CREW
Creativity, Resilience and Empowerment for Work

Project No.2020-1-LT01-KA204-077916

CREW

Creativity, Resilience, Empowerment for Work

IO1 TRAINING COURSE IN DIGITAL LITERACY

CREW
Creativity, Resilience and Empowerment for Work

Co-funded by the Erasmus+ Programme of the European Union

2021

CREW PROJEKTPARTNER

Inhaltsverzeichnis

Zielsetzung und Zweck der IO1

Das Internet wurde im XXI. Jahrhundert zu einer Ware, fast so wie Öl, Getreide oder Zucker. Es ist die Hauptzutat für die Existenz von Dienstleistungen in vielen Bereichen, wie Finanzen, Gesundheit, Marketing, Unterhaltung, Bildung. Das Internet ist eine Art Rohstoff oder ein Gerüst selbst, das als Baumaterial für eine Vielzahl anderer Dienste und Ökosysteme verwendet wird, die sich um es herum entwickeln.

Da sich digitale und Online-Tools schnell weiterentwickeln, miteinander verschmelzen und ein noch breiteres Spektrum an Dienstleistungen und innovativen Produkten hervorbringen, während die Geräte, die bei alltäglichen persönlichen und öffentlichen Aktivitäten verwendet werden, immer schneller werden, weit verbreitet sind und miteinander verbunden sind, werden die Fähigkeiten der digitalen Kompetenz für den Aufbau einer Karriere und den erfolgreichen Wettbewerb auf dem Arbeitsmarkt unerlässlich. Die ständige Entwicklung von Fähigkeiten, sinnvolles und zielgerichtetes Engagement in der digitalen Welt, die Fähigkeit, die Informationen über das Internet zu konsumieren, zu bewerten und zu erstellen, gleichzeitig sicher und widerstandsfähig gegen gefälschte und minderwertige Informationen zu bleiben - all das ist von nicht weniger Bedeutung.

Hochqualifizierte und vielseitige Menschen, die in der Lage sind, sich schnell an die sich ständig ändernden Bedingungen anzupassen, werden von den Arbeitnehmern am meisten geschätzt, insbesondere in einer digitalisierten Welt. Die Fähigkeit, eine Tastatur und eine Maus bedienen zu können, ein gewisses Maß an Wissen zu besitzen, wird nicht mehr als Vorteil angesehen. Von den Menschen wird ein sehr breites Spektrum an grundlegenden und eine Reihe spezialisierter digitaler Fähigkeiten verlangt sowie die Fähigkeit, sich in sehr schnellem Tempo neue Fähigkeiten anzueignen.

Daher ist es das Ziel dieses Kurses, die Grundkenntnisse, die Einzelpersonen bereits besitzen, zu erweitern und ihre allgemeinen digitalen Fähigkeiten zu verbessern und sie für die weitere Entwicklung zu befähigen, während er Menschen mit geringeren technischen Kenntnissen hilft, ihre Ängste bei der Verbesserung der digitalen Fähigkeiten zu bekämpfen. Dieser Kurs richtet sich an weniger geübte erwachsene Lernende, um ihnen zu helfen, sich mehr in die Gesellschaft und den Arbeitsmarkt einzubringen, sowie an Pädagogen, Organisationen und Institutionen, die Lernkurse organisieren, die sich mit der Lehre und Ausbildung von digitalen Kompetenzen und verwandten Themen beschäftigen und die von der Nutzung unserer Kurse für ihre Bildungszwecke profitieren können.

1. Theorie und Methodik der digitalen Kompetenz

1.1. Beschaffung von Informationen

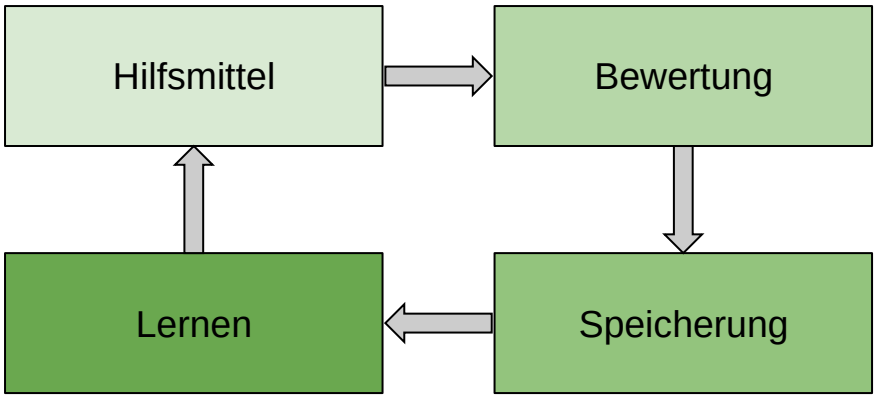
Obwohl der Begriff der Informationsbeschaffung nichts Neues ist, schafft er in einer so stark vernetzten Welt zu Beginn des 3. Jahrzehnts im XXI. Die American Library Association (ALA, 1989) definiert Informationskompetenz als die Fähigkeit, festzustellen, welche Informationen benötigt werden, zu verstehen, wie die Informationen aufbereitet werden, die besten Informationsquellen für ein bestimmtes Bedürfnis zu finden, diese Quellen zu identifizieren, die Quellen analytisch zu bewerten und diese Informationen weiterzugeben.

Die über drei Jahrzehnte alte Erklärung der Informationskompetenz hat sich bewährt und definiert recht gut, was Informationsbeschaffung aus der Perspektive der digitalen Kompetenz sein kann. Allerdings macht der leicht zugängliche, sich schnell verändernde und oft ungewollte Informationsfluss in einer digitalisierten Welt den Informationserwerb aufgrund des enorm unterschiedlichen Umfangs der über das Internet verfügbaren Informationen sehr viel anders.

Wir bleiben bei den Grundlagen und betonen die folgenden Hauptsäulen dessen, was Informationsbeschaffung im Rahmen der digitalen Kompetenz ist:

1. Es ist die Fähigkeit, Online-Tools zur Informationsbeschaffung richtig zu nutzen;
2. Informationen kritisch bewerten und irrelevante von minderwertigen Informationsquellen herausfiltern;
3. Die erworbenen Informationen sicher speichern und verwalten können;
4. Sich das neue Wissen selbst anzueignen und in der Lage zu sein, kontinuierlich neue Fähigkeiten zu entwickeln und ununterbrochen zu lernen, um mehr und qualitativ bessere Informationen zu erwerben.

Abbildung 1.1. Eine Illustration des kontinuierlichen Zyklus der Informationsbeschaffung und Qualitätsverbesserung



Die grundlegenden Hilfsmittel zur Erfassung der digitalisierten Informationen sind in der Regel recht gut bekannt und beliebt:

1. Google und andere Suchmaschinen
2. Wikipedia
3. Youtube und andere Video-Services
4. Social media - Facebook, Twitter, Linkedin
5. Nachrichtenportale, Foren, Internet-Verzeichnisse

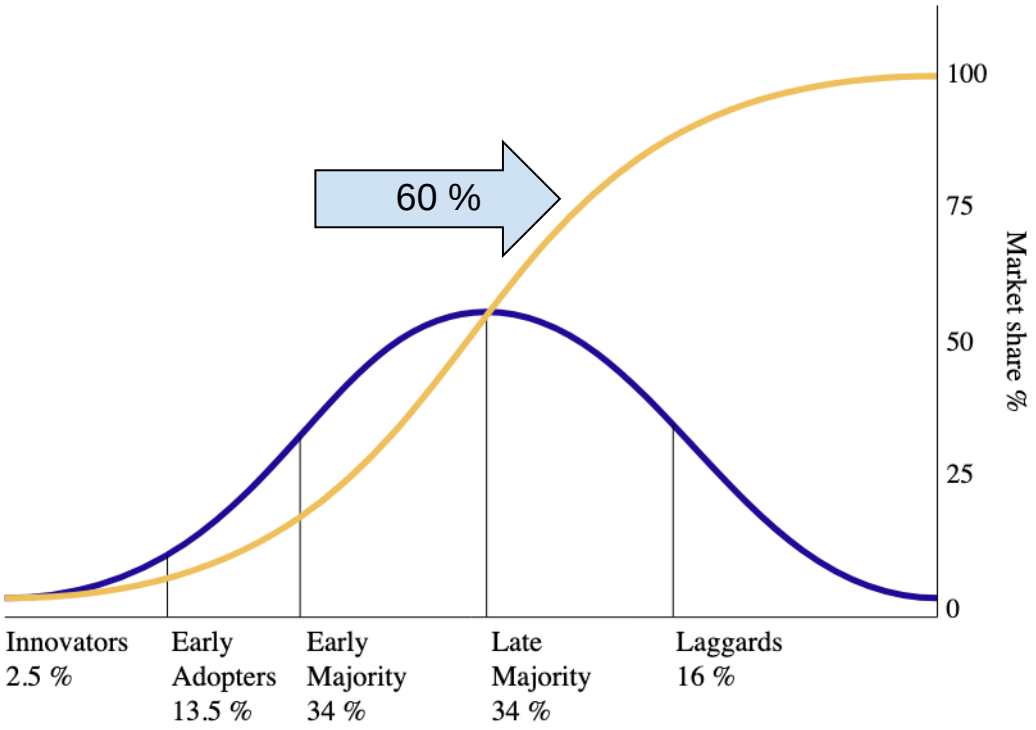
Die Speicherung von Informationen ist ein eher technisches Thema, daher werden wir die Themen, wie Sicherheit, Zuverlässigkeit und Best Practices oder verwandte Themen für die Informationsspeicherung in weiteren Kapiteln behandeln.

Der Evaluationsteil ist entscheidend für die Entwicklung der notwendigen digitalen Fähigkeiten; daher werden wir im nächsten Kapitel tiefer in dieses Thema eintauchen.

Was ist die aktuelle Annahme, wie viel das Internet im Moment ist?

Nach dem Modell der Diffusion von Innovationen von Everett Rogers, mit dem sich die Entwicklung und Annahme jeder Technologie gut beschreiben lässt, sind wir noch weit davon entfernt, dass das Internet auf der ganzen Welt angenommen wird.

Abbildung 1.2. Akzeptanz des Internets basierend auf einer Internet-Penetration von 60 % im Jahr 2021 [Quelle: Statista.com]



Trotz der ungleichmäßigen Verbreitung des Internets auf der ganzen Welt können wir die digitalen Werkzeuge und die Internetverbindung immer noch als den wichtigsten positiven Faktor zur Verbreitung von Ideen, zur Bildung der Menschen und zur Bekämpfung von Armut und Arbeitslosigkeit betrachten.

1.2. Auswertung von Informationen

Warum müssen wir die Informationen auswerten?

Sobald Sie Informationen gefunden haben, die dem Thema und den Anforderungen Ihrer Recherche entsprechen, sollten Sie diese Informationsquellen analysieren oder bewerten. Das Bewerten von Informationen ermutigt Sie dazu, kritisch über die Zuverlässigkeit, Gültigkeit, Genauigkeit, Autorität, Aktualität, den Standpunkt oder die Voreingenommenheit von Informationsquellen nachzudenken.

Nur weil ein Buch, ein Artikel oder eine Website Ihren Suchkriterien entspricht und somit auf den ersten Blick relevant für Ihre Recherche zu sein scheint, bedeutet dies nicht, dass es sich dabei um eine zuverlässige Informationsquelle handelt. Es ist wichtig, daran zu denken, dass Informationsquellen, die die gedruckten und elektronischen Sammlungen der Bibliothek umfassen, bereits für die Aufnahme in die Ressourcen der Bibliothek bewertet wurden. Dies bedeutet jedoch nicht unbedingt, dass diese Quellen für Ihre Recherche relevant sind.

Dies gilt nicht unbedingt für Informationsquellen im Web für die Allgemeinheit. Viele von uns mit Internet/Web-Accounts sind potenzielle Herausgeber von Websites; die meisten dieser Inhalte werden ohne redaktionelle Prüfung veröffentlicht. Denken Sie darüber nach. Es gibt viele Ressourcen, die bei der Bewertung von Webseiten helfen.

Der einfachste Weg, die Informationen zu bewerten, ist, die richtigen Fragen zu stellen. Welche Kriterien sollten Sie zur Beurteilung von Informationsquellen verwenden?

1. Schauen Sie sich zunächst den Autor, den Titel, den Verlag und das Datum der Veröffentlichung an. Diese Informationen sind in der bibliografischen Angabe zu finden und können ermittelt werden, noch bevor Sie den physischen Artikel in der Hand haben.
2. Schauen Sie sich als Nächstes den Inhalt an, z. B. die beabsichtigte Zielgruppe, die Objektivität des Textes, den Umfang, den Schreibstil und, falls vorhanden, bewertende Rezensionen.

Um die Qualität der Informationen schrittweise zu bewerten, sollten zum Beispiel folgende Fragen gestellt werden:

Wer ist der Autor (kann eine Einzelperson oder eine Organisation sein) und/oder der Verleger?

1. Wie lauten die Referenzen und die Zugehörigkeit oder das Sponsoring der genannten Personen oder Organisationen?
2. Wie objektiv, zuverlässig und aussagekräftig sind sie?
3. Haben sie andere Artikel oder Bücher geschrieben?
4. Ist der/die Autor(en) mit Kontaktinformationen (Straße, E-Mail) aufgeführt?
5. Hat der Verlag andere Werke veröffentlicht?
6. Haben sie sich auf die Veröffentlichung bestimmter Themen oder Bereiche spezialisiert?
7. Ist der Verlag wissenschaftlich (Universitätsverlag, wissenschaftliche Vereine)? Kommerziell? Regierungsbehörde? Selbstverlag ("Vanity press")?

Was kann über den Inhalt, den Kontext, den Stil, die Struktur, die Vollständigkeit und die Genauigkeit der von der Quelle gelieferten Informationen gesagt werden?

1. Werden irgendwelche Schlussfolgerungen angeboten? Wenn ja, auf welcher Grundlage und gestützt auf welche primären und sekundären Unterlagen?
2. Was wird durch den Inhalt impliziert?
3. Sind unterschiedliche Perspektiven vertreten?
4. Ist der Inhalt für Ihren Informationsbedarf relevant?

Wann wurde die Information veröffentlicht?

1. Das Erscheinungsdatum befindet sich in der Regel auf der Titelseite oder auf der Rückseite des Titelblatts (Copyright-Datum).
2. Ist die von der Quelle gelieferte Information in ihrer ursprünglichen Form oder wurde sie überarbeitet, um Änderungen im Wissensstand zu berücksichtigen?
3. Sind diese Informationen zeitgemäß und werden sie regelmäßig aktualisiert?

Wo sind die von der Quelle angegebenen Informationen sonst noch zu finden?

1. Ist diese Information authentisch?
2. Ist diese Information einzigartig oder wurde sie kopiert?
3. Warum wurde die von der Quelle gelieferte Information veröffentlicht?

In welchem Kontext stehen diese Informationen?

1. Welche Perspektiven, Meinungen, Annahmen und Vorurteile hat derjenige, der für diese Informationen verantwortlich ist?
2. Wer ist die Zielgruppe?

3. Wird etwas verkauft?

CRAAP (ein Akronym für Currency, Relevance, Authority, Accuracy, and Purpose) Test ist ein gutes Beispiel und auch eine Lösung, wie man die Qualität der Informationsquellen bewerten kann: https://researchguides.ben.edu/source-evaluation.

Eine ordnungsgemäße Einführung in die Bewertung von Informationen ist entscheidend, um wünschenswerte Ergebnisse für die Verbesserung der digitalen Kompetenz zu erzielen, vor allem, wenn man den Lernenden die Richtungen und Richtlinien für ihre Selbstverbesserung und ihr Selbstlernen durch Übung gibt.

1.3. Digitale Informationserstellung als Lernprozess

Informationen in jedem Format werden produziert, um eine Botschaft zu vermitteln und werden über eine ausgewählte Liefer- und Verteilungsmethode geteilt. Die iterativen Prozesse des Recherchierens, Erstellens, Überarbeitens und Teilens der Informationen variieren, daher ist der gesamte Prozess selbst ein großer Teil des ständigen Lernprozesses, während die Informationen sowohl erstellt, konsumiert und verteilt werden.

Learning-by-doing als Bildungsansatz eignet sich sehr gut für die Verbesserung der digitalen Kompetenzen, da es eine sehr große Auswahl an Tools und Software gibt, die von Schülern aller Fähigkeitsstufen genutzt werden können, um bestimmte Ziele für die Ergebnisse und Lernzwecke zu erreichen. Die derzeit existierenden Tools und Instrumente in der digitalen Welt sind in jedem Land verfügbar, unterstützen die meisten Sprachen und sind entweder sehr günstig oder völlig kostenlos zu verwenden. Dies macht den Erwerb digitaler Fähigkeiten für jeden verfügbar und relativ einfach. Um den Bildungsprozess zu verfeinern, müssen die Pädagogen das richtige Medium für die Vermittlung ihrer Ausbildung wählen.

Nehmen Sie das Erstellen von Websites als praktisches Beispiel. Um eine Website erstellen zu können, muss eine Person über grundlegende Kenntnisse und Fähigkeiten im Umgang mit dem Computer verfügen, die ihr helfen, die notwendigen Anweisungen und Anforderungen für die Website-Erstellung zu finden. Diese grundlegenden Fähigkeiten können bereits während der formalen Ausbildung erworben werden, tieferes Wissen wird jedoch erst nach Abschluss der praktischen Aufgaben erworben.

Der Aufbau einer Website ist eine komplexe Aufgabe, die eine Verbesserung der Fähigkeiten bei der Informationssuche und -auswertung, der Speicherung, aber auch der Erstellung und Verteilung erfordert, daher betonen wir, dass diese Art von Übung ein perfekt geeigneter Weg zur Verbesserung der digitalen Fähigkeiten ist. Falls erforderlich, können Übungen zum Aufbau einer Website Marketing und Kommunikation, das Schreiben von Qualitätsartikeln, die mit interaktiven und Rich-Media-Ergänzungen ergänzt werden, Recherchen über das Verhalten und die Erfahrungen von Internetnutzern, Sicherheit und Datenschutz und wie das Design, die Struktur oder die Funktionalitäten einer Website helfen können, die besten Ergebnisse zu erzielen, beinhalten.

Die Lernenden können entweder an der Erstellung eines persönlichen Blogs oder einer einfachen E-Commerce-Website arbeiten, was sie dazu zwingt, die notwendigen Fähigkeiten in Bereichen wie Finanzen, Erstellung einer digitalen Identität, Vorsichtsmaßnahmen gegen Cyberkriminalität, Verwendung von E-Signaturen und E-Government-Diensten zu erwerben. Sie sollten auch beginnen, sich selbst als Teil eines nie endenden Prozesses zu sehen, sowohl bei der Erstellung von Informationen als auch beim gleichzeitigen Konsum von Informationen, was ihre Wahrnehmung der digitalen Kompetenz als Ganzes erweitert.

Unsere methodische Empfehlung für die Vermittlung digitaler Kompetenzen ist es, einen praktischen Ansatz für den Aufbau von Websites zu verwenden und bestimmte Übungen auf der Grundlage der tatsächlichen Fähigkeiten, Motivationen und Erwartungen der Lernenden anzupassen.

2. Entwicklung von Hauptfähigkeiten

2.1. Digitale Kompetenz als kultureller Ansatz

Wir erleben eine Zeit der technologischen Entwicklung, die sowohl beispiellos als auch weitreichend disruptiv ist. In der kurzen Zeit seit der Entstehung des Internets hat sich vieles verändert, darunter das Design von Computeroberflächen, die Verarbeitungsgeschwindigkeit und Portabilität von Geräten, die Zugänglichkeit von Informationen und Wissen, unsere Kommunikationsmethoden, die Pflege unserer Beziehungen, der Handel, der Schutz der persönlichen Privatsphäre, kreative Prozesse, die Veröffentlichung von Inhalten und die Entstehung neuer digitaler Stämme und virtueller Klans (Wheeler, 2009)[1].

Mehrere kürzlich veröffentlichte Artikel haben sich mit dem Begriff der "digitalen Kompetenz" auseinandergesetzt, und wie zu erwarten, gibt es zahlreiche Ansichten. Anderson (2010) zum Beispiel beschreibt digitale Kompetenzen als die Fähigkeit, das Potenzial von Computertechnologien zu nutzen. Literacies, in all ihren Formen, sind gleichzeitig kulturell, sozial und persönlich (Kress, 2009) und ermöglichen es uns, in spezifischen Kulturen vollständig zu interagieren. Einige warnen davor, dass digitale Medien ohne ein angemessenes Niveau an Lese- und Schreibfähigkeiten die Fähigkeit haben, einige zu benachteiligen (van Dijk, 2005) , während andere davor warnen, dass die Natur des Webs Wissen und Kompetenz untergräbt (Carr, 2008; Keen, 2007) . Die überwältigende Mehrheit der Kommentatoren lobt jedoch das Potenzial des Social Web zur Befreiung der Bildung und zur Demokratisierung des Lernens, unter dem Vorbehalt, dass digitale Kompetenzen eingeübt werden. Die American Library Association's digital-literacy task force bietet diese Definition an: "Digitale Kompetenz ist die Fähigkeit, Informations- und Kommunikationstechnologien zu nutzen, um Informationen zu finden, zu bewerten, zu erstellen und zu kommunizieren, was sowohl kognitive als auch technische Fähigkeiten erfordert."

Der Begriff "digitale Kompetenz" ist in den letzten 10 Jahren so populär und weit verbreitet geworden, dass er fast schon als selbstverständlich angesehen wird. Mit unterschiedlichem Grad an Komplexität wird der Ausdruck "digitale Kompetenz" nun verwendet, um unseren Umgang mit digitalen Technologien zu beschreiben, da diese viele (wenn nicht sogar die meisten) unserer sozialen Interaktionen vermitteln.

Mit dieser Definition der American Library Association für digitale Kompetenz als Richtschnur ist es wichtig zu verstehen, dass selbst Digital Natives, die wissen, wie man eine SMS verschickt und in sozialen Medien postet, noch lange nicht als "digital gebildet" gelten. Es ist wichtig anzumerken, dass das bloße Lesen im Internet oder das Abonnieren eines eBook-Dienstes noch keinen digital gebildeten Schüler ausmacht.

[1] Wheeler, S. (2009, Ed) Connected Minds, Emerging Cultures: Cybercultures in Online Learning. Charlotte, NC: Information Age.

Digitale Kompetenz in der Bildung umfasst so viel mehr. So müssen Sie beispielsweise über bestimmte Fähigkeiten verfügen, wenn Sie Online-Texte lesen, die eingebettete Ressourcen wie Hyperlinks, Audioclips, Grafiken oder Diagramme enthalten, bei denen Sie eine Auswahl treffen müssen.

Digitale Kompetenz bedeutet, die Fähigkeiten zu besitzen, die man braucht, um in einer Gesellschaft zu leben, zu lernen und zu arbeiten, in der die Kommunikation und der Zugang zu Informationen durch digitale Technologien wie Internetplattformen, soziale Medien und mobile Geräte zunimmt.

Die Entwicklung Ihres kritischen Denkens ist unerlässlich, wenn Sie mit so vielen Informationen in verschiedenen Formaten konfrontiert werden - das Suchen, Sichten, Bewerten, Anwenden und Produzieren von Informationen erfordert allesamt kritisches Denken.

Auch die Kommunikation ist ein wichtiger Aspekt der digitalen Kompetenz. Wenn Sie in virtuellen Umgebungen kommunizieren, ist die Fähigkeit, Ihre Ideen klar auszudrücken, relevante Fragen zu stellen, Respekt zu wahren und Vertrauen aufzubauen, genauso wichtig wie bei der persönlichen Kommunikation.

Sie brauchen auch praktische Fähigkeiten im Umgang mit Technologie, um auf Informationen zuzugreifen, sie zu verwalten, zu manipulieren und zu erstellen, und zwar auf ethische und nachhaltige Weise. Es ist ein ständiger Lernprozess, weil es ständig neue Apps und Updates gibt und Sie Ihr digitales Leben in Ordnung halten müssen!

Digitale Kompetenz ist jetzt wirklich wichtig und wird auch in Ihrer beruflichen Zukunft sehr wichtig sein. An Ihrem Arbeitsplatz müssen Sie mit Menschen in digitalen Umgebungen interagieren, Informationen auf angemessene Weise nutzen und neue Ideen und Produkte kollaborativ erstellen. Vor allem müssen Sie Ihre digitale Identität und Ihr Wohlbefinden aufrechterhalten, da sich die digitale Landschaft weiterhin in rasantem Tempo verändert.

