Markup Language“ ist das Format, in dem Webseiten standardmäßig geschrieben werden. Browser „lesen“ die HTML-Datei und können eine Webseite somit grafisch darstellen.

**HTTPS** ist eine Kennzeichnung für die geschützte Übertragung von Informationen. In der Browserzeile stellt das „S“ hinter dem http (https) klar, dass die Verbindung zwischen dem Webserver und Browser SSL- bzw. TLS-verschlüsselt ist. Vor allem bei sensiblen Informationen (z. B. beim Online-Banking) ist das nicht wegzudenken und daher Standard.

**Influencer** sind Personen, die in den sozialen Medien eine große Anhängerschaft aufweisen und diese durch ihre Beiträge beeinflussen können.

**IP-Adresse:** Die „Internet Protokoll-Adresse“ ist eine Zahlenabfolge (z. B. 24.68.135.791), über die jedes internetfähige Gerät verfügt. Wie ein digitaler Fingerabdruck macht sie jedes Gerät im Internet eindeutig identifizierbar.

**JPEG/JPG** ist ein Format zum Abspeichern von Bilddateien. Hat eine Datei die Endung „.jpg“, dann handelt es sich um das JPEG-Format.

**Kryptowährungen** sind digitale, bargeldlose Zahlungsmittel. Sie stehen in keiner Abhängigkeit und unter keiner Aufsicht von Banken oder staatlichen Behörden. Bitcoin zählt dabei zu den bekanntesten Währungen.

**LAN:** „Local Area Network“ ist eine Verbindungsmöglichkeit mit dem Internet. Im Unterschied zu WLAN (kabellos) setzt LAN ein eingestecktes Kabel zwischen Router und dem zu verbindenden Gerät (z. B. Laptop) voraus.



**Lesezeichen** ermöglichen das Markieren, Speichern und Wiederfinden von Webseiten im Browser. Die Lesezeichenleiste unter der Adresszeile führt alle abgespeicherten Verlinkungen auf.

**Malware** ist ein Sammelbegriff für jegliche Schadsoftware wie Viren, Würmer und Trojaner. Cyberkriminelle verbreiten diese in den meisten Fällen zum Abgreifen von sensiblen Daten. Sie schleusen sich in ein Gerät ein, indem sie die Malware bspw. als Anhang einer Spam-Mail versenden.

**Memes** sind ein weit verbreitetes Phänomen der Netzkultur. Hierbei handelt es sich meist um Fotomontagen oder aus dem Kontext gerissene Fotos bzw. Screenshots. Ein Meme ist humoristisch und macht sich somit über eine Tatsache lustig oder übt Kritik aus.

**Money Muling** ist eine Betrugsmasche, bei der ahnungslose Opfer über das Internet zum Waschen von Schwarzgeld eingesetzt werden. Betroffene begehen als sogenannter „Money Mule“ eine Straftat.

**Newsletter** sind regelmäßige Rundschreiben eines Unternehmens, die per E-Mail an die Kundschaft geschickt werden.

**Noreply-E-Mail** ist eine E-Mail-Adresse, von der Nachrichten versendet werden, auf die keine Antwort erwartet wird bzw. möglich ist. Zumeist dienen solche E-Mails der reinen Informationsübermittlung.

**Passwordmanager:** Ein Passwortmanager hilft Ihnen, sich sicherer im Internet zu bewegen. Statt vieler verschiedener Passwörter müssen Sie sich nur noch ein Master-Passwort merken und können so jedes Konto mit einem eigenen Passwort sichern.

**Pharming:** Greifen Kriminelle Daten von Internetnutzenden direkt beim Surfen im Browser ab, wird von Pharming gesprochen.

**Phishing:** Unter diesem Begriff versteht man kriminelle Täuschungsversuche. Durch das Versenden von echt aussehenden E-Mails sollen Login-Daten oder andere sensible Informationen „abgefischt“ werden. Damit die Masche glaubwürdig wirkt, werden auch gefälschte Webseiten verwendet. Auf diesen werden Sie dazu aufgefordert, ein Dokument herunterzuladen oder Ihre Anmeldedaten einzugeben.

**Podcasts** sind digitale Medienproduktionen, in denen entweder spezifische oder allgemeine aktuelle Themen besprochen werden. In den meisten Fällen werden sie als Audio-Datei zur Verfügung gestellt, teils gibt es aber auch eine zusätzliche Video-Datei.

**Quellcode** ist der lesbare Text einer Programmiersprache. Die Tastenkombination [Strg] + U kann diesen bspw. auf einer Webseite sichtbar machen.

**Quishing:** Ein Phishing-Angriff über einen QR-Code wird als „Quishing“ bezeichnet.

**QR-Code** steht für „Quick Response Code“. Auf ihm sind Informationen bestehend aus Buchstaben und Zahlen gespeichert, bspw. ein Link. Scannt ein mobiles Endgerät mithilfe einer Kamera diesen Code, so können diese Informationen (wie eine Webseite) schnell abgerufen werden.