Wie bereits erwähnt, entwickeln sich digitale Fertigkeiten über ein Kontinuum und werden ständig im Einklang mit den technologischen Veränderungen aktualisiert. Rahmenwerke für digitale Kompetenzen spielen eine entscheidende Rolle bei der Erfassung des Spektrums an Kompetenzen sowie dieser Veränderungen und ermöglichen es so den politischen Entscheidungsträgern und Anbietern digitaler Kompetenzen, sicherzustellen, dass ihre Programme und Ausbildungslehrpläne relevant und aktuell bleiben. Viele Organisationen und internationale Agenturen haben Frameworks für digitale Kompetenzen entwickelt. Wir heben die Arbeit der Europäischen Kommission hervor - den Digital Competence Framework for Citizens (oder DigComp), der eine gemeinsame Sprache für die Identifizierung und

Beschreibung der Schlüsselbereiche digitaler Kompetenz bietet und somit eine gemeinsame Referenz auf europäischer Ebene darstellt.[2]

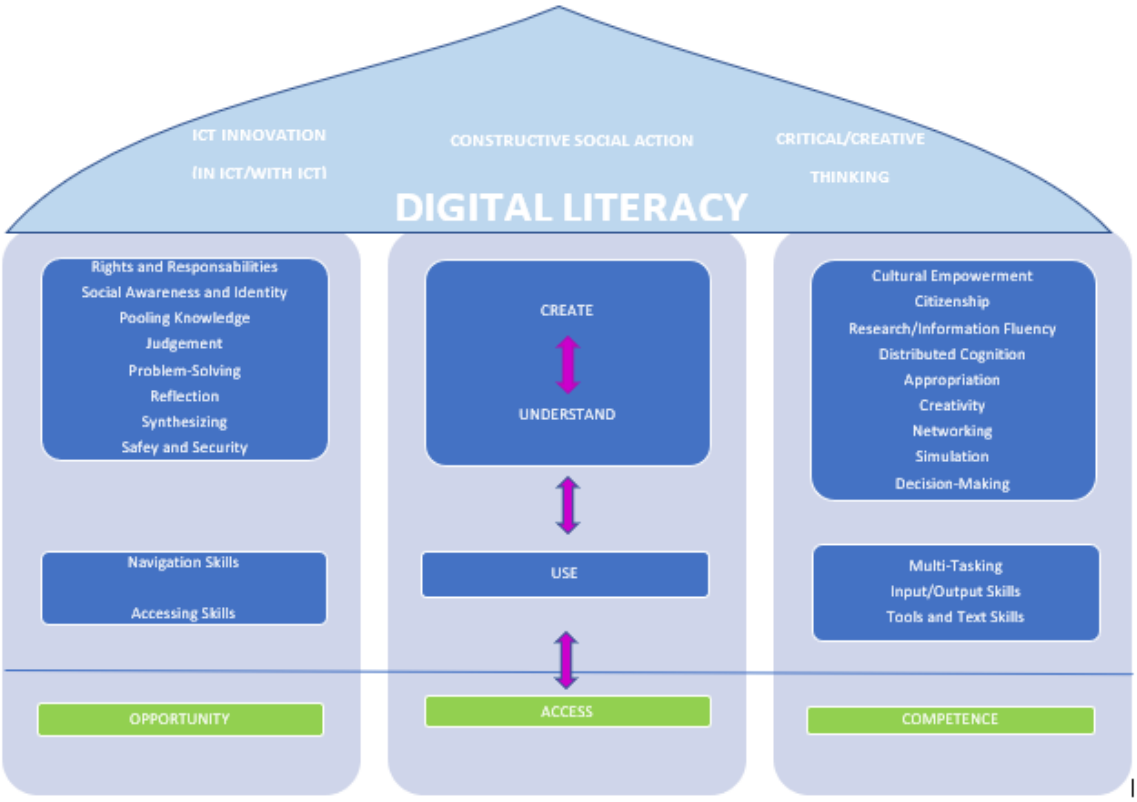
Weltweit setzt die International Society for Technology in Education (ISTE) ihre Maßstäbe für digitale Kompetenz an sechs Standards fest: Kreativität und Innovation, Kommunikation und Zusammenarbeit, Recherche und Informationskompetenz, kritisches Denken, Problemlösung und Entscheidungsfindung, digitale Bürgerschaft sowie technologische Abläufe und Konzepte.[3]

Dieses Modell zeigt die vielen miteinander verbundenen Elemente, die unter das Dach der digitalen Kompetenz fallen. Es gibt eine logische Progression von den grundlegenderen Fähigkeiten hin zu den höheren, transformativeren Ebenen, aber dies ist nicht unbedingt ein sequentieller Prozess: Vieles hängt von den Bedürfnissen der einzelnen Benutzer, von Ihren Bedürfnissen ab.

Modell für digitale Kompetenz

[2] '[DigComp] ist ein Werkzeug, um die digitale Kompetenz der Bürger zu verbessern, den politischen Entscheidungsträgern bei der Formulierung von Maßnahmen zu helfen, die den Aufbau digitaler Kompetenz unterstützen, und Bildungs- und Trainingsinitiativen zu planen, um die digitale Kompetenz von bestimmten Zielgruppen zu verbessern. DigComp stellt auch eine gemeinsame Sprache zur Verfügung, wie die Schlüsselbereiche der digitalen Kompetenz identifiziert und beschrieben werden können und bietet somit eine gemeinsame Referenz auf europäischer Ebene
.'

[3] International Society for Technology in Education (2007). iste.nets.s: Advancing Digital Age Learning. Iste.org/nets.

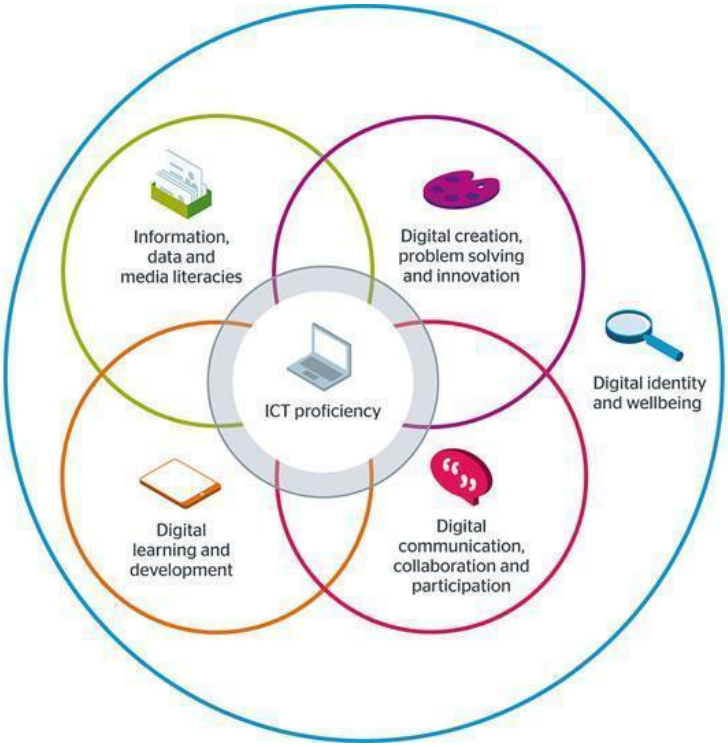


Was sind die Elemente, die Sie zu digitaler Kompetenz machen?

Digitale Kompetenz geht über funktionale IT-Fähigkeiten hinaus und beschreibt ein umfassenderes Spektrum an digitalen Verhaltensweisen, Praktiken und Identitäten.

Das untenstehende Jisc-Modell veranschaulicht die Idee, dass die Beherrschung der IKT (Informations- und Kommunikationstechnologie) ein Kernelement unserer digitalen Kompetenz ist, während andere Fähigkeiten diese überlagern und darauf aufbauen, und über allem steht unsere digitale Identität und unser Wohlbefinden.

Abbildung 2.1. Das Jisc Model



Abgerufen von https://www.jisc.ac.uk/rd/projects/building-digital-capability

1. ICT-Kenntnisse (Funktionale Fähigkeiten).
2. Informations-, Daten- und Medienkompetenz (Kritische Nutzung)
3. Digitale Kreation, Problemlösung und Innovation (Kreative Produktion)
4. Digitale Kommunikation, Kollaboration und Beteiligung (Teilnahme)
5. Digitales Lernen und Entwicklung (Entwicklung)
6. Digitale Identität und Wohlbefinden (Selbstverwirklichung)

2.2. Abbau von Ängsten bei der Entwicklung digitaler Fähigkeiten und beim Unterrichten

Für einige Erwachsene - einschließlich junger Erwachsener - ist die unvollständige Nutzung des Internets mit geringen Lese-, Schreib- und Rechenkenntnissen verbunden sowie mit mangelndem Selbstvertrauen und fehlender Motivation, neue Fähigkeiten zu erlernen und diese in ihrem Leben anzuwenden. Digitale Fähigkeiten sind der Schlüssel zur Integration in die Gesellschaft. Der Erwerb dieser Fähigkeiten, zusammen mit dem Selbstvertrauen und der Motivation, sie im realen Leben anzuwenden, kann den Menschen helfen, ein besseres Leben zu führen. Viele Menschen schämen sich, weil sie nicht wissen, wie man das Internet nutzt, und Computerangst ist eine Folge davon. Computerangst ist ein weit verbreitetes Phänomen seit der Einführung von Computern in unser Leben. Es zeigt sich, dass Benutzer, die wenig über Computer wissen, eher Angst vor ihnen haben, aber Digitalangst kann durch die Steigerung der Fähigkeit, technologische und digitale Probleme zu lösen, reduziert werden. Angst selbst wird als eine psychische Gesundheitsstörung definiert, die "übermäßige" Ängste und Sorgen umfasst. Diese oft "stille" Behinderung kann sich auf zahlreiche Arten manifestieren, und das tägliche Leben ist keine Ausnahme.

Häufige Anzeichen dafür, dass Sie unter digitalem Stress leiden, wenn Sie im Umgang mit digitalen Werkzeugen ungeübt sind, sind u. a. die folgenden:

- Angst oder Panikattacken
- Isolation oder Rückzug von sozialen Aktivitäten
- Erhöhte Geheimhaltung
- Wut
- Depression
- Schlechte Noten
- Aufstand
- Magenschmerzen, Kopfschmerzen oder andere allgemeine Körperschmerzen, die nicht durch eine medizinische Erkrankung erklärt werden können

Der Zugang zu Technologie und digitalen Fähigkeiten ist entscheidend für den Zugang zu wichtigen Bereichen in der Schule und im sozialen Leben, aber trägt die Technologie zu der offensichtlichen Zunahme von Angstproblemen in der modernen Welt bei? Was hat es mit der digitalen und neuen Technologie auf sich, das viele von uns ängstlich und gestresst macht? IT-Angst ist gekennzeichnet durch Gefühle der Sorge und Besorgnis sowie körperliche Anspannung im Zusammenhang mit der aktuellen oder zukünftigen Nutzung von Computern, zum Beispiel die Angst, Fehler zu machen oder Daten zu verlieren. Sie kann auch zu Technostress führen. Im Extremfall kann sich die IT-Angst zu einer "Technophobie" auswachsen, die einen Widerstand gegen die Nutzung von Technologie überhaupt beinhaltet und einen Mangel an Informationen über Technologie und digitale Kompetenz hervorrufen kann.

Wie können Sie mit dieser IT- und Digitalangst umgehen?

Vorbereitet sein

Das ist nicht ohne Grund das Motto der Pfadfinder: Es ist ein kluger Rat. Wenn es um den Umgang mit Computern und den erforderlichen digitalen Fähigkeiten geht, sind viele von uns ein wenig eingeschüchtert, wollen nur die allerersten Grundlagen lernen und sich so wenig wie möglich mit dem technischen Kram beschäftigen. Das ist zwar verständlich, aber Sie können sich Stress ersparen, wenn Sie die Funktionsweise Ihrer Systeme durch das Lesen der Handbücher und vielleicht ein oder zwei Bücher über Computer kennenlernen und üben, üben, üben.

Back up Oft

Wenn Sie dies noch nicht in Ihre Routine eingearbeitet haben, sollten Sie unbedingt damit beginnen, Ihre Dateien regelmäßig zu sichern (wir empfehlen, dies einmal pro Woche zu tun), damit Sie bei größeren Schwierigkeiten nicht viel von Ihrer kostbaren Zeit und Arbeit verlieren.

Aber was passiert, wenn Sie keine Angst vor der Verwendung von Computern haben, aber Sie müssen ständig E-Mails checken und in den sozialen Medien aktiv sein und Sie haben das Gefühl, dass Sie ständig verbunden sein und interagieren müssen und wenn Sie das nicht tun, sind Sie verloren und die Folgen können negativ sein?

F	**Fear**
O	**Of**
M	**Missing**
O	**Out**

Wir alle haben eine Hassliebe zu E-Mails und sozialen Medien und manchmal beschweren wir uns, dass wir zu viele E-Mails bekommen, aber umgekehrt überprüfen wir sie viel zu oft aus Angst, etwas zu verpassen (FOMO). E-Mail wird oft durch mehrere E-Mail-Konten verschlimmert, die verschiedene Lebensbereiche abdecken, d.h. geschäftlich, privat und Interessen wie Sportverein / Kirchengruppe usw. Darüber hinaus haben Sie die Notwendigkeit, immer und immer wieder die sozialen Medien zu überprüfen, damit Sie sich nicht ausgeschlossen fühlen: damit Sie wissen, dass es Ihnen gut geht, damit Sie sich nicht ausgegrenzt fühlen.

Wie wird man mit seiner Fear of Missing Out fertig? FOMO ist eine selbst erfundene psychologische Folter und eine Ausgeburt der schlimmsten Fantasie unseres Geistes.

Hier sind Tipps, um Ihre mentale Gesundheit während des FOMO-Gefühls zu bewahren:

Benachrichtigungen

Seien Sie nett zu sich selbst und schalten Sie alle E-Mail-Ankündigungen auf Ihrem Desktop und Ihrem Mobiltelefon aus - Sie wollen die ständige Unterbrechung nicht. Dazu gehört auch das Abschalten der lästigen E-Mail-Zählung, die oft auf dem Bild Ihres E-Mail-Clients erscheint. Wenn Sie 100 ungelesene E-Mails sehen, wird das Ihren Stresspegel nur noch weiter in die Höhe treiben und Sie dazu verleiten, einen Blick auf Ihre E-Mails zu werfen.

Sie müssen nicht jede E-Mail sehen, auch nicht von wichtigen Stakeholdern; E-Mail ist keine direkte Nachrichtenübermittlung und nimmt Ihnen die Zeit für tiefgreifende Arbeit.

Wenn Sie schon dabei sind, schalten Sie alle unwichtigen Benachrichtigungen aus, einschließlich Facebook, Twitter und WhatsApp - das Ausschalten von Benachrichtigungen kann unglaublich befreiend sein. Verschieben Sie außerdem Ihre E-Mail-Anwendungen auf die zweite Seite Ihres Smartphones.

Gesunder Abstand

Sagen Sie nicht "ja" zu Veranstaltungen aus Angst, etwas zu verpassen, und halten Sie einen gesunden Abstand zu den abgeschirmten Versionen des Lebens anderer Menschen. Schreiben Sie eine Woche lang auf, wie viel Zeit Sie täglich damit verbringen, E-Mails, Texte oder soziale Medien zu lesen. Was könnten Sie sonst mit dieser Zeit anfangen? Die Angst, etwas zu verpassen, ist real und FOMO kann gefährlich sein, aber wenn Sie wissen, worauf Sie achten müssen, ist FOMO reversibel. Denken Sie an JOMO. Joy of Missing Out.

Prioritäten festlegen

Denken Sie daran, dass die Menge der Informationen, die Sie verarbeiten können, begrenzt ist, und konzentrieren Sie sich auf die Personen und Daten, die Sie wirklich interessieren oder die für Sie nützlich sein könnten.

Aktiv werden

Wenn Sie aus Angst vor dem, was Sie verpassen könnten, permanent vernetzt sind, verpassen Sie in Wirklichkeit das Leben. Anstatt zu schauen, was andere tun, und Ihre Freizeit damit zu verbringen, Ihre Aktivitäten zu fotografieren, aufzuzeichnen und zu veröffentlichen, genießen Sie gute Erlebnisse und teilen Sie sie mit denen, die Ihnen wichtig sind.

2.3. Smartes Verbraucherkonzept

Wenn Sie das Wort "konsumieren" hören - wohin gehen Ihre Gedanken? Wahrscheinlich denken Sie zuerst an Essen und was Sie essen. Um fair zu sein, ist das gar nicht so abwegig. Beim Konsum geht es um mehr als das, was Sie in Ihren Mund stecken. Es geht darum, was Sie mit Ihrem Geld und Ihrer Zeit machen. Mit Ihrem Geld kaufen Sie Essen, Unterkunft, Kleidung, Spiele, Auto, Wissen, Rente usw. Ihre Zeit verbringen Sie damit, eine neue Fähigkeit zu erlernen oder die neuesten Nachrichten des Tages zu konsumieren. Diese Balance zwischen Schaffen und Konsumieren zu finden, kann schwierig sein. Wenn Sie die Balance richtig hinbekommen, führt das zu einer verbesserten finanziellen Leistungsfähigkeit.

Neue Technologien verändern die Art und Weise, wie Verbraucher handeln. Dank der Technologie werden die Verbraucher immer besser informiert, befähigt und anspruchsvoll. Bewaffnet mit Wissen, das sie aus einer Vielzahl von Quellen gesammelt haben, verwenden sie ihr Geld für die Waren und Dienstleistungen, die sie schätzen. Sie wollen auf eine Art und Weise interagieren, die sowohl relevant als auch zeitnah ist: relevant für das, was sie einkaufen, unabhängig davon, wo, wann und wie sie es einkaufen; und zeitnah in der Erfüllung ihrer Bedürfnisse. Kurz gesagt, die Verbraucher von heute werden immer intelligenter. Aber wie können Sie ein klügerer Konsument sein?

Verbraucher jeden Alters und in allen Teilen der Welt strömen in die sozialen Medien. Soziale Medien zu verstehen ist nicht mehr optional; es ist ein Muss, um ein kluger Konsument zu sein. Die Mediensättigung erfordert es, als Verbraucher aktiver zu werden, zum Teil, um die Datenflut zu bewältigen, die jeden Tag über uns hereinbricht, aber auch, um informierte Urteile über die Bedeutung dessen zu fällen, was wir sehen..

Was sind die besten Wege, um "Fake News" zu bekämpfen und Informations- und Digitalkompetenzen zu entwickeln? Die Verbreitung von Fake News in den letzten Jahren wurde von einer Vielzahl von Empfehlungen begleitet, wie man damit umgehen kann. Die Fähigkeiten zur Bekämpfung von Fehlinformationen sind in der Tat die Fähigkeiten, die Sie entwickeln müssen. Ihre Herausforderung besteht darin, darüber nachzudenken, wie Faktoren außerhalb der Quelle selbst, wie die Identität des Autors, das Publikum und der Zweck, subtile Verzerrungen hervorrufen können. Der Kampf gegen "Fake News" erfordert also, dass Sie Ihr Gehirn auf eine anstrengendere Art und Weise trainieren, nicht nur mit Verständnis, sondern auch mit Unterscheidungsvermögen lesen - kurz gesagt, kritisches Denken auf das anwenden, was Sie lesen und kaufen.

Hier sind einige Empfehlungen, wie man im digitalen Zeitalter ein klügerer Konsument sein kann:

1. **Beginnen Sie mit dem Wissen, dass es online alles geben kann - und gibt**

   Das bedeutet, dass das Echte neben dem Falschen existiert, das Gute neben dem Bösen, das Legale neben dem Illegalen und alles dazwischen. Das Internet kann ein

Raum voller Träume sein und es ist auch ein Ort, an dem man den empfindlichsten Teil der gesellschaftlichen Bestie sehen kann. Es kann voller Chancen, Annehmlichkeiten und Vergnügen sein; es kann aber auch ein unredlicher Ort sein, der darauf wartet, zu betrügen, aufzuhetzen, unmoralisch zu sein und zu entwürdigen. Vorsicht für den Käufer, mal eine Million. Je mehr Sie die Dualität des Internets erkennen, desto mehr werden Sie es offensichtlich für das sehen, was es ist, und auch für alles, was es nicht ist.

2. **Seien Sie Ihr eigener Forscher**

   Jeder, der online ist, kann technisch gesehen ein "Vordenker" sein, aber es liegt an uns, ob wir uns entscheiden, diesen konkreten Personen genug Macht zu geben, um wirklich diesen Sockel als "Geführte" zu erhalten. Wir alle sind Anhänger von sozialen Influencern, Persönlichkeiten oder Marken, die wir nachahmen wollen, oder denen wir Einfluss auf unsere Gedanken oder Kaufentscheidungen erlauben. Nur weil sie Informationen online veröffentlichen, bedeutet das nicht, dass sie eine Quelle für gültige Informationen sind - das ist keine 1:1-Gleichung. Was Sie online konsumieren, sollte immer hinterfragt, recherchiert und auf Fakten geprüft werden.

3. **Überlegen Sie, wie Ihre Daten verwendet werden**

   Je mehr Daten Sie online zur Verfügung stellen, desto mehr gezielte Werbung erhalten Sie. Seien Sie sich aber bewusst, dass neben den Daten, die Sie anbieten, auch andere private Informationen aus verschiedenen Quellen extrahiert werden. Denken Sie zum Beispiel gründlich nach, bevor Sie Online-Quizern erlauben, auf Ihre Profilinformationen zuzugreifen, zu denen Ihr Geburtsdatum, Ihre Telefonnummer, Ihr Standort, Ihre Freundesliste, Ihr Arbeitsort usw. gehören.

4. **Schützen Sie sich und Ihre Informationen**

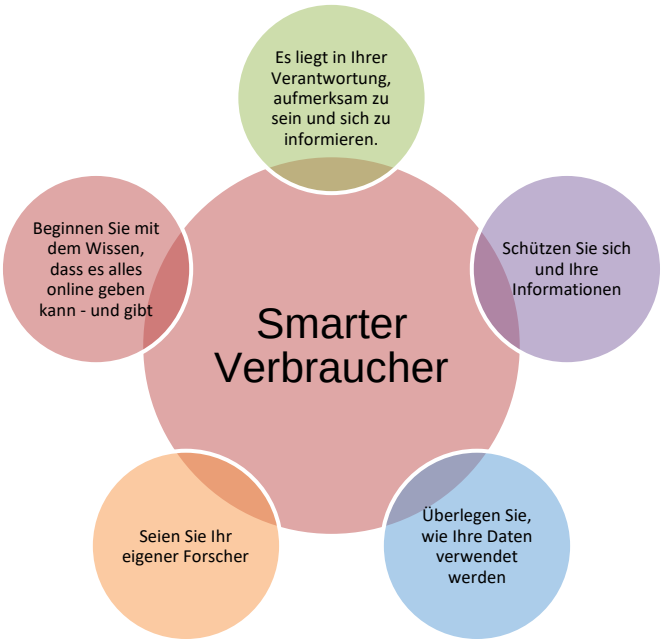
   Das Teilen oder Überteilen von Informationen kann dazu führen, dass Sie lästige Werbung für Dinge erhalten, die Ihnen wichtig erscheinen, oder schlimmer noch, es kann dazu benutzt werden, Sie zur Bildung bestimmter Meinungen zu manipulieren, Geld auszugeben oder Ihren Namen als Befürworter von Dingen hinzuzufügen, die Sie vielleicht nicht ganz verstehen oder unterstützen.

5. **Es liegt in Ihrer Verantwortung, aufmerksam zu sein und informiert zu bleiben**

   Es ist leicht, die Geschehnisse ignorieren zu wollen oder sich einzureden, dass man sich darauf verlassen kann, dass andere über die Änderungen bei der Internetnutzung, den Datenschutzgesetzen und den Benutzervereinbarungen der Plattformen auf dem Laufenden bleiben. Wenn Sie jedoch weiterhin die wertvollen Teile des Internets nutzen, müssen Sie akzeptieren, dass Sie als Gegenleistung für diese Vorteile ein gewisses Maß an Verantwortung tragen.

Unsere moderne Gesellschaft ist viel bewusster geworden, was Produkte und Dienstleistungen angeht, die man kaufen kann. Hochintelligente Werbung und Marketing überzeugen uns, dass wir diesen Diamantring, das neueste Telefon oder das Spielzeug für die Sendungen, die unsere Kinder im Fernsehen sehen, brauchen. Dies zu erkennen, ist ein Argument für das Einüben guter Gewohnheiten.

Abbildung 2.2. Smarter Verbraucher (Quelle: Eigene Ausarbeitung)



2.4. Kritisches Denken und Bewertungstechniken

Die Nutzung des Internets ist wahrscheinlich für viele von Ihnen eine tägliche Aktivität, aber manchmal ist es so selbstverständlich, dass wir nicht darüber nachdenken, was den Informationen zugrunde liegt, die wir nutzen. Wir leben heute in einer Zeit, in der Informationen weithin verfügbar sind. Wann immer Menschen mit einer Frage konfrontiert werden, ist ihre Standardreaktion "Googeln Sie es", anstatt nach einer Antwort zu grübeln. Dies steht in krassem Gegensatz zu dem, was früher geschah, als Bücher die Hauptinformationsquelle waren. Heutzutage ist Ihr kritisches Denken ein Anhaltspunkt, wenn es darum geht, die digitalen Informationen, die uns umgeben, zu analysieren.

Es gibt viele Definitionen von kritischem Denken, in seiner grundlegendsten Form geht es darum, in der Lage zu sein, für sich selbst zu denken. Um kritisch denken zu können, müssen Sie in der Lage sein:

1. Informationen und Argumente prüfen und bewerten
2. Muster und Verbindungen sehen
3. Identifizieren und erstellen Sie aussagekräftige Informationen

Jemand mit Fähigkeiten zum kritischen Denken kannJemand mit Fähigkeiten zum kritischen Denken kann:

1. Verstehen Sie die Verbindungen zwischen Ideen.
2. Bestimmen Sie die Bedeutung und Relevanz von Argumenten und Ideen.
3. Argumente erkennen, aufbauen und einschätzen.
4. Inkonsistenzen und Fehler in der Argumentation erkennen.
5. Probleme konsequent und systematisch angehen.
6. Über die Rechtfertigung ihrer eigenen Annahmen, Überzeugungen und Werte reflektieren.

Abbildung 2.3. Kritisches Denken

Wahrscheinlich haben Sie bereits Übung im kritischen Denken aus anderen Lebensbereichen, z. B. bei der Entscheidung, welches Telefon oder welchen Computer oder welches Auto Sie kaufen, wo Sie wohnen oder sogar, was Sie zu einem bestimmten Anlass anziehen sollen. In jeder Situation tun Sie wahrscheinlich nicht einfach das, was jemand anderes Ihnen sagt, sondern Sie treffen eine Entscheidung, die auf einer Reihe von Faktoren basiert. Kritische Fähigkeiten in Ihren digitalen Fertigkeiten anzuwenden bedeutet, Ihre Fähigkeit zu nutzen, digitale Informationen zu finden, zu bewerten, zu verwalten, zu kuratieren, zu organisieren und zu teilen. Darüber hinaus ist dies die Fähigkeit, digitale Informationen für akademische und berufliche Zwecke zu interpretieren und digitale Informationen in verschiedenen Umgebungen zu überprüfen, zu analysieren und neu zu präsentieren. Eine kritische Herangehensweise an die Bewertung von Informationen hinsichtlich ihrer Herkunft, Relevanz, ihres Wertes und ihrer Glaubwürdigkeit. Ein Verständnis für die Regeln des Urheberrechts und offene Alternativen, z. B. Creative Commons; die Fähigkeit, digitale Werke in verschiedenen Kontexten angemessen zu referenzieren.

Eines der wichtigsten Elemente, um online zu sein, ist die Fähigkeit, kritisch wahrzunehmen, woher Inhalte kommen und wer sie verfasst hat. Sie sollten in der Lage sein, Fragen zu stellen, die es Ihnen ermöglichen, den Kontext besser zu verstehen.

Bezogen auf Ihre kritische Fähigkeit ist es wichtig, die Fähigkeit, digitale Daten in Tabellenkalkulationen, Datenbanken und anderen Formaten zu sammeln, zu verwalten, darauf zuzugreifen und sie zu nutzen sowie Daten durch das Ausführen von Abfragen, Datenanalysen und Berichten zu interpretieren: Ihre Datenkompetenz und die Praktiken der persönlichen Datensicherheit. Ein Verständnis dafür, wie Daten im beruflichen und

öffentlichen Leben verwendet werden; von rechtlichen, ethischen und Sicherheitsrichtlinien bei der Datenerfassung und -nutzung; von der Natur von Algorithmen; und davon, wie personenbezogene Daten erfasst und verwendet werden können. Sie müssen kein Experte oder Fachmann für Daten sein, aber Sie müssen sich ihrer Existenz und der Gefahren, die ihr Missbrauch mit sich bringen kann, bewusst sein.

Ein weiterer wichtiger Faktor ist Ihre Fähigkeit, Botschaften in einer Reihe von digitalen Medien - Text, Grafik, Video, Animation, Audio - kritisch zu rezipieren und darauf zu reagieren sowie Medien zu kuratieren, neu zu bearbeiten und wiederzuverwenden und dabei den Urhebern die gebührende Anerkennung zu zollen. Eine kritische Herangehensweise an die Bewertung von Medienbotschaften in Bezug auf ihre Herkunft und ihren Zweck. Ein Verständnis der digitalen Medien als soziale, politische und pädagogische Werkzeug, und der digitalen Medienproduktion als technische Praxis.

Wenn es darum geht, digitale Inhalte zu bewerten, möchten Sie nach den besten verfügbaren digitalen Inhalten suchen. Sie möchten zum Beispiel Inhalte vermeiden, die einfach nur eine elektronische Version des Lehrbuchs ohne Mehrwert sind. Bei der digitalen Kompetenz geht es darum, digitale Inhalte auf sinnvolle und verantwortungsvolle Weise zu finden, zu bewerten, zu nutzen und zu erstellen. Sie erfordert Denkvermögen und technische Fähigkeiten.

Wenn man bedenkt, dass es bei der Suche nach digitalen Inhalten darum geht, verschiedene Suchstrategien einzusetzen, um qualitativ hochwertige Informationen zu finden, mehrere Suchmaschinen zu verwenden, um persönliche Filterblasen herauszufordern, schriftliche, visuelle und Audio-Ressourcen zu verwenden, um auf verschiedene Arten durch Informationen zu navigieren, sammelt man eine Reihe von Informationen, die dann ausgewertet werden können, um Ihren Anforderungen zu entsprechen.

Ein weiterer wichtiger Punkt ist, dass Sie, bevor Sie mit der Suche nach relevanten digitalen Inhalten beginnen, überlegen müssen, was die Frage ist, die Sie zu beantworten versuchen, oder das Thema, das Sie erforschen wollen, welche Informationen Sie bereits haben, welche Informationen Sie benötigen, welche Art von Informationen Sie benötigen, z. B. einen Überblick, eine detaillierte Analyse/Recherche oder Statistiken, wie viele Informationen Sie benötigen - welche Lücken es in Ihrem Wissen gibt.

Im heutigen digitalen Zeitalter kann jeder beliebige Informationen auf seinen Websites, Social-Media-Plattformen und anderen Online-Foren verbreiten. Leider überprüfen diejenigen, die nach parallelen Informationen suchen, nicht wirklich die Authentizität der Informationen. Infolgedessen werden Propaganda und falsche Informationen oft als die Wahrheit ausgelegt, was zu Entscheidungsproblemen führt. Es gibt keinen Standard für die Verifizierung der Informationen.

Wie kann man effektiv nach digitalen Inhalten suchen? Mit präzisen Schlüsselwörtern und Suchstrategien finden Sie bessere Ergebnisse. Überlegen Sie sich Schlüsselwörter aus Ihrer Fragestellung oder Ihrem Thema, auch Synonyme, Wörterbücher und ein Thesaurus sind

hilfreich, um eine Liste von Schlüsselwörtern zu erstellen. Schauen Sie sich die Frage oder das Thema an, zu dem Sie Informationen wünschen, und wählen Sie die relevanteste Quelle für Ihre Suche aus, z. B. Suchmaschine(n) und/oder Online-Datenbanken, und versuchen Sie, verschiedene Schlüsselwörter und Suchtechniken zu verwenden, um Ihre Suche zu erweitern oder einzugrenzen.

Zu den gängigen Suchtechniken für das Internet gehören:

Wörter von der Suche ausschließen: Setzen Sie - vor ein Wort, das Sie auslassen möchten. Zum Beispiel, jaguar speed - Auto.

Suche nach einer exakten Übereinstimmung: Setzen Sie ein Wort oder eine Phrase in Anführungszeichen. Zum Beispiel: "höchstes Gebäude".

Suche in einem Zahlenbereich: Setzen Sie .. zwischen zwei Zahlen. Zum Beispiel: Kamera €50... €100.

Suchvorgänge kombinieren: Setzen Sie "ODER" zwischen die einzelnen Suchanfragen. Zum Beispiel, Marathon ODER Rennen.

Suche nach einer bestimmten Seite: Setzen Sie "Seite:" vor eine Seite oder Domain. Zum Beispiel: Seite: youtube.com oder Seite:. gov.

Suche nach verwandten Websites: Setzen Sie " verwandt:" vor eine Webadresse, die Sie bereits kennen. Zum Beispiel: verwandt: time.com.

(Quelle: Refine web searches, Google)

Die meisten Informationen, die man im Internet findet, haben einen versteckten Grund. Die Firmen und Autoren, die die Informationen ins Internet stellen, versuchen wahrscheinlich, den Lesern etwas zu verkaufen. Andere sind Propagandisten, die versuchen, die Denkweise des Lesers zu beeinflussen. Kritisches Denken hilft uns, Probleme zu durchdenken und die richtigen Informationen bei der Entwicklung von Lösungen anzuwenden. Es ist wichtig, dass das digitale Zeitalter lernt, sachliche und gefälschte Informationen zu unterscheiden. Außerdem ist es gut, dass Informationen aus verschiedenen Online- und Offline-Quellen stammen, damit sie korrekt sind und genügend Fakten enthalten.

Fragen zu stellen ist immer eine gute Idee. Es wird Sie zu einem besseren Lerner und Denker machen. Kritisches Hinterfragen bedeutet, tiefer in Ihre Fragestellung einzusteigen und nicht nur das Wer, Was, Wann, Wo, Warum und Wie zu fragen, sondern stattdessen beschreibendere Fragen zu stellen wie "Wem nützt das?" "Was steht dem Handeln im Weg?" "Warum ist das schon so lange so?" oder "Wie können wir das zu unserem Besten ändern?"

So sagt Jesse R. Sparks:

> *"Wir müssen die digitalen Informationskompetenzen entwickeln, die notwendig sind, um den Wahrheitsgehalt, die Relevanz, die Glaubwürdigkeit und die*

Argumentationsqualität von Informationen zu bewerten, um effektiv zu lernen, Probleme zu lösen und Entscheidungen in der heutigen Welt zu treffen."

2.5. Kulturelle Wahrnehmung und soziales Verständnis

Digitale Technologien haben die Kulturszene tiefgreifend verändert. Diese Technologie ist in unser Leben eingedrungen, man kann jetzt mit seinem Smartphone oder Gerät einkaufen, Bankgeschäfte erledigen, kommunizieren, soziale Kontakte knüpfen, browsen und mit anderen zusammenarbeiten. In diesem Sinne müssen wir wissen, dass digitale Kultur nicht nur mit der Digitalisierung analoger Begriffe verbunden ist, sondern sich auf einen hochdynamischen Raum bezieht, in dem multimediale Modalitäten, Cross Media, Transmedia, Augmented Reality und Virtual Reality koexistieren. Allerdings ist die digitale Szene nicht ohne Risiken.

Die neuen Technologien haben den Raum, die Zeit, die Beziehungen und die Arten der Kommunikation verändert, die nach wie vor mit den anderen Wissensgebieten einer Kultur koexistieren. Es ist klar, dass die neuen Technologien große Vorteile in Bezug auf den Zugang zur Kultur mit sich bringen und es ist auch offensichtlich, dass es im digitalen Zeitalter viel mehr kulturelle Angebote gibt, als die Nutzer früher gewohnt waren.

Digitale Kultur bezieht sich auf das Wissen, die Überzeugungen und die Praktiken von Menschen, die in digitalen Netzwerken interagieren, die Kulturen der realen Welt nachbilden oder neue kulturelle Denkweisen und Praktiken schaffen, die in digitalen Netzwerken heimisch sind. Digitale Kultur ist das Internet, Transhumanismus, künstliche Intelligenz, Cyber-Ethik, Sicherheit, Datenschutz und Politik. Sie ist Hacking, Social Engineering und moderne Psychologie (Digital Culturist, 2015).

Mobiltelefone werden sowohl von Jugendlichen als auch von Erwachsenen ausgiebig genutzt. Websites wie YouTube und Wikipedia sind für viele Menschen die erste Anlaufstelle, wenn sie Informationen zu einem ausgewählten Interessengebiet suchen. Fernsehen, Filme und Musik werden auf Computern, MP3-Playern und online gespeichert und abgerufen. Online-Shopping und Online-Banking haben an Bedeutung gewonnen, und staatliche Dienstleistungen sind zunehmend internetbasiert. E-Mail ermöglicht die sofortige Kommunikation zwischen Menschen auf der ganzen Welt. Sowohl Online- als auch Offline-Spiele spielen im Leben vieler Menschen eine wichtige Rolle, und Web 2.0-Technologien wie Social-Networking-Sites ermöglichen es Menschen, zusammenzuarbeiten, indem sie Online-Inhalte teilen und bearbeiten.

Die heutige Gesellschaft, die oft als "Informationszeitalter" bezeichnet wird, ist durch die rasante Entwicklung von Kommunikations- und Informationsressourcen gekennzeichnet.

Kulturelles und soziales Verständnis stattet Sie mit einer Sprache und einem Kontext für Ihre digitale Kompetenz aus. Sicherlich ist die Entwicklung eines kulturellen und sozialen Verständnisses entscheidend dafür, dass Menschen nicht nur sozial und kulturell, sondern auch politisch, wirtschaftlich und intellektuell einen Beitrag leisten können. Sie müssen

erkennen, dass es bestimmte soziale, kulturelle und historische Einflüsse gibt, die Ihr Verständnis und Ihr Lernen prägen.

Wie sehr kann sich die Kultur verändern, wenn bestimmte Praktiken online übertragen werden? Wie oft können aktuelle kulturelle Überzeugungen und Erwartungen in eine andere Realität transportiert werden? Wir denken häufig an Information und Kommunikation in einer technischen und instrumentellen Weise - als Daten und Datenübertragung. Doch Information und Kommunikation sind auch soziale Phänomene.

Die Verbreitung von Technologie wirkt sich nicht nur auf den sozialen Klassenstatus aus, sondern auch auf die Bildung sozialer Klassen, die Aufteilung und Aspekte, die zu jeder Gruppe beitragen. Dennoch verstehen viele Personen weniger, wo sie innerhalb der sozialen Klasse fallen, da digitale Kulturen die Arten des Kapitals durcheinander bringen. Dieser Mangel an klarer Identifikation oder Verständnis schmälert nicht die Bedeutung der Klassenhierarchie, da der digitale Raum Inhalte durch Aspekte wie Klasse kategorisiert und Arbeiterfragen durch ein solches Versehen oder einen Mangel an digitalem sozialem Klassenzusammenhalt nicht klar angesprochen werden.

Die digitale Kultur und die Technologie haben neue Möglichkeiten geschaffen, die soziale Klasse theoretisch zu sehen, einschließlich der immateriellen Arbeit, der digitalen Arbeit, der Informations- und Kulturarbeit, des "Konzepts der freien Arbeit unter den Bedingungen der New Economy sowie der inzwischen berühmten Begriffe der sozialen Fabrik" (Qiu, 2018)[4].

Der Aufbau einer globalen Online-Kultur über neue Medien sollte sich darauf konzentrieren, wie radikale Veränderungen von demokratischen Regeln und Prinzipien übernommen werden. Digitale Technologien, vor allem Online-Räume, bieten die Möglichkeit für viele neue Formen der Interaktion. Zunehmend werden diese Interaktionen durch unterschiedliche Darstellungsformen wie Bilder und Töne vermittelt. Die Fähigkeit, diese multimodalen Texte zu entschlüsseln, erfordert ein Verständnis der sozialen und kulturellen Praktiken, die ihre Entstehung umgeben.

Wir unterscheiden die Kulturepochen nach der verwendeten Kommunikationstechnologie. In der mündlichen Kultur konnte der Wissenstransfer nur in direkter Kommunikation erfolgen. In der Schriftkultur konnten bestimmte Arten von Wissen oder die Erinnerung an eine bestimmte Person bewahrt werden und schriftliche Nachrichten konnten durch den Raum geschickt und für die Zukunft aufgezeichnet (und bewahrt) werden. Die Presse- und Rundfunkkultur ermöglichte die massenhafte Verbreitung von Nachrichten aus zentralisierten Quellen. Heutzutage können wir uns auf Konzepte wie digitale Kultur, Internet und seine partizipatorische Natur, Konvergenz, Ambient Intelligence usw. beziehen.

Die Auswirkung der Kommunikationstechnologien auf die Kultur ist wichtig, weil die Art und Weise, wie wir sie nutzen, Veränderungen im Wesen unserer Kultur- und Kommunikationsmodelle bewirken kann. Doch obwohl die digitalen Werkzeuge Ihre

[4] Qiu, Jack Linchuan. 2018. "China's Digital Working Class and Circuits of Labor." Communication and the Public 3 (1): 5–18. https://doi.org/10.1177/2057047318755529.

Möglichkeiten intensivieren, hat das exponentielle Wachstum des Inhaltsangebots aus aller Welt paradoxerweise manchmal den gegenteiligen Effekt: Es führt zu einer Überfülle, die Ihre Aufmerksamkeit ablenken kann.

Denken Sie auf der Grundlage dieser vorgestellten Ideen nach:

1. Inwieweit verbessern die digitalen Bürger ihre Kommunikationsstile und -fähigkeiten über die neuen Medien weiter?
2. Welche Art von authentischen Online-Erfahrungen sind mit der Entwicklung von Kommunikationsstilen und -fähigkeiten über neue Medien verbunden?
3. Wie sind die Kommunikationsstile und -fähigkeiten der digitalen Bürger über die neuen Medien verteilt?
4. Was sind die Auswirkungen von Kommunikationsstilen und -fähigkeiten über neue?

Individuen können zu aktiven Teilnehmern an ihren Wissenskonstruktionen werden, statt zu passiven Empfängern. In diesem konstruktivistischen Milieu können digitale Bürger über neue Medien an komplexen globalen Projekten arbeiten.

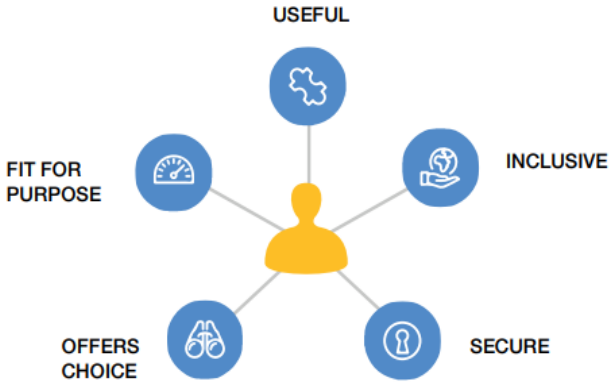
2.6. Erstellung, Verwaltung und Auswirkungen von virtuellen Identitäten

Unsere Identität ist im wahrsten Sinne des Wortes, wer wir sind, und sich online mit einem persönlichen Blog, einer Webseite oder einem sozialen Netzwerk zu präsentieren, erfordert eine gezielte Auswahl von Text, Bildern, Grafiken und Audio, um einen Eindruck zu erzeugen. Dies geschieht nicht zufällig. Die Online-Welt verlangt von den Menschen, dass sie sich selbst in die Existenz schreiben und so bieten ihre Profile die Möglichkeit, den beabsichtigten Eindruck durch Sprache, Bilder und Medien zu gestalten.

Auf dem Jahrestreffen des Weltwirtschaftsforums in Davos 2018 wurde eine erste Reihe von fünf Elementen identifiziert, die eine gute Identität erfüllen muss:

1. Fit für den Zweck. Gute digitale Identitäten bieten eine verlässliche Möglichkeit für Einzelpersonen, Vertrauen in die Person aufzubauen, die sie vorgeben zu sein, ihre Rechte und Freiheiten auszuüben und/oder ihre Lesbarkeit für den Zugang zu Dienstleistungen zu demonstrieren.
2. Inklusiv. Inklusive Identität ermöglicht es jedem, der es braucht, eine digitale Identität aufzubauen und zu nutzen, frei von der Gefahr der Diskriminierung aufgrund seiner identitätsbezogenen Daten und ohne mit Authentifizierungsprozessen konfrontiert zu werden, die ihn ausschließen.
3. Nützlich. Nützliche digitale Identitäten bieten Zugang zu einer breiten Palette nützlicher Dienste und Interaktionen und sind einfach einzurichten und zu nutzen.
4. Bietet Wahlmöglichkeiten. Der Einzelne hat die Wahl, wenn er sehen kann, wie Systeme seine Daten verwenden, und wählen kann, welche Daten er für welche Interaktion, mit wem und für wie lange teilt.
5. Sicher. Sicherheit umfasst den Schutz von Personen, Organisationen, Geräten und Infrastruktur vor Identitätsdiebstahl, unbefugter Datenweitergabe und Menschenrechtsverletzungen.

Abbildung 2.4. Fünf Elemente guter Identität



Ressource: Insight Report - Identität in einer digitalen Welt Ein neues Kapitel im Gesellschaftsvertrag. Weltwirtschaftsforum (Sep 2018)

http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Wenn Sie Ihren Namen googeln würden, was würden Sie finden? Wenn Sie bedenken, dass Ihre Online-Identität nicht dasselbe ist wie Ihre reale Identität, weil die Eigenschaften, die Sie online repräsentieren, sich von den Eigenschaften unterscheiden, die Sie in der physischen Welt repräsentieren, haben Sie vielleicht schon von der Idee eines digitalen Fußabdrucks gehört. Dies bezieht sich auf die Spuren Ihrer persönlichen und beruflichen Informationen, die in Online-Netzwerken hinterlassen werden - sowohl absichtlich als auch unabsichtlich. Manchmal hören Sie vielleicht den Ratschlag, nichts zu veröffentlichen, von dem Sie nicht möchten, dass es jemand sieht. Das macht Sinn, aber denken Sie auch daran, was Sie zukünftigen Generationen zeigen möchten. Wenn Sie Material online stellen, geben Sie die Kontrolle darüber ab. Sie sollten also sicher sein, dass es Ihrem Ruf oder Ihrer Glaubwürdigkeit nicht schadet. Selbst wenn Sie sich später entscheiden, es zu löschen, gibt es keine Garantie, dass es nicht bereits jemand ohne Ihr Wissen kopiert oder weitergegeben hat. Leider gibt es Menschen, die es genießen, andere in digitalen Räumen zu schikanieren, oder die Sie ausnutzen werden, wenn sie die Gelegenheit dazu haben.

Was müssen Sie bei der Erstellung und dem Schutz Ihrer Online-Identität beachten?

Es gibt eine Vielzahl von Möglichkeiten, wie Sie soziale Online-Medien bei der Arbeitssuche nutzen können:

1. Soziale Netzwerkseiten wie Facebook, Twitter und LinkedIn
2. Teilnahme an Online-Foren und Diskussionslisten
3. Persönliches Blog erstellen

Bei der Teilnahme an sozialen Medien ist es immer ratsam, sich auf professionelle Weise zu präsentieren, und es ist auch wichtig, Ihre persönlichen Informationen zu schützen.

Einige grundlegende Tipps, die Sie beachten sollten, wenn Sie online sind:

1. Das Internet ist ein öffentlicher Raum. Wenn Sie online posten, verzichten Sie auf Ihr Recht auf Privatsphäre.
2. Online-Inhalte können dauerhaft sein - sie können durchsucht werden; sie können viele Menschen erreichen und sie können Ihren Standort offenlegen.
3. Wenn Sie Informationen herausgeben, stellen Sie sicher, dass Sie wissen, wie sie verwendet werden.
4. Geben Sie sensible oder vertrauliche Informationen nur über sichere Websites weiter
5. Nutzen Sie soziale Netzwerke mit Bedacht; passen Sie Ihre Privatsphäre-Einstellungen an Ihr eigenes Komfortniveau an
6. Trotz aller Vorsichtsmaßnahmen sollten Sie sich nicht scheuen, mitzumachen und sich zu verbinden!

Was ist mit Ihrer beruflichen Identität?

Heutzutage wollen Arbeitgeber wissen, wen sie eingestellt haben, und viele Personalverantwortliche überprüfen die sozialen Medien von potenziellen Mitarbeitern. Soziale Netzwerke sind eine gute Möglichkeit, Ihre Interessen, Fähigkeiten und den Bedarf an Arbeit zu verbreiten. Laut einer Umfrage aus dem Jahr 2017 nutzen 70 Prozent der Arbeitgeber soziale Medien, um Kandidaten vor der Einstellung zu überprüfen. Außerdem nutzen 69 Prozent der Arbeitgeber Online-Suchmaschinen wie Google, Yahoo und Bing, um Kandidaten zu recherchieren. Bauen Sie Ihre öffentlichen Online-Profile auf und verwalten Sie sie so, dass potenzielle Arbeitgeber positive und professionelle Informationen über Sie finden, das ist ein wichtiger Punkt bei der Jobsuche.

Facebook, LinkedIn, Twitter, Pinterest (und jede andere Online-Community) können hervorragende Werkzeuge für das Networking, die Suche nach Ressourcen und die Förderung persönlicher oder beruflicher Interessen sein - aber nur, wenn sie intelligent und absichtlich eingesetzt werden. Der erste Eindruck entsteht, bevor Sie jemanden überhaupt physisch treffen. Genau wie das Sprichwort "Ihr Ruf eilt Ihnen voraus", eilt Ihr Online-Ruf heute oft persönlichen Treffen und Vorstellungsgesprächen voraus.

Sie müssen bedenken, dass Online-Reputationsmanagement eines der Dinge ist, die besser funktionieren, wenn Sie es implementieren, bevor Sie es tatsächlich brauchen.

Die 5 besten Tipps & Tricks

1. **Googeln Sie sich selbst**. Es mag eitel klingen, aber in diesem Fall sind Sie entschuldigt - Sie müssen wissen, was die Leute sehen, wenn sie nach Ihnen suchen.
2. **Wenn Sie es nicht benutzen - löschen Sie es**. Suchen Sie alle alten Profile und alle nicht mehr verwendeten Konten, die Sie nicht mehr verwenden, und löschen Sie sie.
3. **Denken Sie daran, dass es mehr als eine Seite bei Google gibt**. Stellen Sie sicher, dass Sie so viel von Google wie möglich durchsehen, falls Sie etwas übersehen.