**Romance Scamming** bezeichnet eine Betrugsmasche auf Dating-Plattformen. Cyberkriminelle erschleichen sich das Vertrauen ihrer Opfer, um sie auszunutzen oder um sie aus erfundenen Gründen um Geld zu bitten.

**Router** dienen zur Herstellung eines Internetzugangs. Sie ermöglichen eine Verbindung zwischen dem öffentlichen Internet und dem Heimnetzwerk, sodass per LAN- oder WLAN-Verbindung das Internet genutzt werden kann.

**RSS-Feed:** Eine „Real Simple Syndication“ (zu Deutsch: „sehr einfache Verbreitung“) ist ein Web-Feed, der Sie automatisch über Änderungen oder auch neue Inhalte einer Webseite auf dem Laufenden hält. Er lässt sich als Add-on für den Browser installieren.

**Selfies:** Meist mit dem Smartphone aufgenommene Selbstporträts. Selfies sind vor allem in den sozialen Medien beliebt und werden von Influencern zur Selbstdarstellung und -vermarktung genutzt.

**Scareware:** Cyberkriminelle versuchen, Sie mit Scareware zu verunsichern und zu verängstigen. Diese Art von Schadsoftware enthält falsche Warnungen und soll Sie zu unüberlegten Handlungen verleiten, wie zum Beispiel zum Kauf unnötiger Software.

**Sharenting** beschreibt das Phänomen, dass Eltern Fotos und Informationen ihrer Kinder in sozialen Medien veröffentlichen. Ob unbedacht oder bewusst, dies kann negative Auswirkungen auf die Privatsphäre der Kinder haben und auch weitere negative Konsequenzen nach sich ziehen.

**Social Media** bezeichnet soziale Netzwerke und dient zum Erstellen und Verbreiten von Inhalten. User können sich mit einem eigenen Profil miteinander vernetzen und mit den Inhalten anderer interagieren.

**Spam** sind unerwünschte E-Mails, die unter anderem unverlangte Werbung oder Viren beinhalten können. In den meisten Fällen landen diese dank des Spam-Filters direkt in dem dafür vorgesehenen Spam-Ordner.

**Screenshot** bedeutet übersetzt Bildschirmfoto. Hierbei handelt es sich um eine digitale Aufnahme des aktuell dargestellten Bildschirminhalts. Er lässt sich sowohl am PC als auch am Smartphone durchführen.

**Streaming** ermöglicht das Konsumieren von Audio- und Filmdateien ohne Download oder analoge Datenträger wie CDs oder DVDs. Streaming-Dienste wie etwa Netflix benötigen zum Übertragen lediglich eine stabile Internetverbindung.

**Taskleiste** bezeichnet die Leiste, die sich in der Regel am unteren Rand des Bildschirms befindet. Hier haben Sie einen schnellen Zugriff auf Ihre Programme und können sie zentral starten und konfigurieren.



**Trojaner:** Der Begriff ist abgeleitet vom Trojanischen Pferd. Es handelt sich um Programme, die ähnlich wie Viren unerwünschte Aktionen auf Ihrem Gerät ausführen. Allerdings harmlos getarnt als bspw. ein Antiviren-Programm. Wird hierbei Lösegeld erpresst, spricht man von Ransomware.

**Twitch** ist eine internationale Streaming-Plattform. Hier können vorrangig Live-Übertragungen von Videospielen angeschaut oder auch selbst gestartet werden.

**URL:** Die „Uniform Resource Locator“ ist notwendig, um eine Webseite aufrufen zu können. Sie ist deren individuelle Internet-Adresse.

**Viren** sind Schadsoftware und können erheblichen Schaden auf jedem Gerät verursachen. Sie befallen Dateien und Programme, um sich zu vermehren. Im Gegensatz zu Computer-Würmern, vermehren sie sich nicht selbstständig, sondern werden durch eine Aktion Ihrerseits ausgelöst.

**Weblinks** oder Hyperlinks sind Querverweise zwischen Webseiten oder Dokumenten, die per Klick eine automatische Weiterleitung ermöglichen. Die Bestandteile sind eine spezifische URL und ein Linktext.

**WLAN** steht für „Wireless Local Area Network“. Für einen Internetzugang wird im Gegensatz zur LAN-Verbindung kein Kabel mehr benötigt, stattdessen wird über Funk kommuniziert.

**WiFi** ist die am weitesten verbreitete WLAN-Technologie. Vor allem im Ausland ist die Bezeichnung WiFi gebräuchlicher als WLAN. Daher ist jedes WiFi ein WLAN, aber nicht jedes WLAN ist ein WiFi.

**Wurm:** Bösartige Software, die Kopien von sich selbst an andere Computer im Netzwerk sendet und sich selbstständig verbreitet. Computer-Würmer können großen Schaden anrichten.

**YouTube** ist eine Plattform, auf der Videos und Livestreams angeschaut, kommentiert und geteilt werden können.

**ZIP** ist ein Format, mit dem sich Dateigrößen von Bildern oder Dokumenten ohne Qualitätsverlust verkleinern lassen. So können Sie leichter weitergeleitet werden, müssen allerdings im Anschluss wieder „entzippt“ werden.