4. **Führen Sie einen Frühjahrsputz in Ihrer Historie durch**. Es wird einige Zeit in Anspruch nehmen, aber gehen Sie durch Ihr Twitter/Instagram/Facebook und überprüfen Sie jeden Beitrag und löschen Sie alle, die Sie in einem schlechten Licht darstellen.
5. Werden Sie die Beweise los. Nehmen Sie alle Bilder herunter, die Sie schlecht aussehen lassen, und bitten Sie Ihre Freunde, das Gleiche zu tun.

Was nun?

Denken Sie darüber nach, was Sie posten. Sie haben so viel Zeit damit verbracht, Ihren digitalen Fußabdruck zu säubern. Machen Sie diese gute Arbeit nicht zunichte, indem Sie in alte Gewohnheiten abrutschen und seien Sie vorsichtig mit den Inhalten, die Sie teilen.

Verriegelung einschalten

Achten Sie darauf, Ihre Sicherheitseinstellungen auf Plattformen wie Facebook so zu verschärfen, dass nur Freunde Sie sehen können.

Seien Sie vorsichtig, wenn Sie die Hinzufügen-Taste drücken

Wir alle lieben einen neuen Facebook-Freund oder Twitter-Follower, aber seien Sie vorsichtig. Manchmal ist es nicht klug, Kollegen oder Dozenten in sozialen Medien hinzuzufügen. Es ist immer eine gute Idee, Ihr Privatleben, Ihre Privatsphäre zu wahren.

Tolle Inhalte erstellen

Tun Sie Dinge, die Sie gut aussehen lassen und machen Sie dies zu einem Teil Ihres digitalen Fußabdrucks. Wenn Ihr Chef auf Facebook geht, lassen Sie ihn ein Album mit Bildern finden, auf denen Sie sich freiwillig in der Gemeinde engagieren. Falls Sie es noch nicht nutzen - LinkedIn ist eine großartige Möglichkeit, all die tollen Dinge zu präsentieren, die Sie tun, und kann wie ein Online-Lebenslauf wirken.

2.7. Finanzielle Allgemeinbildung

Finanzielle Allgemeinbildung - eine Reihe von Kenntnissen und Fähigkeiten, die erforderlich sind, um finanzielle Informationen richtig zu verstehen, zu bewerten und zu interpretieren und auf dieser Grundlage solide finanzielle Entscheidungen zu treffen.

Finanzielle Kompetenz bedeutet nicht, dass ein Individuum eine spezielle Ausbildung in diesen Bereichen absolvieren muss, da das Leben selbst eine Schule der finanziellen Kompetenz ist (z. B. werden Fragen der persönlichen Budgetverwaltung von jedem täglich konfrontiert, Zahlungs- oder andere Finanzdienstleistungen werden von fast jedem auf einer täglichen Basis genutzt, usw).

Warum ist finanzielle Allgemeinbildung im täglichen Leben wichtig?

Finanzielle Kompetenz ist notwendig, damit der Einzelne in der Lage ist, seine persönlichen Finanzen effektiv zu verwalten, seine finanziellen Bedürfnisse, Möglichkeiten und Chancen optimal einzuschätzen, und sie hilft ihm, bessere finanzielle Lösungen zu finden (z. B. sein/ihr Einkommen mit den Ausgaben in Einklang zu bringen, zu sparen, ein zusätzliches Einkommen zu erwirtschaften, usw.). Um die besten Ergebnisse zu erzielen, sollten Finanzkompetenzen parallel zu anderen allgemeinen Kompetenzen entwickelt werden, wie z. B. digitales, soziales, politisches, wirtschaftliches, rechtliches Wissen usw.

Jeder Einzelne muss die grundlegenden Fakten über Finanzen verstehen, wie z. B. den Wert des Geldes, lernen, seine persönlichen Finanzen zu planen, seine finanziellen Verpflichtungen unter Kontrolle zu halten (z. B. keine finanziellen Verpflichtungen einzugehen, die über seine Möglichkeiten hinausgehen), seine Ausgaben zu überwachen und zu wissen, wie man unnötige Kosten reduziert oder eliminiert, eine angemessene Recherche durchzuführen, bevor man Investitionen tätigt (vermeiden Sie es, in unbekannte Bereiche zu investieren), nach Wegen zu suchen, um eine sichere Zukunft zu gewährleisten, sein Einkommen oder Vermögen zu schützen (z. B. Versicherungsleistungen in Anspruch zu nehmen, einen Pensionsfonds anzulegen) usw.

Finanzielle Bildung hilft auch, persönliche Daten und Vermögenswerte zu schützen. Eine finanziell gebildete Person ist eher in der Lage, Betrügereien oder andere betrügerische Aktivitäten (z. B. Phishing) zu erkennen, zu verstehen, wie wichtig persönliche Daten sind und wie sie vor unbefugter Nutzung durch Dritte geschützt werden müssen, um finanzielle Verluste zu vermeiden. Finanziell gebildete Personen sind in der Lage, die ihnen angebotenen Finanzdienstleistungen besser zu nutzen, deren Eignung für ihre Bedürfnisse sowie die damit verbundenen Risiken (z. B. investitionsbezogene Risiken) und die damit verbundenen Vorteile zu beurteilen.

Wie können Sie Ihr Finanzwissen verbessern und davon profitieren?

Der erste Schritt sollte darin bestehen, zu verstehen, dass es wichtig ist, über genügend finanzielle Kenntnisse zu verfügen und Interesse daran zu zeigen, solche Fähigkeiten zu erwerben.
Danach sollten Sie die folgenden Schritte durchführen (sofern Sie dies nicht bereits getan haben):

1. Bewerten Sie selbst, wie Ihre Finanzen derzeit verwaltet werden, und ermitteln Sie, was Sie an dieser Verwaltung verbessern und ändern möchten und was Ihre wichtigsten finanziellen Ziele sind.
2. Erstellen Sie Ihren Budgetplan und Ihre Sparstrategie.
3. Verfolgen Sie Ihre Ausgaben, bewerten Sie die Gebühren, die Sie für die Inanspruchnahme von Finanz- oder anderen Dienstleistungen zahlen, und überlegen Sie, wie Sie diese Kosten reduzieren können (z. B. ist die Inanspruchnahme und/oder Bezahlung von Dienstleistungen aus der Ferne in der Regel billiger, als wenn Sie dies physisch und/oder in bar erledigen; wenn Sie mehrere Kreditverträge mit verschiedenen Finanzinstituten haben, kann die Umfinanzierung dieser Kredite in einen einzigen die damit verbundenen Kosten sparen).
4. Schätzen Sie ein, welches Wissen Ihnen fehlt oder in welchem Bereich Sie Ihr Wissen vertiefen möchten und streben Sie solche Ziele an.
5. Konsultieren Sie regelmäßig Informationen. Es ist wichtig, dass Sie mit den Finanzinformationen, die Ihnen direkt zur Verfügung gestellt werden oder die Ihnen auf andere Weise zugänglich sind, gut vertraut sind. Wenn Sie unsicher sind, wie Sie diese Informationen verstehen oder in der Praxis anwenden sollen, können Sie jederzeit Hilfe in Anspruch nehmen (z. B. Beratung durch Dritte, Teilnahme an entsprechenden Schulungen oder Seminaren).
6. Erhöhen Sie Ihren Verdienst nicht nur durch Kosteneinsparungen, sondern auch durch die Erschließung alternativer Einkommensquellen (z. B. können Sie Erträge aus den Zinsen für platzierte Einlagen erhalten, Einkommen durch sichere Investitionen in zuverlässige gegenseitige Kreditplattformen oder Wertpapiere erzielen).
7. Sorgen Sie für Ihre eigene Sicherheit und die Ihres Eigentums (z. B. versichern Sie Ihre Gesundheit und Ihr Leben, Ihr Eigentum und oder Ihren Einkommensverlust, wählen Sie die richtige Pensionskasse);
8. Wenn Sie sich für eine finanzielle oder andere kostenpflichtige Dienstleistung entscheiden, prüfen Sie genau, ob Sie diese wirklich benötigen, machen Sie sich mit den Bedingungen vertraut, kalkulieren Sie den Nutzen und die damit verbundenen Risiken voraus. Wenn Sie z. B. die Aufnahme eines Kredits in Erwägung ziehen, schätzen Sie ab, wie viel Zinsen Sie zahlen werden und welche anderen Kosten mit dem Kredit verbunden sind (Sie sollten nur den Betrag aufnehmen, den Sie tatsächlich benötigen und nicht aus Ihrem vorhandenen Einkommen ansammeln können); schätzen Sie ab, ob Sie in der Lage sein werden, diesen Kredit termingerecht

zurückzuzahlen und / oder ob Sie keine Schwierigkeiten bei der Rückzahlung haben werden, wenn sich Ihre finanzielle Situation ändert (z. B. im Falle unvorhergesehener zusätzlicher Kosten); vergleichen Sie die Bedingungen mehrerer Kreditgeber und wählen Sie denjenigen, dessen Kreditbedingungen am besten zu Ihrer finanziellen Situation passen, usw.

9. Überwachen Sie die erzielten Ergebnisse und nehmen Sie die notwendigen Änderungen vor, und überprüfen Sie ggf. Ihr Budget und Ihre Sparpläne.

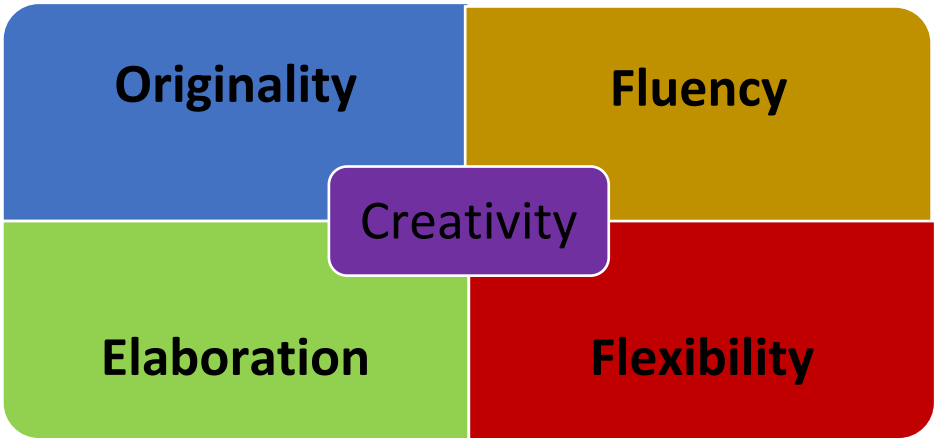
2.8. Kreativität und Fähigkeit zur Zusammenarbeit

"Kreativität hat eine wichtige Lücke in meinem Bücherregal gefüllt, wo es eigentlich schon immer hätte stehen sollen. Es gibt keine andere Herangehensweise an kreatives Denken wie diese: frisch, lebendig, weitreichend in seiner Wissenschaft, oft links und immer beunruhigend treffend."

Jo Shapcott, Dichter und Stipendiat des Royal Literary Fund

Sind Sie kreativ? Wie kreativ sind Sie? Können Sie noch kreativer werden? Das sind Fragen, die Sie sich selbst stellen können. Man kann lange darüber nachdenken oder reden, ohne sich in hochgradig verwickelte Fragen zu verstricken: darüber, ob nur bestimmte, singuläre Menschen kreativ sind oder ob hypothetisch jeder in irgendeiner Weise kreativ ist; und ob bestimmte Tätigkeiten, Kulturen oder Epochen kreativer sind als andere. Was ist überhaupt Kreativität? Denken Sie nur: Kreativität ist das, was passiert, wenn ein Individuum etwas produziert, das sowohl neu als auch angemessen, generativ oder einflussreich ist[5].

Abbildung 2.5. Die häufigsten Kriterien und Fähigkeiten von kreativen Menschen. (Quelle: Eigene Ausarbeitung)



1. **Flexibilität**: Hier wird die Fähigkeit erfasst, Grenzen zu überschreiten und entfernte Assoziationen herzustellen. Dies wird durch eine Reihe von verschiedenen Kategorien von generierten Ideen gemessen.

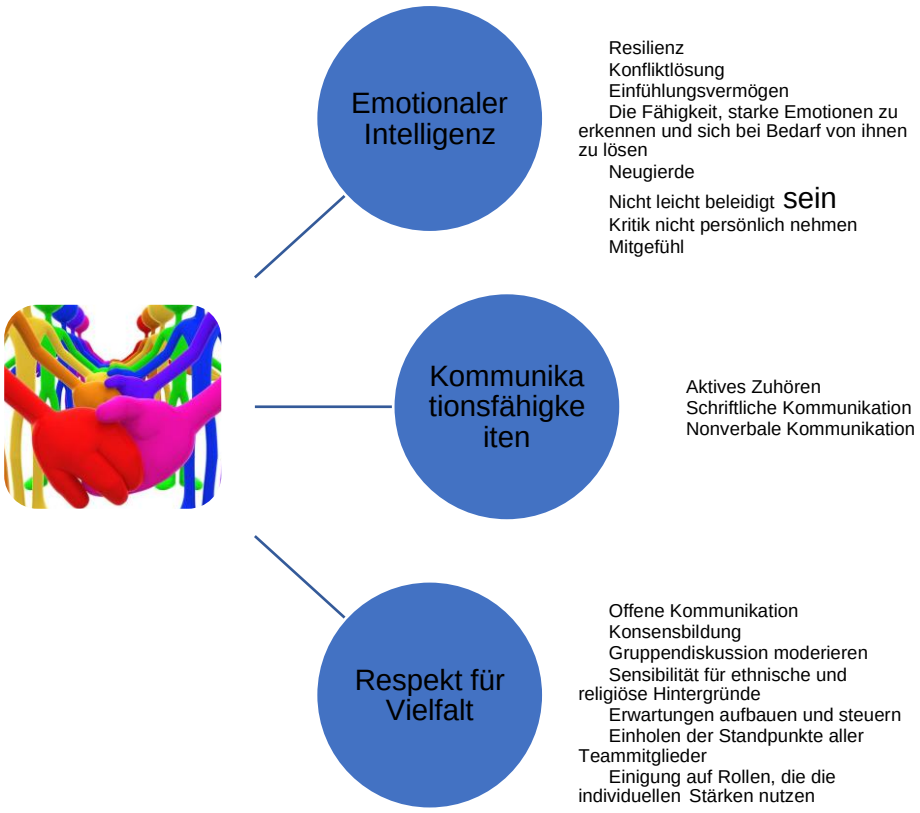
[5] Stokes, Patricia D. Creativity From Constraints: the Psychology of Breakthrough. New York: Springer Pub., 2006. Print. 1.

2. **Originalität**: Dies misst, wie statistisch anders oder neuartig die Ideen im Vergleich zu einer Vergleichsgruppe sind. Dies wird als Anzahl der generierten neuartigen Ideen gemessen.
3. **Geläufigkeit**: Hier wird die Fähigkeit erfasst, schnell auf viele verschiedene Ideen zu kommen. Gemessen wird dies an der Gesamtzahl der generierten Ideen
4. **Ausarbeitung**: Dies misst die Menge der Details, die mit der Idee verbunden sind. Die Ausarbeitung hat mehr damit zu tun, sich auf jede Lösung/Idee zu konzentrieren und sie weiter zu entwickeln.

Lernen beinhaltet das Hinterfragen, Verfeinern und Verbessern des Verständnisses, indem man zum Nachdenken angeregt wird. Um neue Konzepte zu verstehen und Perspektiven zu erweitern, müssen unsere Denkansätze manchmal kreativ, phantasievoll und lateral (unter Einbeziehung neuer Sichtweisen) sowie linear (unter Verwendung bestehender Denkmuster) sein. In diesem Sinne nutzen Sie Ihren Kreativitätsteil für die Entwicklung Ihrer digitalen CREW-Fähigkeiten. Sie sollten verstehen, wie Sie etabliertes Wissen in Frage stellen oder herausfordern können, um Ihr eigenes Verständnis zu formulieren, wobei die Vorstellungskraft eine wichtige Rolle spielen kann:

“Man kann nicht kreativ denken, wenn man nicht das Wissen hat, mit dem man kreativ denken kann. Kreativität stellt ein Gleichgewicht zwischen Wissen und der Befreiung von diesem Wissen dar" (Johnson-Laird, 1988, S.207, zitiert nach Sternberg, 2012, S.4).

Abbildung 2.6. Kollaboration Fähigkeiten (Quelle: Eigene Ausarbeitung)



Kollaborationsfähigkeiten ermöglichen es Ihnen, erfolgreich mit anderen auf ein gemeinsames Ziel hinzuarbeiten. Dazu gehört es, klar zu kommunizieren, anderen aktiv zuzuhören, Verantwortung für Fehler zu übernehmen und die Vielfalt der Menschen zu respektieren.

Kommunikationsfähigkeiten:

1. **Aktives Zuhören**: Aktives Zuhören geht über das Hören der Worte, die Ihre Kollegen sagen, hinaus. Es bedeutet, ohne zu urteilen zuzuhören und sicherzustellen, dass Sie die Bedeutung hinter dem, was sie sagen, verstehen. Wenn Sie etwas nicht verstehen, fragen Sie nach, und nehmen Sie sich die Zeit, das Gesagte zusammenzufassen, bevor Sie weitergehen.
2. **Schriftliche Kommunikation**: Ein Großteil der Zusammenarbeit findet schriftlich statt, vor allem, wenn Sie aus der Ferne arbeiten. Wir neigen dazu, uns auf nonverbale Hinweise zu verlassen, um Bedeutung zu vermitteln, daher ist es besonders wichtig, darauf zu achten, wie Nachrichten bei der schriftlichen Kommunikation empfangen werden könnten.
3. **Mündliche Kommunikation:** Was Sie in einer Teamumgebung sagen, ist entscheidend, aber wie Sie es sagen, ist genauso wichtig. Ihre Sichtweise kurz und bündig darzustellen und respektvoll zu widersprechen sind wesentliche Aspekte der verbalen Kommunikation.
4. **Nonverbale Kommunikation**: Nonverbale Kommunikation, wie Körpersprache und Tonfall, wirkt sich auf Ihre verbale Kommunikation aus. Die gleichen Worte, die auf zwei verschiedene Arten ausgesprochen werden, können für die Zuhörer zwei unterschiedliche Bedeutungen haben. Achten Sie darauf, was Sie sagen und wie Sie es sagen, wenn Sie eng mit Kollegen zusammenarbeiten.

Emotionale Intelligenz ist die Fähigkeit, die eigenen Emotionen zu identifizieren und zu managen, Emotionen bei anderen zu erkennen und angemessen zu reagieren, die eigenen Emotionen auf Aufgaben anzuwenden und ist eine der gefragtesten Soft Skills.

Einige Eigenschaften zur Förderung Ihrer emotionalen Intelligenz beinhalten:

1. Belastbarkeit
2. Konfliktlösung
3. Einfühlungsvermögen
4. In der Lage sein, starke Emotionen zu erkennen und sich bei Bedarf von ihnen zu lösen
5. Neugierde
6. Nicht leicht beleidigt sein
7. Kritik nicht persönlich nehmen

8. Mitgefühl.

In unserer universellen Wirtschaft arbeiten Sie möglicherweise mit Kollegen aus anderen Kulturen und Ländern zusammen. Es ist wichtig, über implizite Vorurteile nachzudenken, die Sie möglicherweise haben, damit Sie respektvoll mit Ihren Kollegen zusammenarbeiten und erfolgreich sein können.

Respekt für Vielfalt in einer kollaborativen Umgebung bedeutet:

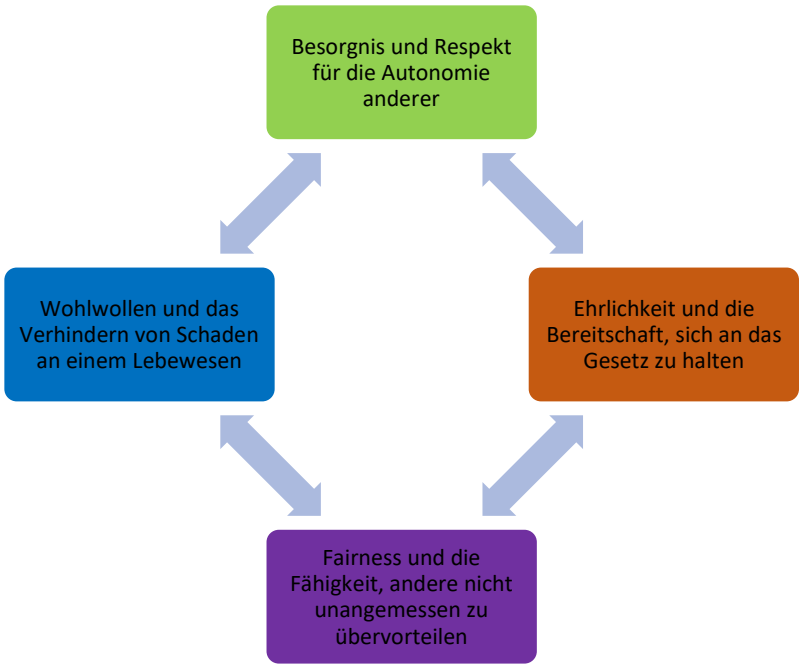
1. Offene Kommunikation
2. Konsensbildung
3. Gruppendiskussion moderieren
4. Sensibilität für ethnische und religiöse Hintergründe
5. Aufbau und Steuerung von Erwartungen
6. Einholen von Standpunkten von allen Teammitgliedern
7. Rollen vereinbaren, die die individuellen Stärken ausnutzen

Eine Umgebung zu schaffen, in der die Zusammenarbeit gedeiht, bedeutet, vorauszusehen, wie die Zusammenarbeit scheitern könnte, und Maßnahmen zu ergreifen, um dies zu verhindern, bevor es passiert.

2.9. Ethische Grundsätze

Persönliche Ethik bezieht sich auf die Überzeugungen einer Person darüber, was richtig und falsch ist und leitet Menschen bei ihren Entscheidungen. Ihre einzigartige Ethik bestimmt, wie Sie mit bestimmten Dingen umgehen und wie Sie wachsen und sich entwickeln. Die persönliche Ethik entwickelt sich im Laufe des Lebens kontinuierlich weiter, passt sich neuen Erkenntnissen an und verfeinert sich mit zunehmendem Alter.

Abbildung 2.7. Ethische Grundsätze. (Quelle: Eigene Ausarbeitung)



Die Prinzipien der persönlichen Ethik sind:

1. Besorgnis und Respekt für die Autonomie anderer.
2. Ehrlichkeit und die Bereitschaft, sich an das Gesetz zu halten.
3. Fairness und die Fähigkeit, andere nicht unangemessen zu übervorteilen.
4. Wohlwollen und das Verhindern von Schaden an irgendeiner Kreatur.

Abbildung 2.8. Ethische Grundsätze für die Wirtschaft und für Ihre berufliche Laufbahn. (Quelle: Eigene Ausarbeitung)

Diese Prinzipien beinhalten die Eigenschaften und Werte, die die meisten Menschen mit ethischem Verhalten in Verbindung bringen.

3. Wichtigste Werkzeuge der Medienkompetenz im Allgemeinen

3.1. Basissoftware Software und Kommunikationswerkzeuge

Die grundlegende Software und Computerprogramme, die die Ausführung der meisten üblichen Aufgaben für Computerbenutzer ermöglichen, können in zwei Gruppen unterteilt werden: freie Software und bezahlte. Wir möchten die freie Software hervorheben, jedoch haben bezahlte und lizenzierte Produkte ihre eigenen Vorteile, z. B. Support und eine größere Auswahl an zusätzlichen Tools und Möglichkeiten. Die meiste bezahlte Lizenzsoftware bietet auch eingeschränkte, aber kostenlose Versionen davon an, ungewöhnlicherweise für den persönlichen Gebrauch.

Um es einfach zu machen, haben wir eine Liste der häufigsten Aufgaben vorbereitet, die entweder mit kostenloser oder bezahlter Software gelöst werden können. Diese Liste deckt auch die meisten Tools ab, die normalerweise von den Arbeitgebern benötigt werden.

Wir geben auch die Links zu alternativen Online-Tools weiter, da viele der Aufgaben mit cloudbasierten Lösungen gelöst werden können, zumal sich die digitale Entwicklung schnell in Richtung cloudbasiertes Computing bewegt. Persönliche Geräte werden immer mehr zu Terminals, um auf die entfernten und leistungsstarken Maschinen zuzugreifen und die Ergebnisse anzuzeigen. Beachten Sie, dass die Mehrheit der Tools und Programme ihre eigenen alternativen Versionen in Smartphone-Geräten haben und in App-Stores zum Herunterladen zur Verfügung stehen.

Tabelle 3.1. Eine Liste von grundlegender kostenloser und Pad-Software

Eine Aufgabe oder ein Zweck	**Kostenlos (installieren)**	**Kostenpflichtig / alternativ (installieren)**	**Zugriff und Nutzung Online**
Internet-Zugang	Chrome, Firefox, Opera	Google News (app)	N/A
Suche nach Informationen	Google, Yahoo, Bing, Yandex	Duckduckgo	Quora, Wikipedia
Zugriff auf und Erstellen von E-Mail-Konten	Thunderbird	Microsoft Outlook	Gmail
Mitarbeit und Kommunikation	Skype, Telegram, Viber	Slack, Zoom	Trello, Asana
Bearbeiten von Dokumenten, Speichern und	OpenOffice (Writer)	Microsoft Word	Google Docs

Anzeigen von PDF			
Berechnungen durchführen, Tabellen und Diagramme zeichnen	OpenOffice (Calc)	Microsoft Excel	Google Sheets, Infogram.com
Computer gegen Viren schützen	GIMP	Photoshop	Snappa.com, Canva.com
Bildbearbeitung	VLC	Vimeo.com	Youtube.com
Media Player	Avast, Avira	ESET Antivirus	Eset online scanner
Sichern und Verwalten der Passwörter	LastPass (for individuals)	1password, Bitwarden	N/A
Werkzeuge zum sicheren Surfen (VPN)	Opera built-in VPN	Nord VPN, Express VPN	N/A

In weiteren Kapiteln werden wir auf bestimmte grundlegende Werkzeuge und Software näher eingehen.

3.2. Suchmaschine

Eine Suchmaschine ist eine Website, über die Benutzer Internetinhalte suchen können. Suchmaschinen ermöglichen es Benutzern, das Internet mit Hilfe von Schlüsselwörtern nach Inhalten zu durchsuchen. Jede Suchmaschine funktioniert auf ähnliche Weise.

Wenn Sie auf die Homepage einer Suchmaschine gehen, finden Sie ein einziges Feld. In dieses Feld geben Sie einfach ein, wonach Sie suchen möchten. Suchmaschinen sind eine großartige Möglichkeit, Dinge im Web zu finden. Wenn Sie sorgfältig suchen, können Sie zuverlässige und vertrauenswürdige Informationen finden. Bei einer solchen Vielfalt an Inhalten und der enormen Menge an Informationen im Internet kann es eine besondere Herausforderung sein, die relevanten Informationen zu finden.

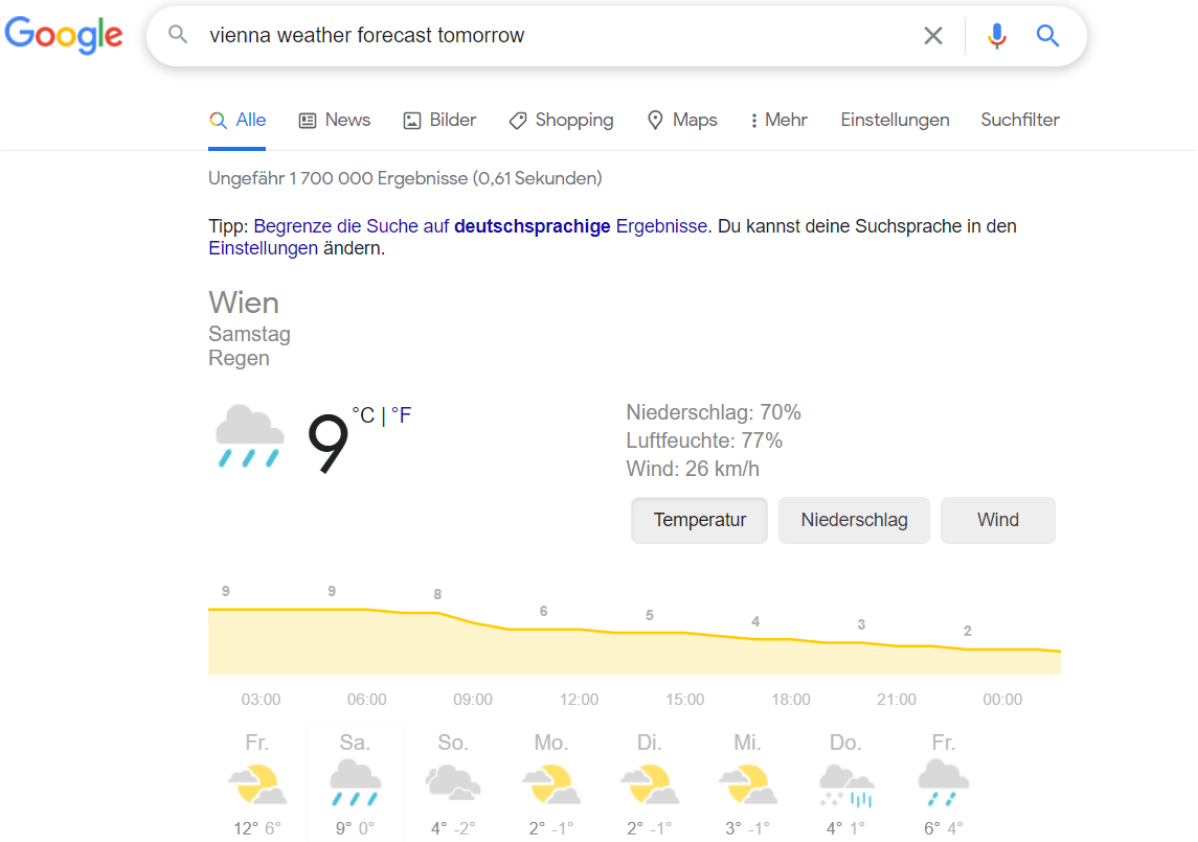
Schlüsselwörter in Ihren Suchkriterien

Sie müssen sorgfältig über die Schlüsselwörter nachdenken, die Sie in Ihre Suche eingeben. Sie müssen relevant sein. Um zum Beispiel herauszufinden, wie die Wettervorhersage für morgen ist, können Sie die Schlüsselwörter eingeben wie: "Wien Wettervorhersage morgen" und die relevantesten Suchergebnisse werden angezeigt.

Sie müssen auch über die Anzahl der Schlüsselwörter, die Sie verwenden, nachdenken. Wenn Sie zu wenige Suchbegriffe verwenden, könnten Sie zu viele Ergebnisse erhalten und diese werden nicht alle relevant sein. Wenn Sie jedoch zu viele Schlüsselwörter verwenden, erhalten Sie möglicherweise überhaupt keine Ergebnisse. Um Ihre Suche spezifischer zu

machen, können Sie "Anführungszeichen" um eine Reihe von Wörtern herum verwenden, um einen genauen Ausdruck zu finden.

Abbildung 3.1. Suchbeispiel: "Wien Wettervorhersage für Morgen" (Quelle: Google)



Wenn Sie ein Minuszeichen (-) vor ein Wort setzen, werden Seiten, die dieses Wort enthalten, ausgeschlossen. Zum Beispiel sucht 'Römische Kaiser -Caesar' nach Seiten, die 'Römer' und 'Kaiser' enthalten, aber nicht 'Caesar'.

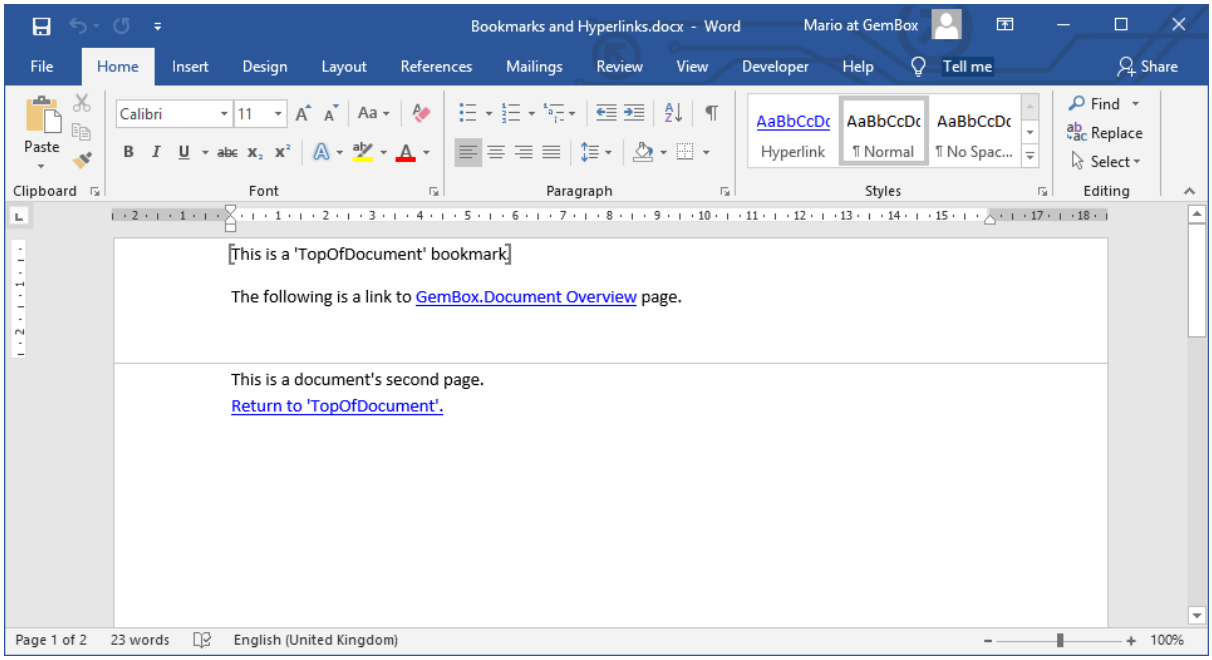
Was ist ein URL?

Jede Website hat ihre eigene Online-Adresse, die sogenannte URL, die für Uniform Resource Locator steht. Wenn Sie eine Seite im World Wide Web aufrufen, ist dies die lange Adresse, die in der Adressleiste oben in Ihrem Browser erscheint.

Es gibt noch ein paar weitere verschiedene Methoden, um die Informationen im Internet zu finden

1. Sie können direkt zu einer Webseite gehen, indem Sie einfach deren Standort kennen (z. B. möchten Sie die Website des Unternehmens besuchen, bei dem Sie sich bewerben, und Sie kennen die genaue Adresse der Website).
2. Der Hypertext-Link, der von einer Webseite ausgeht, bietet eingebaute Assoziationen zu anderen Seiten, die nach Ansicht des Autors relevante Informationen liefern.

Abbildung 3.2. Lesezeichen und Hyperlinks (Quelle: Eigene Ausarbeitung)



"Narrowcast"-Dienste können Ihnen Seiten "aufdrängen", die Ihrem Benutzerprofil entsprechen.

Es ist bekannt, dass Google die bekannteste Online-Suchmaschine der Welt ist, aber es gibt auch viele andere Optionen. Darüber hinaus sind einige dieser alternativen Suchmaschinen auf ihre Weise immens populär - sie erscheinen nur im Vergleich zu Google nicht übermäßig populär. Wenn Sie jedoch nicht bereit sind, Ihre Privatsphäre gegen Bequemlichkeit einzutauschen oder spezielle Suchanforderungen haben, gibt es mehrere Alternativen zu Google, die eine geeignetere Sucherfahrung bieten. Die richtige Suchmaschine für Ihre Anfrage zu kennen, bedeutet, dass Sie Ihre wertvolle Zeit nicht mit dem Durchsuchen von Dingen verbringen, die Sie nicht brauchen. Ohne die richtigen Werkzeuge kann man sich in der weiten Welt des Internets leicht verirren. Hier unten stellen wir Ihnen 15 Suchmaschinen vor, die Sie als Alternativen zu Google ausprobieren sollten, um bessere Suchergebnisse zu erzielen..

Abbildung 3.1. Beliebteste alternative Suchmaschinen

1. https://duckduckgo.com/	6. https://www.aol.com/	11. https://swisscows.com/
2. https://www.bing.com/	7. http://seznam.com/	12. https://startpage.com/
3. https://www.yahoo.com/	8. https://usearch.com/	13. https://www.ecosia.org/
4. https://yandex.com/	9. https://www.yippy.com/	14. https://www.naver.com/

5. https://www.ask.com/	10.https://www.searchencrypt.com/	15. https://www.baidu.com/

3.3. Email

Elektronische Post (E-Mail oder E-Post) ist eine Methode zum Austausch von Nachrichten ("Post") zwischen Personen mit elektronischen Geräten. Sie ist wie die herkömmliche Post, hat aber auch einige wichtige Unterschiede.

Zum Beispiel: Traditionelle Post wird mit dem Namen des Empfängers, der Straße, der Adresse, der Stadt, dem Bundesland oder der Provinz und der Postleitzahl adressiert. E-Mails werden elektronisch über das Internet zugestellt. Eine E-Mail enthält einen Benutzernamen, das Symbol @ (at) und die Domain des E-Mail-Anbieters. Benutzernamen enthalten oft Zahlen und verkürzte Versionen eines Namens, um eine eindeutige E-Mail-Adresse zu erstellen, und sehen normalerweise wie folgt aus: emarosa82@gmail.com

Wenn Sie eine E-Mail an jemanden senden, kommt sie fast sofort an und wartet im "Posteingang", bis der Empfänger sie liest. Bei E-Mails gibt es die Möglichkeit, Bilder hinzuzufügen. Bevor wir jedoch weiter ins Detail gehen, ist es wichtig zu erklären, wie man ein E-Mail-Konto einrichtet.

Um mit dem Versenden von E-Mails beginnen zu können, benötigen Sie eine E-Mail-Adresse, die für Sie eindeutig ist. Um diese zu erhalten, müssen Sie sich bei einem E-Mail-Anbieter für ein Konto anmelden - Sie können zwischen den verschiedenen Anbietern wählen - Yahoo, Gmail, Hotmail, Outlook, GMX... Es hängt von Ihren Vorlieben und Bedürfnissen in Bezug auf die elektronische Post ab. Wenn Sie zum Beispiel viel Platz und Einfachheit brauchen, ist Gmail sehr gut geeignet. Wenn Sie nur ein einfaches E-Mail-Programm zum Senden und Empfangen von Mails benötigen, mit wenigen Funktionen, kann Yahoo eine gute Wahl sein. Sie können Informationen über jeden Dienstanbieter erhalten, indem Sie seinen Namen in das Suchfeld der Suchmaschine eingeben und den Vergleich durchführen.

Da Gmail im Jahr 2020 der beliebteste Anbieter war, erkläre ich nun, wie man ein Gmail-Konto erstellt (beachten Sie, dass diese Methode zum Erstellen einer E-Mail für fast alle Dienstanbieter gelten kann).

Schritt 1. Geben Sie in Ihre Suchmaschine www.gmail.com ein, und Sie werden auf diese Seite weitergeleitet.

Klicken Sie auf "Konto erstellen", unten links, und die folgende Seite wird angezeigt:

Abbildung 3.3 Google Anmeldungsformular

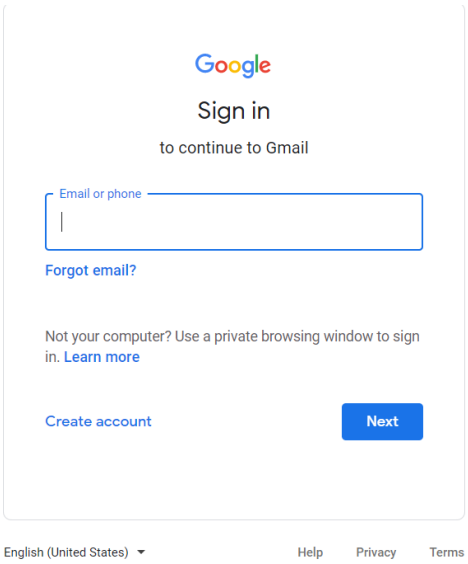
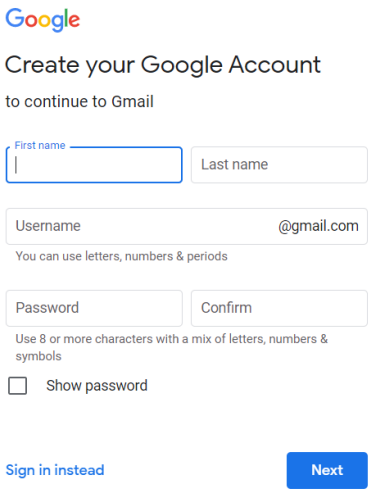
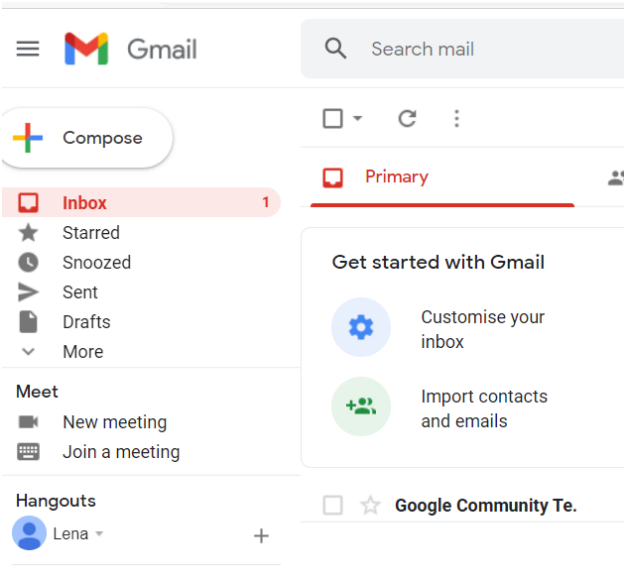


Abbildung 3.4. Formular für die Erstellung eines Kontos bei Google



Geben Sie Ihren Vor- und Nachnamen, Ihren Benutzernamen und Ihr Passwort ein. Seien Sie vorsichtig bei der Wahl des richtigen Passwortes, stellen Sie sicher, dass es nicht leicht zu erraten ist (vermeiden Sie z.B. das Datum Ihres Geburtstages, da Ihre Familie, Freunde und Bekannte es leicht erraten und auf Ihre privaten Mails zugreifen könnten). Sie können eine Kombination aus Buchstaben, Zahlen und Zeichen bilden, um ein starkes und zuverlässiges Passwort für Ihr Konto zu erstellen. Nachdem Sie ein Konto erstellt haben, können Sie auf die Gmail-Oberfläche zugreifen.

Abbildung 3.5. Gmail Hauptseite



Wie Sie sehen können, ist es sehr benutzerfreundlich und intuitiv. Wenn Sie eine E-Mail erstellen möchten, klicken Sie auf die Schaltfläche "Verfassen" und ein kleineres Fenster erscheint in der unteren rechten Ecke, in das Sie den Namen (E-Mail-Adresse) des Empfängers und den Betreff Ihrer E-Mail eingeben müssen. Der Platz für den Text befindet sich unterhalb der Zeile "Betreff". Am unteren Rand des Fensters sehen Sie eine "Senden"-Schaltfläche sowie ein "Büroklammer"-Symbol, wenn Sie Ihrer E-Mail Dateien hinzufügen möchten, oder "Emoji einfügen", wenn Sie Ihrer E-Mail lächelnde Gesichter hinzufügen möchten. Wenn Sie Ihre E-Mail verfasst haben, klicken Sie auf die Schaltfläche "Senden" und Ihre E-Mail wird an die gewünschte E-Mail-Adresse zugestellt und in den "Gesendet"-Nachrichten gespeichert.

Wenn Sie eine E-Mail von jemandem erhalten, erscheint sie in Ihrem "Posteingang" als fettgedruckte, ungelesene Nachricht. Die wichtigsten Nachrichten können mit einem "Stern" gekennzeichnet sein und es erleichtert das Auffinden durch die Suche im "Sternchen"-Bereich.

3.4. Soziale Netzwerke

Ein soziales Netzwerk ist definiert als eine Kette von Individuen und deren persönlichen Verbindungen. Alternativ auch als virtuelle Gemeinschaft oder Profilseite bezeichnet, ist ein soziales Netzwerk eine Website, die Menschen zusammenbringt, um sich zu unterhalten, Ideen und Interessen auszutauschen oder neue Freunde zu finden. Diese Art der Zusammenarbeit und des Austauschs wird als soziale Medien bezeichnet.

Die 10 Top-Social-Media-Seiten, um die Sie sich im Jahr 2021 kümmern müssen

Name	Information
Facebook www.facebook.com	Das beliebteste soziale Netzwerk, um einen persönlichen Bereich einzurichten und sich mit Freunden zu verbinden, Bilder auszutauschen, Filme zu teilen, usw.
Youtube www.youtube.com	Ein hervorragendes Netzwerk, um Video-Blogs oder Vlogs und andere lustige und spannende Videos zu veröffentlichen.
Twitter www.twitter.com	Ein sehr beliebtes Medium, um zu kommunizieren (30-65 Jahre), aktuelle Nachrichten, mundgerechte Inhalte zu verdauen (150 Zeichen sind erlaubt). Durch die Verwendung des Hashtags können Sie die Informationen filtern.
Instagram www.instagram.com	Weit verbreitetes soziales Netzwerk, das von Fotografie-Enthusiasten (20-35 Jahre) genutzt wird.
Tik tok www.tiktok.com	Unterhaltsamer, interessanter, komödiantischer Kurzvideo-Content, meist vertont mit bekannten Songs.
Snapchat www.snapchat.com	Stark genutzte App von unter 25-jährigen Nutzern mit videogestütztem Storytelling.
LinkedIn www.linkedin.com/	professionelles soziales Netzwerk, mit Stellenangeboten, Diskussionsgruppen und Foren zum Meinungsaustausch

Pinterest www.pinterest.com	Sehr beliebtes Social-Bookmarking-Tool, um Ideen zu speichern und kreative Inspirationen zu finden, vom Kochen bis hin zu Heimwerkerprojekten, Urlaubsideen, Inneneinrichtung. Wird hauptsächlich von Frauen genutzt.
Redditt www.reddit.com	Gemeinschaft von registrierten Benutzern (Redditoren), die Inhalte einreichen, die von der Gemeinschaft hochgestuft werden.
Google+ https://plus.google.com/collections/featured	Werden Sie Teil von "Kreisen", Gruppen, die über bestimmte Themen sprechen, und wählen Sie die Gruppe, die Sie interessiert.

Der Prozess zum Erstellen eines neuen Kontos für ein soziales Netzwerk unterscheidet sich für jedes soziale Netzwerk.

Im Allgemeinen besuchen Sie die Website des sozialen Netzwerks, bei dem Sie ein Konto einrichten möchten, und suchen Sie nach einem Link "Anmelden" oder "Neues Konto erstellen".
Folgen Sie den Schritten zur Kontoerstellung, um Ihr neues Konto zu erstellen.

Sie müssen wahrscheinlich mindestens Ihren Namen, Ihren Altersbereich und Ihre E-Mail-Adresse angeben. Je nach den Anforderungen des sozialen Netzwerks können weitere Informationen erforderlich sein.

Achten Sie auf die Privatsphäre-Einstellungen, um bestimmte Inhalte auf Freunde zu beschränken und gleichzeitig ein gutes Bild in der Öffentlichkeit zu wahren.

3.6. Entwicklung von Websites, Blogging und Marketing

Websites sind zweifelsohne das wichtigste Element des Internets und ermöglichen die Darstellung von Inhalten wie Texten, Bildern und Videos im Internet.
Die zentrale Seite einer Website wird Homepage oder Startseite/Indexseite genannt. Der Benutzer taucht dann in die Unterseiten der Website ein.

Je nach Größe der Website haben die Besucher der Website die Möglichkeit, auf Unterseiten der Website zuzugreifen. Hyperlinks, oder einfach 'Links', werden verwendet, um einzelne HTML-Dokumente einer Website zu verbinden.

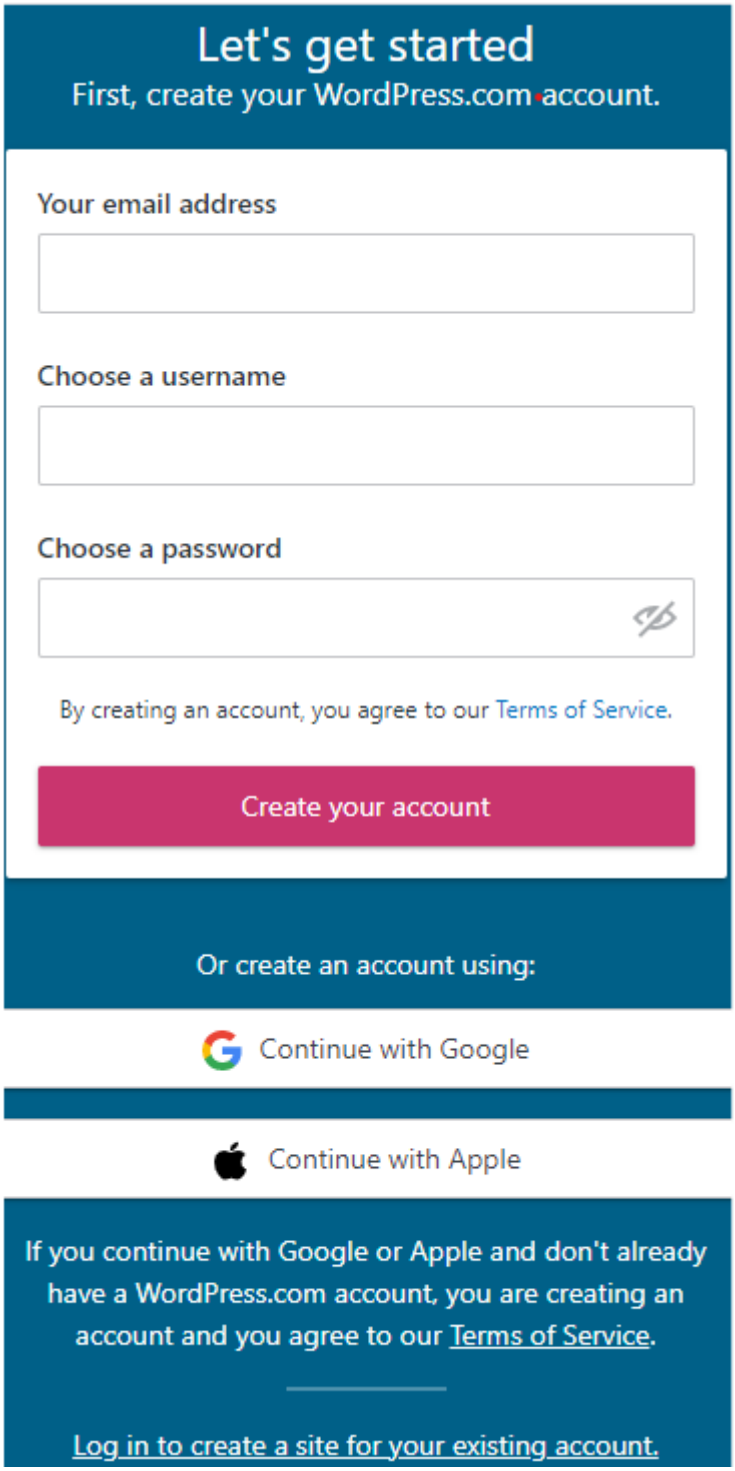
- Links zu wichtigen Unterseiten (z. B. Abteilungen, Produktkategorien oder repräsentative Informationsseiten) werden in der Regel in der Navigation zusammengefasst und sind im Kopfbereich der Website zu finden. Sie werden auf jeder Unterseite der Website angezeigt und nicht nur auf der Startseite.
- Die Navigation hilft dem Benutzer, sich zu orientieren und einen Überblick über die Struktur der Website zu erhalten.
- Links zu weiteren Unterseiten können auch in den Text- und Bildelementen im Inhalt der Website platziert werden.

Die Fußzeile am unteren Ende einer Seite enthält oft Links zu weiteren Informationen wie dem Betreiber der Website und den rechtlichen Rahmenbedingungen.

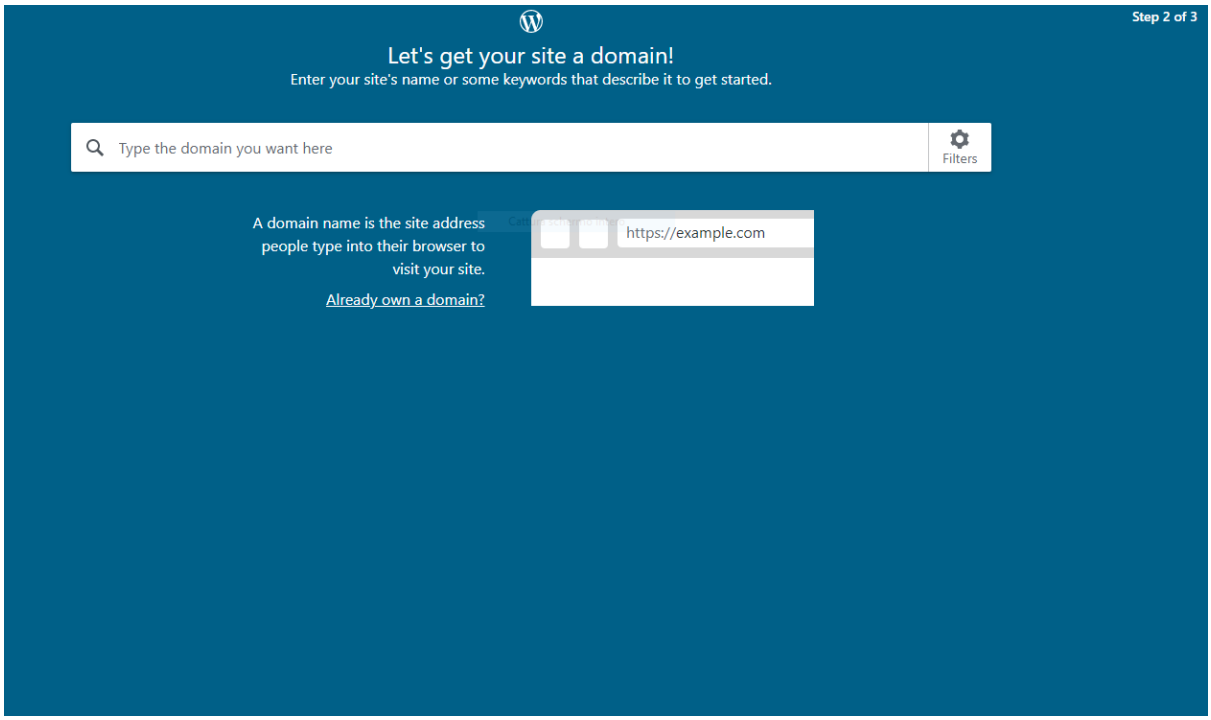
Wie Sie eine kostenlose Website mit WORDPRESS erstellen

WordPress.com ist die erste Lösung, die Sie in Betracht ziehen sollten, um eine kostenlose Website mit dem berühmten CMS zu erstellen. Diese Plattform ermöglicht es Ihnen, Ihre eigene Website mit einer Third-Level-Domain (www.namewebsite.wordpress.com) zu erstellen, indem Sie einen Speicherplatz von 3 GB zur Verfügung stellen.

Gehen Sie auf die Startseite https://wordpress.com/, klicken Sie auf die Schaltfläche Konto erstellen. Geben Sie anschließend in dem entsprechenden Textfeld die Adresse kostenlos an.



Geben Sie dann in das Feld "Geben Sie einen Namen oder ein Stichwort ein" den Namen ein, der in der Domain Ihrer Website angezeigt werden soll, und klicken Sie auf die Schaltfläche Auswählen für die Option Kostenlos. Auf der neu geöffneten Seite klicken Sie auf die Schaltfläche "Start with free", geben die erforderlichen Daten in die Felder "Your e-mail address", "Choose a username" und "Choose a password" ein, klicken zweimal hintereinander auf die Schaltfläche "Continue" und sind fertig.



Klicken Sie nun auf die Schaltfläche Website anzeigen, um Ihre mit WordPress.com erstellte Website zu betrachten. Um neue Seiten und Artikel hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen, die sich auf die Optionen Site-Seiten und Blog-Artikel bezieht, während Sie durch Auswahl des Elements Anpassen in der linken Seitenleiste das Aussehen ändern und ein anderes verfügbares kostenloses Theme auswählen können. Wählen Sie eine der vielen verfügbaren Vorlagen aus: Klicken Sie dazu auf die Vorschau der Vorlage, die Sie interessiert, und klicken Sie auf die Schaltfläche Anwenden, um sie direkt auf die von Ihnen erstellte Website anzuwenden; oder klicken Sie auf die Schaltfläche Anpassen, wenn Sie sie ein wenig ändern möchten.

Um der Website neue Seiten oder neue Beiträge hinzuzufügen, klicken Sie stattdessen auf die Wörter Seiten oder Beiträge (auf der linken Seite) und klicken Sie auf die Schaltfläche (+) Neue Seite oder (+) Neuer Beitrag, die sich oben links befindet. In dem sich öffnenden Fenster können Sie eine neue Seite oder einen neuen Beitrag erstellen, indem Sie den Titel und den Text in die entsprechenden Textfelder eingeben. Mit den Schaltflächen in der Symbolleiste oben können Sie auch den Text formatieren, Links, Bilder usw. einfügen. Durch Klicken auf die

Schaltflächen Vorschau und Veröffentlichen können Sie den Inhalt in der Vorschau anzeigen und ihn veröffentlichen.

Während der Betrieb einer Website über die Hosting-Lösung Worpress.com einfach und bequem ist, vor allem für Anfänger, ist es manchmal besser geeignet, einen vollständig anpassbaren Ansatz für den Aufbau einer Website zu wählen und sie selbst zu hosten. Sie müssten einen Hosting-Plan von einem der vielen Hosting-Service-Provider erwerben und das Wordpress-CMS mithilfe einer Reihe von Tools installieren, die vom Betreiber bereitgestellt werden.

Da Wordpress eine Plattform ist, die ursprünglich für Blogger geschaffen wurde, wuchs es in seiner Popularität zur ersten Wahl für alle Arten von individuellen Website-Entwicklern und auch Unternehmen. Es unterstützt eine breite Palette von Tools und Plugins, mit denen Wordpress an E-Commerce, Foren, Auktionen oder sogar Social-Media-Plattformen angepasst werden kann. Wordpress-Profis sehen es eher als einen sehr gut optimierten Kern, auf dem jede Art von Online-Projekt entwickelt werden kann, wobei die ursprünglichen Wordpress-Komponenten entfernt werden.

Es gibt viele alternative CMS-Plattformen für Wordpress und zu den populärsten gehören Joomla, Drupal als CMS-Plattformen, während Wix.com, Shopify.com Web-Plattformen und Dienstleistungspakete sind, die für bestimmte Bedürfnisse, wie E-Commerce und andere, bestimmt sind.

Abbildung 3.9. Einige der beliebtesten CMS-Plattformen und -Dienste

Abschließend ist zu betonen, dass eine wirklich erfolgreiche Website in der Regel diejenige ist, die den Besuchern der Website - den Internetnutzern - einen echten Mehrwert bietet. Eine Möglichkeit, einen Mehrwert zu bieten, kann die Erstellung von qualitativ hochwertigen Inhalten sein, indem man in der Lage ist, interessante und fesselnde Artikel und Geschichten zu schreiben, daher sind Storytelling-Fähigkeiten bei der Erstellung jeglicher Art von Inhalten

im Internet sehr nützlich. Im folgenden Kapitel haben wir ein paar Tipps für einen erfolgreichen Geschichtenerzähler vorbereitet, indem wir vorstellen, was persönliches Geschichtenerzählen ist und welche Fähigkeiten dabei nützlich sein können.

3.6.1 Persönliches Storytelling

Storytelling ist die Fähigkeit, jemanden oder eine Gruppe von Menschen mit einer fesselnden Erzählung zu fesseln, die sie beeinflusst und ihnen das Gefühl gibt, ein Teil der Geschichte zu sein. Menschen erinnern sich an Geschichten viel besser als an Fakten und Zahlen. Es ist eine der wichtigsten Fähigkeiten, die Sie lernen können, zu meistern.

Hauptpunkte:

Why is storytelling valuable to the storyteller?

1. Storytelling beeinflusst Veränderungen sowohl auf individueller Praxis- als auch auf Organisationsebene
2. Das Zuhören von Geschichten erleichtert eine bessere personenzentrierte Pflege und kann zu verbesserten Dienstleistungen führen
3. Das Anhören persönlicher Geschichten führt zu größerem Verständnis, Empathie und Reflexion
4. Rapport, Vertrauen und Fürsorge können durch das Erzählen von Geschichten in der Beziehung zwischen Therapeuten und Nutzern gefördert werden.
5. Persönliche Geschichten kommen dem Erzähler zugute, da sie ihn stärken, sein persönliches Wachstum fördern und seine Widerstandskraft stärken können.

1. **Fördert die Selbstidentität und die persönliche Entwicklung**
   Es gibt Hinweise darauf, dass der Prozess des persönlichen Geschichtenerzählens es ermöglicht, das Konzept des Selbst und der Lebensgeschichte auf eine Art und Weise zu verbinden, die ein Reframing der Identität ermöglicht und persönliches Wachstum begünstigt. Beim Erzählen einer Geschichte drückt eine Person die bedeutenden Ereignisse in ihren eigenen Worten und in ihrer eigenen Zeit aus und wird zur Reflexion befähigt. Der Prozess ermöglicht es, ein neues Bewusstsein und neue Bedeutungen des Selbst zu entwickeln.
2. **Ist eine Beziehung, die Bedeutung koproduziert**
   Die Beziehung des Geschichtenerzählens beinhaltet ein Zuhören und ein Engagement, das sich von dem eines Darstellers-Zuschauers oder Interviewers-Teilnehmers unterscheidet. Es ist eine Beziehung, die die Kluft zwischen der Person und denjenigen, die sie unterstützen, überbrückt, z. B. zwischen Therapeut und Anwender.
3. **Fördert die Belastbarkeit**
   .
4. **Is therapeutic**
   The therapeutic value of telling a story is often reported in storytelling work (Hardy, 2007; Scottish Recovery Network, 2012). Resilienz beinhaltet die Bereitschaft, negative Emotionen, die mit störenden Lebensereignissen einhergehen, in etwas Stärkendes und Ermächtigendes zu verwandeln. Resilienz wird durch einen Prozess der Reflexion über Bedeutungen entwickelt, der emotionale Einsichten ermöglicht.

Die Unterstützung von Peer- und anderen Netzwerken ist der Schlüssel, um Bindungen aufzubauen und sich mit anderen Menschen verbunden zu fühlen. Die Kombination dieser Faktoren führt zu einer Stärke im Menschen, die auf der Prämisse beruht, dass Lebenserfahrungen (auch negative) Chancen für persönliches Wachstum bieten. Häufiger ist es so, dass der Akt des Erzählens einer Geschichte und des Reflektierens darüber eine kathartische Wirkung hat und ein Katalysator zur Genesung ist.

Storytelling-Techniken

Die besten Geschichtenerzähler sind in der Lage, erzählerische Entscheidungen zu treffen, die nützlich sind, um ihre Geschichten voranzutreiben, das Zielpublikum durch die Verbreitung wichtiger Informationen einzubeziehen, die Aufmerksamkeit aufrechtzuerhalten, sie wissen, wie sie sich auf ihre Lebenserfahrungen beziehen können, um dem Text Emotionen zu verleihen.
Sie sollten auch in der Lage sein, mit sich selbst in Kontakt zu treten, bis zu dem Punkt, dass Worte und Emotionen zu einer Einheit werden, die in der Lage ist, bei den Gesprächspartnern Bewusstsein und Reflexion zu wecken.
Letztere stellen das Ziel dar, also eine Gruppe potenzieller Kunden, denen ein Unternehmen seine Produkte, Dienstleistungen oder den Inhalt selbst verkaufen möchte, und müssen sich in die Idee und die erzählte Geschichte "verlieben". Storytelling kann für jeden Bereich angepasst werden, der kommunikativ unterstützt werden muss: ein Unternehmen, ein geistiges oder physisches Produkt, eine Dienstleistung, eine Marke, eine Person oder ein Ereignis.

3.7. E-Unterschrift und E-Dienstleistungen

Elektronische Unterschrift

Elektronische Signaturen bieten eine Möglichkeit, Dokumente in der Online-Welt zu unterschreiben, ähnlich wie man in der realen (Offline-)Welt ein Dokument mit einem Stift unterzeichnet. In der Vergangenheit waren nur handschriftliche Unterschriften rechtsgültig. Mit der 1999 verabschiedeten Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (eSignatur-Richtlinie) wurde diese Anerkennung auf elektronische Signaturen erweitert. Ein zuverlässiges System elektronischer Signaturen, das in allen EU-Ländern funktioniert, ist für den sicheren elektronischen Geschäftsverkehr und die effiziente elektronische Erbringung öffentlicher Dienstleistungen für Unternehmen und Bürger von entscheidender Bedeutung. Mit der eSignatur-Richtlinie wurde auf europäischer Ebene der rechtliche Rahmen für elektronische Signaturen und Zertifizierungsdienste geschaffen. Ziel ist es, die Nutzung elektronischer Signaturen zu erleichtern und ihre rechtliche Anerkennung innerhalb der EU-Mitgliedstaaten zu fördern[6].

Die Definition von elektronischen Signaturen variiert je nach geltender Rechtsprechung. Ein gemeinsamer Nenner in den meisten Ländern ist das Niveau einer fortgeschrittenen elektronischen Signatur (eine E-Signatur, die die Anforderungen der EU-Verordnung erfüllt), die Folgendes erfordert:

1. Authentizität: Die Nachricht stammt von dem angegebenen Absender, und der Absender kann eindeutig identifiziert werden.
2. Integrität: Manipulationen an der Signatur des unterschriebenen Dokuments können sofort erkannt werden.

Mit der Erfindung der Handy-Signatur wurden Werkzeuge entwickelt, um rechtsverbindliche Dokumente, Rechnungen und Verträge elektronisch zu unterschreiben. Es ist möglich, dem PDF-Dokument schnell und sicher eine elektronische Signatur hinzuzufügen, die das rechtliche Äquivalent einer handschriftlichen Unterschrift ist. Die Authentizität der Signatur und die Echtheit der übertragenen Daten können jederzeit von Absender oder Empfänger überprüft werden.

Elektronische Unterschrift

Elektronische Unterschriften sind kryptografische Implementierungen elektronischer Signaturen, die als Beweis für die Authentizität, Datenintegrität und Nachweisbarkeit der über das Internet durchgeführten Kommunikation dienen. Wenn sie in Übereinstimmung mit den Standards für digitale Signaturen implementiert werden, sollte die digitale Signatur einen durchgängigen Datenschutz bieten, wobei der Signiervorgang benutzerfreundlich und sicher ist. Digitale Signaturen werden durch standardisierte Verfahren wie den Digitalen Signaturalgorithmus (DSA) erzeugt und verifiziert.

Am Prozess der digitalen Signatur sind in der Regel drei Algorithmen beteiligt:

1. **Key generation** – dieser Algorithmus liefert einen privaten Schlüssel zusammen mit dem zugehörigen öffentlichen Schlüssel.
2. **Unterzeichnung** – dieser Algorithmus erzeugt eine Unterschrift nach Erhalt eines privaten Schlüssels und der zu unterzeichnenden Nachricht.

[6] https://ec.europa.eu/digital-single-market/en/trust-services

3. **Überprüfung** – dieser Algorithmus prüft die Authentizität der Nachricht, indem er sie zusammen mit der Signatur und dem öffentlichen Schlüssel verifiziert.

Der Prozess des digitalen Signierens erfordert, dass die Signatur, die sowohl von der festen Nachricht als auch vom privaten Schlüssel erzeugt wurde, anschließend durch den dazugehörigen öffentlichen Schlüssel authentifiziert werden kann. Mit diesen kryptografischen Algorithmen kann die Signatur des Benutzers nicht repliziert werden, ohne dass er Zugriff auf seinen privaten Schlüssel hat. Ein sicherer Kanal ist normalerweise nicht erforderlich. Durch die Anwendung asymmetrischer Kryptografieverfahren verhindert das digitale Signaturverfahren mehrere gängige Angriffe, bei denen der Angreifer versucht, sich durch die folgenden Angriffsmethoden Zugang zu verschaffen.

Biometrische Unterschrift

Elektronische Signatur kann sich auch auf elektronische Formen der Verarbeitung oder Überprüfung der Identität durch Verwendung biometrischer "Signaturen" oder biologisch identifizierende Eigenschaften einer Person beziehen. Solche Signaturen verwenden den Ansatz, einige biometrische Messungen als Beweismittel an ein Dokument anzuhängen. Biometrische Signaturen umfassen Fingerabdrücke, Handgeometrie (Fingerlängen und Handflächengröße), Irismuster, Stimmmerkmale oder sogar Netzhautmuster. Alle diese Merkmale werden mit Hilfe von elektronischen Sensoren erfasst, die in irgendeiner Form eingesetzt werden. Da jedes dieser physischen Merkmale einen Anspruch auf Einzigartigkeit unter Menschen hat, ist jedes bis zu einem gewissen Grad als Unterschrift nützlich.

Abbildung 3.10. Anwendung für elektronische Unterschriften (Quelle: https://bit.ly/2ZdPQmX)

Die fünf beliebtesten elektronischen Unterschriftendienste:

1. **eSignly** ist eine führende E-Signatur-Lösung für Millionen von Nutzern auf der ganzen Welt, weil sie das Unterschreiben und Verwalten von Dokumenten so einfach macht. Die App bietet

mehrere Funktionen wie persönliche Unterzeichnung, geplante Unterzeichnung, Selbstunterzeichnung, Team-Management, erstklassige Sicherheit, Integration mit beliebten Arbeitsanwendungen, Audit Trail usw.

2. **PandaDoc** ist sowohl für Android- als auch für iOS-Mobilplattformen verfügbar. Die Online-Software ist eine preisgekrönte Software für elektronische Signaturen, die über eine einfach zu bedienende Benutzeroberfläche verfügt.

3. Die **Adobe Sign-App** ist sowohl für die iOS- als auch für die Android-Mobilplattform verfügbar. Adobe ist ein bekannter Name in der Welt der Grafik und gilt als einer der Pioniere im Bereich eSign Services. Die Software ist funktionsreich und gibt dem Benutzer die Möglichkeit, kontinuierliche Arbeitsabläufe von jedem Ort oder Gerät aus zu verwalten.

4. **SignEasy** ist eine weitere elektronische Signatursoftware, die mit den Plattformen Android und iOS kompatibel ist. SignEasy ist keine schwerfällige Signaturanwendung, da sie eine minimale Benutzeroberfläche mit der Absicht bietet, sie einfach zu bedienen. Die Unterzeichnung mit SignEasy ermöglicht die Selbstunterzeichnung, die Fernunterzeichnung und die persönliche Unterzeichnung.

5. Die **RightSignature** - Mobile Applikation nutzt die Plattformen Android und iOS. Diese E-Signatur-App setzt auf Geschwindigkeit, um ihre Benutzer zu beeindrucken, da Dokumente beim Senden und Empfangen für Signaturen schneller ankommen. Mit ihr können Sie Dokumente in kürzester Zeit hochladen, formatieren und versenden.

Hinzufügen oder Entfernen einer elektronischen Unterschrift in einem Microsoft Word- oder Adobe

Mit einer E-Signatur-Zeile in einem Word-Dokument können Sie Informationen über den Unterzeichner anfordern und Anweisungen geben. Wenn eine elektronische Kopie an den Unterzeichner geht, sieht diese Person die Signaturzeile und eine Benachrichtigung, in der ihre Unterschrift angefordert wird. Der Unterzeichner kann:

1. Eine Unterschrift eingeben
2. Wählen Sie ein Bild einer eingefärbten Unterschrift
3. Schreiben Sie eine Unterschrift mit Hilfe der Tintenfunktion auf einem Touchscreen-Computer oder einem anderen Gerät

So erstellen Sie eine Unterschriftszeile in Word oder Excel (Office 365 oder 2019):

1. Setzen Sie den Cursor im Dokument an die Stelle, an der Sie eine Unterschriftszeile wünschen.
2. Klicken Sie auf der Registerkarte Einfügen in der Gruppe Text auf die Liste Signaturlinie. Klicken Sie dann auf Microsoft Office Unterschriftszeile.
3. Geben Sie im Dialogfeld " Unterschrift einrichten" die Informationen ein, die unter der Unterschriftszeile erscheinen sollen:

● Vorgeschlagener Unterzeichner: der vollständige Name des Unterzeichners

● Vorgeschlagener Titel des Unterzeichners: der Titel des Unterzeichners, falls vorhanden

● Vorgeschlagene E-Mail-Adresse des Unterzeichners: die E-Mail-Adresse des Unterzeichners, falls erforderlich

● Anweisungen für den Unterzeichner: Anweisungen für den Unterzeichner, wie z. B. "Überprüfen Sie vor dem Unterschreiben des Dokuments, ob der Inhalt korrekt ist".

4. Aktivieren Sie eines oder beide der folgenden Kontrollkästchen:

● Erlauben Sie dem Unterzeichner, im Dialogfeld " Unterschreiben" Kommentare hinzuzufügen: Der Unterzeichner kann den Zweck der Unterzeichnung eingeben.

- Unterschriftsdatum in der Signaturzeile anzeigen: Das Datum, an dem das Dokument signiert wurde, wird mit der Unterschrift angezeigt.

Außerdem können Sie eine Signatur entfernen, indem Sie im Signaturbereich auf den Pfeil neben der Signatur und dann auf Signatur entfernen klicken.

Alternativ können Sie auch eine elektronische Signatur in einem PDF-Dokument benötigen. Im nächsten Abschnitt erfahren Sie, wie Sie E-Signaturen in PDF-Dateien verwenden können.

Elektronisches Unterschreiben einer PDF-Datei

Das Portable Document Format (PDF) von Adobe ist ein gängiges Format für Dokumente mit festem Layout. Wie Word hat auch Adobe PDF seit seiner Markteinführung im Jahr 1993 eine Reihe von Funktionen hinzugefügt. Es ist jetzt möglich, eine PDF-Datei zur Authentifizierung elektronisch zu signieren.

Wenn Sie ein Windows-Benutzer sind, sind Sie wahrscheinlich mit PDF-Readern vertraut. Dabei handelt es sich um Computerprogramme, mit denen Sie PDF-Dateien öffnen können, d. h. Dateien mit der Dateierweiterung .pdf. Die beliebteste Option ist heutzutage der Adobe Acrobat Reader.

Gehen Sie folgendermaßen vor, um einer PDF-Datei eine elektronische Signatur hinzuzufügen::

1. Öffnen Sie die PDF-Datei in Adobe Acrobat Reader.
2. Klicken Sie rechts im Bereich Werkzeuge auf Ausfüllen & Unterschreiben.
3. Klicken Sie auf Unterschreiben und wählen Sie dann Unterschrift hinzufügen.
4. Ein Popup-Fenster wird geöffnet. Wählen Sie eine Option - Typ, Zeichnen oder Bild.
5. Klicken Sie auf die Schaltfläche Anwenden.

Ziehen, ändern Sie die Größe und positionieren Sie die Unterschrift in Ihrer PDF-Datei

E-Dienstleistungen (E-service)

E-Service (oder eservice) ist ein sehr allgemeiner Begriff, der sich in der Regel auf die "Bereitstellung von Dienstleistungen über das Internet" bezieht (wobei die Vorsilbe "e", wie in vielen anderen Verwendungen, für "elektronisch" steht). E-Services umfassen alle Dienstleistungen und Aktivitäten, die mit Hilfe von Computern erstellt und interaktiv über elektronische Medien, wie z. B. das Internet, angeboten und ausgeführt werden.

E-Services können Informations- und Bildungsdienste wie E-Education, E-Learning, E-Teaching, E-Publishing, E-Book, E-Zine und E-Katalog, Beschaffungs-, Handels- und Bestelldienste wie E-Business, E-Commerce, E-Procurement, E-Cash, E-Shop, E-Intermediary, E-Auction sein, Kultur- und Verwaltungsdienste wie E-Kultur, E-Government oder E-Vote,

Verbesserung von Marketing-, Produkt- oder Kundenbeziehungsdiensten, elektronische Beratungsdienste wie E-Consultancy oder E-Advising, sicherheitsbezogene Dienste (E-Security), Produktions-, wissenschaftliche oder logistische Dienste. E-Services werden in Zukunft in vielen weiteren Anwendungen zum Einsatz kommen.

Wie nutzen Sie E-Services?

Um die Dienste nutzen zu können, müssen Sie sich zunächst oben auf einer beliebigen Seite als neuer Benutzer registrieren.

1. Sie wählen den Link "Registrieren" und füllen die erforderlichen Felder aus.
2. Bei der Registrierung erhalten Sie eine Bestätigung, dass Sie registriert wurden, was die Beantragung von Behördenleistungen online ermöglicht.

3.7. Sicherheits-Software

Jedes angeschlossene Gerät kann ein Einfallstor für eine Sicherheitsbedrohung sein. Der beste Weg, ein Gerät zu schützen, insbesondere eines, das mit dem Internet verbunden ist, ist die Verwendung einer geeigneten und aktuellen Sicherheitssoftware, die normalerweise als Antivirus bekannt ist.

Eine zusätzliche Sicherheitsebene für persönliche Daten und sowohl für die über das Internet übertragenen Informationen als auch für das Gerät selbst können spezielle Tools namens VPNs bieten, was für Virtual Private Network steht.

Beim Surfen oder vor allem bei Finanztransaktionen, die über ein unsicheres WLAN durchgeführt werden, können Sie sich und Ihre sensiblen Daten einem Sicherheitsrisiko aussetzen.

Antiviren-Tools und -Dienste bieten in der Regel eine Reihe von Tools, die den Internetverkehr überwachen, die Dateien scannen und versuchen, potenzielle Sicherheitsbedrohungen, auch unbekannte Viren, zu erkennen. Solche Tools helfen dabei, Malvertising zu vermeiden, potenziell schädliche Websites zu blockieren und andere Lösungen zu verwenden, um das Gerät und die Daten des Benutzers zu schützen.

VPN-Tools helfen dabei, sich über einen gesicherten Remote-Server mit dem Internet zu verbinden, der die ursprüngliche IP-Adresse des Benutzers verbirgt und es dem Benutzer ermöglicht, seinen Datenverkehr zu verschlüsseln und seine Online-Identität zu verschleiern. Auf diese Weise wird die Anonymität und Sicherheit beim Surfen über öffentliche WiFi-Hotspots oder andere unsichere Netzwerkverbindungen erhöht.

Einige Antivirensoftware kann auch einen VPN-Dienst anbieten.

Die am häufigsten verwendete Antiviren-Software:

- Avira
- Avats
- McAfee
- ESET

- Bitdefender
- AVG
- Kaspersky
- Microsoft security essentials
- Norton

Die am häufigsten verwendeten VPN-Tools:

- Nord VPN
- Express VPN
- Surfshark
- Tunnelbear

3.8. Gerätesicherheit und Hardware

Wir alle wissen, wie ärgerlich es ist, ein Telefon zu verlieren, es gestohlen zu bekommen oder es einfach auf den Boden fallen zu lassen und den Bildschirm so weit zu beschädigen, dass das Gerät unbrauchbar wird. Das Problem wird normalerweise nicht als wichtig angesehen, bis es passiert. Um alle Arten von Schäden an einem Gerät zu vermeiden

Wenn wir über physische Sicherheit sprechen, gehen wir davon aus, dass jedes Gerät durch einen Sturz, einen Hardware-Defekt oder einen Wasserschaden beschädigt werden kann oder dass es verloren geht oder gestohlen wird.

Wir haben eine Liste von Möglichkeiten und Lösungen zusammengestellt, wie Verluste durch einfache Techniken zur Sicherung eines physischen Geräts vermieden werden können:

1. **Kennwort oder Verschlüsselung.** Vermeiden Sie den Verlust von Informationen aufgrund von Diebstahlversuchen. Verwenden Sie ein starkes Passwort, einen Fingerabdruck oder andere biometrische Daten, um den Zugriff auf Ihr Gerät zu schützen, sowohl auf dem Mobiltelefon als auch auf dem Desktop. Vermeiden Sie es, überall das gleiche Kennwort zu verwenden, und sperren oder verschlüsseln Sie wichtige Dateien mit einem Kennwort. Aktivieren Sie die integrierte oder installierte Ortungssoftware, die einige Anbieter zur Verfügung stellen, um Ihr Gerät mithilfe von Ortungsdiensten verfolgen zu können, auch wenn es bei Verlust oder Diebstahl gesperrt ist.
2. **Backup**. Sichern Sie wichtige Dateien immer, speichern Sie sie auf CDs oder Speichersticks oder sogar in einem Cloud-Speicher eines Drittanbieters.
3. **Hausverstand.** Verleiten Sie Diebe nicht mit unbeaufsichtigten mobilen Geräten, insbesondere an öffentlichen Orten. Lassen Sie Ihre Laptoptasche nicht im Auto, unbeaufsichtigt in einem Café, am Flughafen oder an anderen öffentlichen Orten.

4. **Updates**. Halten Sie Ihre Software und Geräte auf dem neuesten Stand, installieren Sie Updates des Betriebssystems, wenn Sie dazu aufgefordert werden.

5. **Schnell handeln**. Je nach Situation sollten Sie bei Verlust des Geräts nicht in Panik verfallen, sondern zunächst Ihr Passwort für die wichtigsten Systeme ändern, Ihren Vorgesetzten oder die IT-Abteilung informieren und ggf. die Polizei verständigen.
6. Wenn Sie ein altes Gerät, ein Telefon, Tablet oder einen Computer verkaufen, stellen Sie sicher, dass alle persönlichen Informationen dauerhaft von der Festplatte oder dem Speicher des Geräts gelöscht werden. Sie können spezielle Software wie Eraser, File Shredder oder WipeFile oder andere ähnliche Tools verwenden.

3.9. Internet of things (IoT)

Das Internet der Dinge (Internet of Things, IoT) ist ein System miteinander verbundener Computer, mechanischer und digitaler Maschinen, Objekte, Tiere oder Menschen, die mit eindeutigen Identifikatoren und der Fähigkeit ausgestattet sind, Daten über ein Netzwerk zu übertragen, ohne dass eine Interaktion von Mensch zu Mensch oder Mensch zu Computer erforderlich ist.

Diese neue Welle der Konnektivität geht über Laptops und Smartphones hinaus und führt zu vernetzten Autos, intelligenten Häusern, vernetzten Wearables, intelligenten Städten und einer vernetzten Gesundheitsversorgung. Im Grunde genommen, ein vernetztes Leben.

Die Idee von miteinander verbundenen Geräten, bei denen die Geräte intelligent genug sind, um Informationen mit uns, mit Cloud-basierten Anwendungen und untereinander (von Gerät zu Gerät) zu teilen.
Intelligente Geräte oder "**Connected Devices**", wie sie gemeinhin genannt werden, sind so konzipiert, dass sie jedes bisschen Daten, das im täglichen Leben geteilt oder verwendet wird, erfassen und nutzen. Und diese Geräte werden diese Daten nutzen, um mit Ihnen auf einer täglichen Basis zu interagieren und Aufgaben zu erledigen. Sie werden die Lücke zwischen der physischen und der digitalen Welt überbrücken, um die Qualität und Produktivität des Lebens, der Gesellschaft und der Industrie zu verbessern. Mit der Einführung der Apple Watch und weiteren Geräten, die noch hinzukommen werden, werden uns diese vernetzten Geräte in der vernetzten Welt halten.

10 Real-World-Anwendungen des Internet of Things (IoT) - erklärt in Videos

Anwendung	Erklärung	Video link
1. Smart Home	Smart Home ist zur revolutionären Erfolgsleiter in den Wohnräumen geworden und es wird vorhergesagt, dass	https://youtu.be/NjYTzvAVozo

	Smart Homes so alltäglich werden wie Smartphones. Smart-Home-Produkte versprechen, Zeit, Energie und Geld zu sparen	
2. Wearables	Wearable-Geräte sind mit Sensoren und Software ausgestattet, die Daten und Informationen über den Benutzer sammeln. Diese Daten werden später vorverarbeitet, um wichtige Erkenntnisse über den Benutzer zu gewinnen. Diese Geräte decken im Großen und Ganzen die Anforderungen in den Bereichen Fitness, Gesundheit und Unterhaltung ab. Die Voraussetzung der Internet-of-Things-Technologie für Wearable-Anwendungen ist, dass sie sehr energieeffizient oder extrem stromsparend sind und eine geringe Größe haben.	https://youtu.be/h8-TAqzYrno
3. Vernetzte Autos	Die digitale Technologie im Automobil hat sich auf die Optimierung der internen Funktionen des Fahrzeugs konzentriert. Doch jetzt wächst die Aufmerksamkeit auf die Verbesserung des Fahrerlebnisses im Auto. Ein vernetztes Auto ist ein Fahrzeug, das in der Lage ist, seinen eigenen Betrieb, seine Wartung sowie den Komfort der Passagiere mithilfe von Onboard-Sensoren und Internetkonnektivität zu optimieren. Die meisten großen Autohersteller sowie einige mutige Startups arbeiten an Connected-Car-Lösungen. Große Marken wie Tesla, BMW, Apple und Google arbeiten daran, die nächste Revolution im Automobilbereich zu bringen.	https://youtu.be/0HxZuQ0woLY
4. Internet für die Industrie	Das industrielle Internet ist der neue Trend in der Industrie, auch Industrial Internet of Things (IIoT) genannt. Es befähigt die Industrietechnik mit Sensoren, Software und Big-Data-Analysen, brillante Maschinen zu schaffen.	https://youtu.be/8NGzrtK7eV0

	Laut Jeff Immelt, CEO von GE Electric, ist IIoT ein "schönes, begehrenswertes und investierbares" Gut. Die treibende Philosophie hinter IIoT ist, dass intelligente Maschinen genauer und konsistenter als Menschen durch Daten kommunizieren können. Und diese Daten können Unternehmen helfen, Ineffizienzen und Probleme früher zu erkennen. IIoT birgt großes Potenzial für Qualitätskontrolle und Nachhaltigkeit. Anwendungen zur Warenverfolgung, Echtzeit-Informationsaustausch über Bestände zwischen Lieferanten und Einzelhändlern und automatisierte Lieferung werden die Effizienz der Lieferkette erhöhen. Laut GE wird die Verbesserung der Industrieproduktivität in den nächsten 15 Jahren weltweit 10 bis 15 Billionen US-Dollar an BIP generieren.	
5. Smart Cities	Smart City ist eine weitere leistungsstarke Anwendung des IoT, die die Neugierde der Weltbevölkerung weckt. Intelligente Überwachung, automatisierter Transport, intelligentere Energiemanagementsysteme, Wasserversorgung, städtische Sicherheit und Umweltüberwachung sind alles Beispiele für Anwendungen des Internets der Dinge für intelligente Städte. Das IoT wird die größten Probleme lösen, mit denen die Menschen in den Städten konfrontiert sind, wie z. B. Umweltverschmutzung, Verkehrsstaus und Energieknappheit usw. Produkte wie z. B. Smart Belly Mülltonnen, die mit Mobilfunkkommunikation ausgestattet sind, senden Warnungen an die städtischen Dienste, wenn eine Tonne geleert werden muss. Durch die Installation von Sensoren und die Nutzung von Webanwendungen können die Bürger freie Parkplätze in der ganzen Stadt finden. Außerdem können die	https://youtu.be/Br5aJa6MkBc

	Sensoren Zählermanipulationen, allgemeine Fehlfunktionen und Installationsprobleme im Stromsystem erkennen. Um die Funktionsweise von Smart Cities besser zu verstehen, sehen Sie sich dieses Video an.	
6. IoT in der Landwirtschaft	Mit dem kontinuierlichen Anstieg der Weltbevölkerung ist die Nachfrage nach Nahrungsmitteln extrem gestiegen. Regierungen unterstützen Landwirte dabei, fortschrittliche Techniken und Forschung einzusetzen, um die Nahrungsmittelproduktion zu steigern. Smart Farming ist einer der am schnellsten wachsenden Bereiche im IoT. Landwirte nutzen aussagekräftige Erkenntnisse aus den Daten, um eine bessere Rendite zu erzielen. Das Erfassen von Bodenfeuchtigkeit und Nährstoffen, die Steuerung des Wasserverbrauchs für das Pflanzenwachstum und die Bestimmung von maßgeschneidertem Dünger sind einige einfache Anwendungen des IoT. Wenn Sie neugierig geworden sind, erklärt Ihnen das folgende Video dieses Konzept näher. Lesen Sie mehr, um das Neueste über IoT in der Landwirtschaft zu erfahren.	https://youtu.be/q0FnMD2_0Fw
7. Intelligenter Handel	Das Potenzial des IoT im Einzelhandel ist enorm. IoT bietet Einzelhändlern die Möglichkeit, sich mit den Kunden zu verbinden, um das Erlebnis im Laden zu verbessern. Mit Smartphones können Einzelhändler mit ihren Kunden auch außerhalb des Geschäfts in Verbindung bleiben. Die Interaktion über Smartphones und die Verwendung von Beacon-Technologie kann Einzelhändlern helfen, ihre Kunden besser zu bedienen. Sie können auch die Wege der Kunden durch ein Geschäft verfolgen und das Ladenlayout	https://youtu.be/gUcuqhduWao

	verbessern sowie Premiumprodukte in stark frequentierten Bereichen platzieren. Sehen Sie sich dieses Video an, um herauszufinden, wie der vernetzte Einzelhandel Ihr Leben einfacher machen wird. Lesen Sie mehr über die neuesten Technologien, die das Gesicht des Einzelhandels verändern.	
8. Energie Engagement	Die Stromnetze der Zukunft werden nicht nur intelligent genug sein, sondern auch sehr zuverlässig. Das Konzept der intelligenten Stromnetze (Smart Grids) wird auf der ganzen Welt immer beliebter. Die Grundidee hinter den Smart Grids ist es, Daten auf automatisierte Weise zu sammeln und das Verhalten von Stromverbrauchern und -lieferanten zu analysieren, um die Effizienz sowie die Wirtschaftlichkeit der Stromnutzung zu verbessern. Smart Grids werden auch in der Lage sein, Quellen von Stromausfällen schneller und auf der Ebene einzelner Haushalte zu erkennen, wie z. B. ein nahegelegenes Solarpanel, wodurch ein dezentrales Energiesystem möglich wird. Hier ist ein Video, das erklärt, wie ein Smart Grid funktioniert.	https://youtu.be/JwRTpWZReJk
9. IOT in der Gesundheitsfürsorge	Das vernetzte Gesundheitswesen ist nach wie vor der schlafende Riese unter den Anwendungen des Internets der Dinge. Das Konzept eines vernetzten Gesundheitswesens und intelligenter medizinischer Geräte birgt enormes Potenzial nicht nur für Unternehmen, sondern auch für das Wohlbefinden der Menschen im Allgemeinen. Forschungen zeigen, dass das IoT im Gesundheitswesen in den kommenden Jahren massiv zunehmen wird. IoT im Gesundheitswesen zielt darauf ab,	https://youtu.be/8AkXW9EPFJg

	Menschen durch das Tragen von vernetzten Geräten zu einem gesünderen Leben zu befähigen. Die gesammelten Daten werden bei der personalisierten Analyse der Gesundheit eines Individuums helfen und maßgeschneiderte Strategien zur Bekämpfung von Krankheiten liefern. Das folgende Video erklärt, wie das IoT die Behandlung und medizinische Hilfe revolutionieren kann.	
10. IoT in der Geflügelzucht und Landwirtschaft	Bei der Überwachung von Viehbeständen geht es um Tierhaltung und Kosteneinsparungen. Mithilfe von IoT-Anwendungen zum Sammeln von Daten über die Gesundheit und das Wohlbefinden des Viehs können Viehzüchter, die frühzeitig über das kranke Tier Bescheid wissen, dieses herausziehen und eine große Anzahl kranker Rinder verhindern. Mit Hilfe der gesammelten Daten können Viehzüchter die Geflügelproduktion steigern. Sehen Sie sich dieses interessante Video an.	https://youtu.be/eZ2sVriiluU

4. Beispiele, Fallstudien und Vorkehrungen zur Entwicklung von Resilienz gegen

4.1. Datenschutzverletzungen und Datendiebstahl

Was ist eine Datenschutzverletzung?

1.Eine Datenverletzung ist ein Vorfall, bei dem Informationen gestohlen oder aus einem System entwendet werden, ohne dass der Eigentümer des Systems davon weiß oder dazu autorisiert ist. Ein kleines Unternehmen oder eine große Organisation kann von einer Datenverletzung betroffen sein.

2. Eine Datenschutzverletzung liegt vor, wenn jemand ohne Erlaubnis auf Informationen zugreift. Es beginnt mit einer Sicherheitsverletzung - dem Eindringen in ein geschütztes Computernetzwerk - und endet mit der Offenlegung oder dem Diebstahl von Daten. Diese Daten können persönlich identifizierbare Informationen wie Ihren Namen, Ihre Adresse, Ihre Sozialversicherungsnummer und Kreditkartendetails enthalten.

Was sind Ihre Datenschutzrisiken?

1. Datenschutz bezieht sich auf alle Rechte, die Sie haben, um Ihre persönlichen Informationen zu kontrollieren und wie diese Informationen verwendet werden. Ihre Informationen befinden sich an vielen Orten. Dazu gehören Regierungsbehörden, Organisationen des Gesundheitswesens, Finanzinstitute, Plattformen sozialer Netzwerke, Hersteller von Computer-Apps und viele andere Stellen.
2. Ihre Informationen haben einen Wert. Aus diesem Grund haben es Cyberkriminelle oft auf Organisationen abgesehen, bei denen sie persönliche Daten abgreifen können. Sie können damit Verbrechen wie Identitätsdiebstahl begehen oder sie im Dark Web verkaufen.
3. Eine weitere Gemeinsamkeit zwischen Datenschutzverletzungen und Datenverletzungen? Es gibt nicht viel, was Sie tun können, um sie zu verhindern. Die Sicherheit Ihrer Informationen liegt in den Händen von jemand anderem. Dennoch gibt es Dinge, die Sie tun können, um sich zu schützen?

Video: The Dangers of a Data Breach - https://www.youtube.com/watch?v=0kK902-ZvNM

Wie kann man eine Datenverletzung verhindern?

1. Erstellen Sie komplexe Passwörter. Verwenden Sie unterschiedliche für jedes Konto und ändern Sie Ihre Passwörter, wenn ein Unternehmen, mit dem Sie kürzlich interagiert haben, gehackt wurde.
2. Verwenden Sie die Multi-Faktor-Authentifizierung, wenn sie verfügbar ist. Diese erlaubt den Zugriff nur, wenn zwei oder mehr Beweise vorgelegt werden - in der Regel ein Passwort und ein Code, der dem Benutzer während der Anmeldung per Telefon, SMS oder E-Mail zugeschickt wird.

3. Kaufen Sie mit einer Kreditkarte ein. Sie haften möglicherweise weniger für betrügerische Kreditkartenabrechnungen.
4. Achten Sie auf Betrug. Wenn Sie eine Benachrichtigung über die Datenschutzverletzung erhalten, rufen Sie das Unternehmen an, um sich zu vergewissern, dass die Nachricht echt ist.
5. Schützen Sie sich vor Identitätsdiebstahl. Weltweit führen 65 % der Datenschutzverletzungen zu Identitätsdiebstahl und sind damit die häufigste Folge. Wenn Sie Opfer eines Identitätsdiebstahls werden, wenden Sie sich an jedes Kreditkartenunternehmen, um eine Betrugswarnung einzurichten und Ihre Konten zu sperren. Wenden Sie sich dann an Ihr örtliches Sozialversicherungsbüro, um die nächsten Schritte zu besprechen.
6. Richten Sie Kontowarnungen ein. Möglicherweise können Sie Benachrichtigungen über verdächtige Einkäufe oder solche, die einen bestimmten Dollarbetrag überschreiten, erhalten. Dies kann Ihnen eine Vorwarnung geben, dass Sie gehackt worden sind.

4.2. Hacken und Cyber-Erpressung

Hacken ist ein Versuch, ein Computersystem oder ein privates Netzwerk innerhalb eines Computers auszunutzen. Einfach ausgedrückt, handelt es sich um den unbefugten Zugriff auf oder die Kontrolle über die Sicherheitssysteme von Computernetzwerken zu einem unerlaubten Zweck.

Cyber-Erpressung ist ein Internet-Verbrechen, bei dem jemand elektronische Dateien oder Ihre Geschäftsdaten als Geisel hält, bis Sie ein gefordertes Lösegeld zahlen.

Video: Cyber Extortion - https://www.youtube.com/watch?v=UNCBuFJRrYk

Cyber-Erpressung ist eine Online-Kriminalität, bei der Hacker Ihre Daten, Website, Computersysteme oder andere sensible Informationen als Geisel halten, bis Sie ihre Zahlungsforderungen erfüllen. Dies geschieht häufig in Form von Ransomware und DDoS-Angriffen (Distributed Denial-of-Service), die beide Ihr Unternehmen lahmlegen können.

Cyber-Erpresser haben mehrere gängige Techniken, um in Ihre Computer-Hardware, -Software und -Netzwerke einzubrechen und sie lahmzulegen, bis Sie eine Gebühr zahlen.

Eine Taktik ist Ransomware, bei der ein Hacker einen Ihrer Mitarbeiter dazu verleitet, auf einen Link oder eine Datei in einer E-Mail-Nachricht zu klicken. Dadurch wird die Ransomware aktiviert, die sich im gesamten Netzwerk ausbreitet und Ihre Server und Daten verschlüsselt, sodass Sie nicht mehr auf Anwendungen und Dateien zugreifen können. Die einzige Möglichkeit, den Zugriff wiederherzustellen, besteht darin, den Hacker für einen Verschlüsselungsschlüssel zu bezahlen.

Bei so genannten DDoS-Angriffen (Distributed Denial of Service) nutzen Hacker ein Netzwerk von infizierten Computern, um eine überwältigende Flut von Nachrichten an Ihren Webserver zu senden, wodurch dieser effektiv außer Betrieb gesetzt wird, bis die Nachrichtenübermittlung aufhört.

Eine Cyber-Haftpflichtversicherung bietet Versicherungsschutz, um die finanziellen Auswirkungen dieser Angriffe zu mildern.

Viele Cyber-Haftpflichtversicherungspolicen decken Cyber-Erpressung ab, aber in der Regel nur durch einen Zusatz (d. h. einen Zusatz auf der Seite mit den Erklärungen Ihrer Police).

Solche Policen, die sogenannte First-Party-Cyber-Haftpflichtversicherung, bieten finanzielle Unterstützung für drei Zwecke.:

1. Um die Lösegeldforderung eines Hackers zu erfüllen.
2. Um erpressungsbedingte Ausgaben zu bezahlen, z. B. die Beauftragung eines Beraters zur Behebung eines Angriffs.
3. Um beschädigte Computerhardware oder Datenbanken wieder in den ursprünglichen Betriebszustand zu versetzen.

4.3. Identitätsdiebstähle

Identitätsdiebstahl ist das Verbrechen, sich die persönlichen oder finanziellen Informationen einer anderen Person zu beschaffen, um deren Identität zu benutzen, um Betrug zu begehen, wie z. B. nicht autorisierte Transaktionen oder Einkäufe zu tätigen. Identitätsdiebstahl wird auf viele verschiedene Arten begangen, und die Opfer erleiden in der Regel einen Schaden an ihrem Kredit, ihren Finanzen und ihrem Ruf. Identitätsdiebstahl liegt vor, wenn jemand Ihre persönlichen Informationen und Anmeldedaten stiehlt, um Betrug zu begehen. Es gibt verschiedene Formen des Identitätsdiebstahls, aber die häufigste ist die finanzielle. Der Schutz vor Identitätsdiebstahl ist eine wachsende Branche, die die Kreditauskünfte, finanziellen Aktivitäten und die Verwendung der Sozialversicherungsnummer von Personen verfolgt.

Video: What is Identity Theft? https://www.youtube.com/watch?v=kDFeSUUwRnA

Arten von Identitätsdiebstahl

1. **Finanzieller Identitätsdiebstahl**: Jemand nutzt die Identität oder Informationen einer anderen Person, um Kredite, Waren, Dienstleistungen oder Vorteile zu erhalten.
2. **Identitätsdiebstahl der Sozialversicherung**: Wenn Identitätsdiebe in den Besitz Ihrer Sozialversicherungsnummer gelangen, können sie diese zur Beantragung von Kreditkarten und Darlehen verwenden.
3. **Medizinischer Identitätsdiebstahl**: Jemand gibt sich als eine andere Person aus, um kostenlose medizinische Versorgung zu erhalten.
4. **Synthetischer Identitätsdiebstahl:** Ein Krimineller kombiniert echte (in der Regel gestohlene) und gefälschte Informationen, um eine neue Identität zu erstellen, mit der er betrügerische Konten eröffnet und betrügerische Einkäufe tätigt.
5. **Identitätsdiebstahl bei Kindern:** Jemand nutzt die Identität eines Kindes für verschiedene Formen der persönlichen Bereicherung.
6. **Steueridentitätsdiebstahl**: Jemand verwendet Ihre persönlichen Daten, einschließlich Ihrer Sozialversicherungsnummer, um eine gefälschte staatliche oder bundesstaatliche Steuererklärung in Ihrem Namen einzureichen und eine Rückerstattung zu erhalten.
7. **Strafrechtlicher Identitätsdiebstahl:** Ein Krimineller gibt sich während einer Verhaftung als eine andere Person aus, um zu versuchen, eine Vorladung zu vermeiden, die

Entdeckung eines auf seinen echten Namen ausgestellten Haftbefehls zu verhindern oder eine Verhaftungs- oder Verurteilungsakte zu vermeiden.

Video: Watch Out These 8 Types of Identity Theft

https://www.youtube.com/watch?v=EZa2um76rFY

Schutz bei Identitätsdiebstahl

Eine Möglichkeit ist, die Richtigkeit der persönlichen Dokumente ständig zu überprüfen und Unstimmigkeiten umgehend zu beseitigen. Es gibt verschiedene Dienste zum Schutz vor Identitätsdiebstahl, die Menschen dabei helfen, die Auswirkungen des Identitätsdiebstahls zu vermeiden und abzuschwächen. In der Regel stellen solche Dienste Informationen zur Verfügung, die den Menschen helfen, ihre persönlichen Daten zu schützen; sie überwachen öffentliche und private Aufzeichnungen, wie z. B. Kreditberichte, um ihre Kunden vor bestimmten Transaktionen und Statusänderungen zu warnen; und sie bieten den Opfern Unterstützung an, um ihnen bei der Lösung von Problemen im Zusammenhang mit Identitätsdiebstahl zu helfen. Einige Regierungsbehörden und gemeinnützige Organisationen bieten ähnliche Unterstützung an, in der Regel mit Websites, die Informationen und Tools zur Verfügung stellen, um Menschen zu helfen, Vorfälle von Identitätsdiebstahl zu vermeiden, zu beheben und zu melden. Viele der besten Kreditüberwachungsdienste bieten auch Tools und Dienste zum Identitätsschutz an.

4.4. Cyberbullying

Cybermobbing kann als eine aggressive, absichtliche und wiederholte Handlung definiert werden, die von einer Gruppe oder einem Einzelnen über elektronische Mittel wie Mobiltelefone oder das Internet gegen ein Opfer ausgeführt wird, das sich nicht leicht verteidigen kann (Slonje, Smith und Frisén, 2013).

Mobbing wird im Allgemeinen anhand von zwei Aspekten von anderen aggressiven Verhaltensweisen abgegrenzt. Der erste ist die Wiederholung, wie in der obigen Definition erwähnt, und der zweite ist das Machtungleichgewicht. Normalerweise ist es nicht die Absicht des Täters, die missbräuchliche Handlung zu wiederholen, aber aufgrund der exzessiven Nutzung von Technologie kann dies seiner Kontrolle entgleiten. Zum Beispiel kann ein Bild mit beleidigendem Inhalt einmal ins Internet gestellt werden, aber in der Folge mehrfach von anderen Personen geteilt werden, nicht von dem ursprünglichen Täter. Auf diese Weise ist eine Wiederholung vorprogrammiert und das Opfer wird mehrfach in Verlegenheit gebracht.

Was das Machtungleichgewicht in Bezug auf Cybermobbing betrifft, wird es nicht unbedingt auf physische oder psychische "Schwäche" bezogen, sondern auch auf die mangelnden Kenntnisse im Umgang mit IKTs und/oder die Anonymität, die der Cyberspace bietet (Slonje, Smith und Frisén, 2013). Bisherige Studien zeigen, dass es eine Korrelation zwischen Schülern mit fortgeschrittenen IKT-Kenntnissen und durchgeführten, delinquenten Online-Aktivitäten gibt. Was die Anonymität betrifft, so ist dem Opfer die Identität des Täters in der Regel nicht bekannt und es ist daher schwierig, ihm wirksam zu begegnen. (Slonje, Smith und Frisén, 2013).

Motive

Die Motive von Cybermobbing können in zwei Kategorien unterteilt werden: interne und externe. Zu den internen Motiven zählen Wut, Eifersucht, Rachegelüste oder auch Langeweile (Slonje, Smith und Frisén, 2013). Diese können auch auf gestörte Familienverhältnisse hinweisen. Des Weiteren kann das Cybermobbing-Verhalten dem Bedürfnis nach Machtausübung entsprechen (Nika, Gioldasi und Vitta, 2017). Bei den externen Motiven kann es sich entweder um das mögliche Ausbleiben ernsthafter Konsequenzen gegen den Täter handeln oder um die Tatsache, dass der Täter zögert oder Angst hat, in einer persönlichen Begegnung mit dem möglichen Opfer vorzugehen. (Slonje, Smith und Frisén, 2013).

Auswirkungen

1. Das Opfer und der Täter erleben zeitweise negative Emotionen wie Wut, Traurigkeit, Angst, Scham, Furcht, Selbstvorwürfe und mangelndes Selbstwertgefühl.
2. In Bezug auf den schulischen Kontext wurden negative Auswirkungen auf die Konzentration, schlechte schulische Leistungen, aber auch Abwesenheit von der Schule festgestellt (Šléglová und Cerna, 2011).
3. Die Opfer können sich so hilflos, einsam, beschämt und verzweifelt fühlen, dass sie sich zu einem Selbstmord entschließen können.
4. Sowohl Opfer als auch Täter können sozial ausgegrenzt sein, wodurch die oben genannten Gefühle verstärkt werden.
5. Die Opfer versuchen möglicherweise nicht, sich zu wehren, weil sie denken, dass dieses missbräuchliche Verhalten "normal" ist oder erwartet wird oder dass sie es verdienen, wenn sie sich minderwertig fühlen (Šléglová und Cerna, 2011).

Wege zum Gegensteuern

1. Es ist wirklich wichtig, dass sowohl Jugendliche als auch Erwachsene informiert sind und sich der Internetsicherheit und der funktionalen Unterschiede zwischen verschiedenen technischen Mitteln bewusst sind (Olweus, 2012).
2. Andere praktische Lösungen sind das Blockieren von unbekannten Personen in sozialen Medien und das häufige Ändern von Passwörtern und Benutzernamen.
3. Bitten Sie eine vertraute Person oder einen Experten um Hilfe (Slonje, Smith und Frisén, 2013). Öffnen Sie sich über eine schlechte Erfahrung, die Sie gerade machen oder die Sie in der Vergangenheit durchgemacht haben, und teilen Sie Ihre Gefühle mit. Dies wird Ihnen helfen, sich erleichtert zu fühlen, und es wird Ihnen leichter fallen, eine Lösung zu finden.
4. Eltern müssen aufgeschlossen sein und ihren Kindern grundsätzlich nahe stehen, damit diese sich frei fühlen, über Themen wie Cybermobbing und Cyberviktimisierung zu sprechen.
5. Beim Surfen im Internet ist es von entscheidender Bedeutung, sich der Rechte von Personen bewusst zu sein und diese zu respektieren.
6. Organisieren Sie Schulungen oder Seminare zum Thema Cybermobbing und Möglichkeiten, dem entgegenzuwirken.

Case studies

Brandy Vela (1998-2016), Alter 18, war ein High-School-Senior, der sich im November 2016 nach Jahren der Mobbing in Person und online von ihren Kollegen über ihr Gewicht getötet. Laut ihrer Schwester erstellten die Mobber Dating-Webseiten, auf denen sie über ihr Alter logen, ihr Bild hochstellten und ihre Telefonnummer benutzten, um Leuten zu sagen, dass sie sich kostenlos für Sex hergibt, um sie anzurufen. Brandy schoss sich mit einer Pistole in die Brust und starb am nächsten Tag im Krankenhaus. Nach ihrem Tod wurden ein paar Teenager verhaftet, weil sie sie gemobbt hatten (Wikipedia-Mitarbeiter, 2020).

Megan Meier (1992-2006), 13 Jahre alt, war ein amerikanischer Teenager aus Missouri, der sich wenige Wochen vor seinem vierzehnten Geburtstag durch Erhängen tötete. Ein Jahr später fanden ihre Eltern nach einer Untersuchung heraus, dass ihr Selbstmord auf Cyber-Mobbing über die Social-Networking-Website Myspace zurückzuführen war. Einzelpersonen beabsichtigten, Meiers Nachrichten zu nutzen, um mehr über sie zu erfahren und sie später zu demütigen (Wikipedia-Mitarbeiter, 2020).

Quellenangaben

Nika, D., Gioldasi, P., & Vitta, F. (2017). Cyber bullying) vs cyber stalking.

Olweus, D. (2012). Cyberbullying: An overrated phenomenon?. European journal of developmental psychology, 9(5), 520-538.

Šléglová, V., & Cerna, A. (2011). Cyberbullying in adolescent victims: Perception and coping. Cyberpsychology: journal of psychosocial research on cyberspace, 5(2).

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in human behavior, 29(1), 26-32.

Wikipedia contributors. (2020, November 27). List of suicides that have been attributed to bullying.Wikipedia.
https://en.wikipedia.org/wiki/List_of_suicides_that_have_been_attributed_to_bullying

4.5. Phishing Techniken

Phishing - betrügerische Aktivitäten, die darauf abzielen, persönliche und / oder andere vertrauliche Informationen zu stehlen (z. B. Identitätsdaten, Passwörter, Zahlungskartendetails usw.).

Normalerweise ist das Hauptziel von Phishing, an persönliche Daten und Anmeldeinformationen für das Online-Banking zu gelangen. Benutzer-IDs, Passwörter und andere Anmeldedaten ermöglichen es Betrügern, auf die Bankkonten von Personen zuzugreifen und aus der Ferne über die auf diesen Konten befindlichen Gelder zu verfügen (z. B. durch Überweisung dieser Gelder auf eigene Bankkonten).

Der Datendiebstahl erfolgt im Wesentlichen auf zwei Arten:

1. Direkte Kontaktaufnahme mit Einzelpersonen, um sie dazu zu bringen, solche Informationen bereitwillig preiszugeben;
2. Verwendung spezieller Technologien, die Daten von verschiedenen Websites oder Geräten kopieren, die zum Surfen im Internet und / oder zur Nutzung von Remote-Diensten verwendet werden.

Die häufigste Art des Phishings ist das sogenannte betrügerische Phishing.

In diesem Fall gibt sich ein Betrüger als legitime Institution oder Firma aus (z. B. Regierungsbehörde, Strafverfolgungsbehörde, Finanzdienstleister, großes bekanntes Markenunternehmen usw.) und wendet sich direkt an Einzelpersonen mit der Aufforderung, persönliche Daten einzugeben. Die gleiche E-Mail oder eine andere Art von Nachricht wird an Tausende von Personen gesendet, in deren Hoffnung, dass einige von ihnen darauf reagieren werden.

Solche Nachrichten fordern in der Regel dazu auf, sehr schnell zu reagieren, und weisen darauf hin, dass es unerwünschte negative Folgen haben könnte, wenn eine Person nicht rechtzeitig reagiert (z. B. wird die Institution rechtliche Schritte einleiten, Geldmittel von der Bank der Person könnten gestohlen werden, der Preis wird an eine andere Person vergeben usw.).

Meistens enthalten solche Nachrichten bösartige Links und / oder andere Verweise auf spezielle Websites, in denen die Personen aufgefordert werden, die angeforderten Informationen dort einzugeben. Sobald eine Person diese Informationen auf solchen Seiten angibt, werden sie für den Betrüger verfügbar.

Fortgeschrittene Betrüger können den Sitzungssteuerungsmechanismus ausnutzen und die Sitzung einer legitimen Website entführen. Wenn sich eine Person bei einer Webanwendung

anmeldet, setzt der Server ein temporäres Sitzungs-Cookie in ihrem Browser. Betrüger könnten solche Sitzungs-Cookies stehlen oder einer Person einen Link mit einer vorbereiteten Sitzungs-ID zur Verfügung stellen, bevor sie eine solche Authentifizierungssitzung betritt. Diese Aktionen ermöglichen es Betrügern später, die Sitzung zu kapern, indem sie dieselbe Sitzungs-ID für ihre eigene Browser-Sitzung verwenden.

Phishing-Methoden können auch durch das Erstellen von gefälschten E-Shops oder anderen Websites genutzt werden. Um solche Seiten auffällig zu machen, locken die Betrüger mit niedrigen Preisen, schneller Lieferung von Waren oder anderen Vorteilen. Es werden verschiedene Suchmaschinen verwendet, um die Zielgruppe zu erreichen und sie auf solche Seiten zu leiten. Die Daten werden gestohlen, während eine Zielperson versucht, sich auf solchen Seiten zu registrieren oder die Ware zu kaufen.

Betrüger können bestehende legitime Websites ausnutzen, indem sie eine IP-Adresse so ändern, dass sie zu einer gefälschten Website und nicht zu der Website, die eine Person besuchen wollte, weiterleitet.

Das Versenden von Links oder anderen Verweisen auf Dateien, die mit bestimmten Viren infiziert sind, ist ebenfalls eine sehr beliebte Technik. Solche Dateien infizieren Computer oder andere Geräte und können so programmiert sein, dass sie zur erneuten Eingabe von Passwörtern oder anderen Anmeldeinformationen auffordern, während sie sich mit Online-Banking oder anderen Remote-Diensten verbinden, nur um diese Informationen an Betrüger zu übertragen.

Erstens, es ist wichtig zu verstehen und sich bewusst zu sein, dass Phishing und Datendiebstähle überall, in jeder Form und zu jeder Zeit stattfinden können, daher müssen Sie ständig aufmerksam und wachsam sein.

Zweitens, treffen Sie Vorkehrungen, um die von Ihnen verwendeten Geräte sicher zu halten:

1. Verwenden Sie Tools und Software, die dazu beitragen, Ihren Computer oder ein anderes Gerät sicher zu halten (Antivirenprogramme usw.). Laden Sie solche Tools oder Software nur von offiziellen und vertrauenswürdigen Quellen herunter. Aktualisieren Sie diese Tools und Software rechtzeitig.
2. Vermeiden Sie es, obskure und unzuverlässige Sites zu besuchen, sich auf solchen Sites zu registrieren oder Dateien von ihnen herunterzuladen. Solche Sites können Links oder Dateien enthalten, die Ihren Computer oder ein anderes Gerät mit Viren infizieren können, die Ihre persönlichen Daten erfassen.
3. Melden Sie sich nach der Nutzung Ihres persönlichen Kontos ab und schließen Sie das Browserfenster.
4. Wählen Sie sichere und starke Passwörter, die aus Zahlen, Buchstaben und anderen Symbolen bestehen. Verwenden Sie keine leicht zu erratenden Passwörter (z. B. 12345, nur Ihren Vor- oder Nachnamen oder Ihr Geburtsdatum). Falls Sie

mehrere verschiedene Konten haben, verwenden Sie immer unterschiedliche Passwörter.

5. Wählen Sie beim Erstellen von Konten oder E-Mails Dienstanbieter, die Zwei-Faktor-Authentifizierungssysteme verwenden (z. B. ein Passwort und eine Telefonnummer)..

Drittens: Beachten Sie, dass seriöse Institutionen und Dienstleistungsunternehmen (z. B. Banken oder andere Finanzdienstleister) ihre Kunden nicht auffordern, ihre Login-Passwörter oder andere Anmeldedaten preiszugeben. Solche Informationen sind persönlich und nur Sie dürfen sie kennen. Wenn solche Informationen Dritten bekannt werden, müssen Sie diese Dienstleister unverzüglich über diesen Umstand informieren und Ihre Passwörter oder andere Anmeldedaten ändern.

Viertens: Wenn Sie eine Anfrage nach sensiblen Informationen erhalten, achten Sie auf diese Umstände:

1. **Die Adresse des Absenders**. Prüfen Sie, ob die Angaben zur Institution / Firma in E-Mails oder anderen Nachrichten mit den Daten übereinstimmen, die auf deren offiziellen Websites oder anderen öffentlichen Quellen veröffentlicht sind. Institutionen / Unternehmen verwenden in der Regel ihre eigenen Postfächer anstelle von öffentlich zugänglichen allgemeinen Postfächern (z. B. @gmail.com, @yahoo.com, etc.).

2. **Textqualität und Inhalt**. Täuschende E-Mails oder Nachrichten enthalten oft Schreib- oder Stilfehler. Der Text kann wörtlich übersetzt werden, ohne die Regeln der jeweiligen Sprache zu beachten (durch Verwendung öffentlich zugänglicher Übersetzungsprogramme). Der Text kann auch die Haushaltssprache, ungenaue Namen oder Rechtsformen von Institutionen oder Unternehmen verwenden (z. B. kann eine Behörde als Unternehmen bezeichnet werden). Gründe oder andere Umstände für die Kontaktaufnahme mit Ihnen können so beschrieben werden, dass sie an jede Situation angepasst werden können (z. B. informiert Sie angeblich die Polizei darüber, dass Ihre Zugangsdaten zu den Bankdiensten gestohlen wurden und Sie diese sofort ändern müssen, nennt aber nicht einmal die Bank).

3. **Links, die angeboten werden**. Betrügerische Links enthalten oft eine Reihe von Zahlen oder unbekannte Webadressen. Wenn Sie nicht sicher sind, dass ein Link legitim ist, klicken Sie ihn nicht an.

4. **Wahrscheinlichkeit, dass Sie die Anfrage oder das Angebot erhalten**. Sie sollten einschätzen, ob Sie ein solches Schreiben erwarten konnten und ob es mit den tatsächlichen Gegebenheiten oder der üblichen Praxis übereinstimmt (z. B. Sie erhalten eine E-Mail, dass Sie im Lotto gewonnen haben, obwohl Sie an keiner Lotterie teilgenommen haben; Sie erhalten eine Nachricht, die angeblich von Ihrer Bank stammt, obwohl diese niemals Nachrichten in dieser Art verschickt).

Wenn Sie Zweifel an einer E-Mail oder einer Nachricht haben, die Sie erhalten haben, wenden Sie sich an die Institution / das Unternehmen (das Sie angeblich erreicht hat) über die

Kontaktdaten, die öffentlich auf der offiziellen Website oder einer anderen zuverlässigen Quelle verfügbar sind.

4.6. Finanzkriminalität und Anlagebetrug

Finanzverbrechen sind Verbrechen, bei denen kriminelle Organisationen finanziell profitieren. Bei Finanzdelikten erbringt in der Regel eine Partei einen finanziellen Vorteil, und die andere Partei erleidet einen finanziellen Verlust. Sie werden häufig zum persönlichen Vorteil des Kriminellen begangen und beinhalten die illegale Umwandlung des Eigentums an dem betreffenden Objekt.

Von "Verbraucherbetrug" spricht man, wenn jemand einen finanziellen Verlust erleidet, der mit der Anwendung trügerischer, unfairer oder falscher Geschäftspraktiken einhergeht. In den vergangenen zwei Jahren haben beispielsweise 60 % der europäischen Verbraucher, die in einem Zeitraum von 12 Monaten online eingekauft haben, einen Betrug erlebt. Trotz strenger Cybersicherheitsmaßnahmen von Finanzinstitutionen (Banken, Zahlungsunternehmen usw.) setzen sich Betrüger immer wieder durch, indem sie das schwächste Glied in der Kette ausnutzen: den Menschen und seine Vorliebe, seinesgleichen zu vertrauen.

Die häufigsten Arten von Betrug:

Phishing – E-Mails und Telefonanrufe, in denen sich die Betrüger als seriöse Institution ausgeben, um an persönliche Daten ihrer Opfer zu gelangen.

Pharming – Wenn Verbraucher von offiziellen, legitimen Websites auf gefälschte Websites umgeleitet werden, mit dem Ziel, persönliche und sensible Daten zu stehlen.

Manipulation des Gerätes – Hacking von POS-Systemen (Point-of-Sale), Geldautomaten. Smartphones oder PCs, um auf Daten und/oder Geld zuzugreifen.

Identitätsbetrug – Verwendung der persönlichen Daten von Verbrauchern, um Kreditkarten zu kündigen, Passwörter zu ändern, Konten zu eröffnen usw.

Social engineering – Manipulation von Opfern, um vertrauliche Informationen zu erhalten.

Geldkuriere – Unschuldige Menschen dazu verleiten, gestohlenes oder illegales Geld über ihr Bankkonto zu waschen.

Wie Sie vermeiden, Opfer eines Finanzbetrugs zu werden:

1. Überprüfen Sie Ihr Bankkonto regelmäßig und melden Sie verdächtige Aktivitäten an Ihre Bank.
2. Denken Sie daran, dass Ihre Bank Sie niemals per Telefon oder E-Mail nach sensiblen Informationen (z. B. Online-Kontozugangsdaten) fragen wird.
3. Wenn Sie glauben, dass Sie Ihre Kontodaten an einen Betrüger weitergegeben haben, kontaktieren Sie sofort Ihre Bank.
4. Führen Sie Online-Zahlungen nur auf sicheren Websites durch: Achten Sie in der URL-Leiste auf das Vorhängeschloss und https und verwenden Sie nur sichere Verbindungen (Mobilfunknetz statt öffentliches Wi-Fi).
5. Wenn ein Angebot zu gut klingt, um wahr zu sein, ist es fast immer ein Betrug.
6. Bewahren Sie Ihre persönlichen Daten sicher und geschützt auf.

7. Seien Sie sehr vorsichtig, wie viele persönliche Informationen Sie in sozialen Netzwerken preisgeben. Betrüger können Ihre Informationen und Bilder verwenden, um eine falsche Identität zu erstellen oder Sie mit einem Betrug anzusprechen.

8. Melden Sie jeden mutmaßlichen Betrugsversuch immer der Polizei, auch wenn Sie nicht Opfer des Betrugs geworden sind.

Bei Anlagebetrug handelt es sich um den illegalen Verkauf oder vorgetäuschten Verkauf von Finanzinstrumenten. Die typischen Anlagebetrugsschemata sind durch das Angebot von risikoarmen oder risikolosen Anlagen, garantierten Renditen, übermäßig gleichmäßigen Renditen, komplexen Strategien oder nicht registrierten Wertpapieren gekennzeichnet.

Arten von Investitionsbetrug:

Von einem **Schneeballsystem** spricht man, wenn Betrüger behaupten, dass sie eine kleine Investition innerhalb kurzer Zeit in große Gewinne verwandeln können. In Wirklichkeit verdienen die Teilnehmer jedoch Geld, indem sie neue Teilnehmer für das Programm gewinnen. Die Betrüger, die hinter diesen Programmen stehen, geben sich in der Regel große Mühe, ihre Programme als legitime Multi-Level-Marketing-Programme erscheinen zu lassen.

Von einem Schneeballsystem spricht man, wenn ein Betrüger oder ein "Hub" Geld von neuen Investoren einsammelt und es dazu verwendet, angebliche Renditen an Investoren aus früheren Phasen zu zahlen, anstatt das Geld wie versprochen zu investieren oder zu verwalten. Wie bei Schneeballsystemen ist auch bei Ponzi-Schemata ein ständiger Zustrom von Geld erforderlich, um sich über Wasser zu halten. Aber im Gegensatz zu Schneeballsystemen müssen Investoren in einem Schneeballsystem normalerweise keine neuen Investoren anwerben, um einen Anteil am "Gewinn" zu verdienen.

Pump-and-Dump ist ein Schema, bei dem ein Betrüger absichtlich Aktien einer sehr günstigen Aktie eines kleinen, wenig gehandelten Unternehmens kauft und dann falsche Informationen verbreitet, um das Interesse an der Aktie zu wecken und den Aktienkurs zu erhöhen. In dem Glauben, ein gutes Geschäft mit einer vielversprechenden Aktie zu machen, erzeugen Investoren eine Kaufnachfrage zu immer höheren Preisen. Der Betrüger wirft dann seine Aktien zu dem hohen Preis ab und verschwindet, so dass viele Leute mit wertlosen Aktien erwischt werden.

Advance Free Fraud ist eine Art von Betrug, die mit der Hoffnung eines Anlegers spielt, einen früheren Investitionsfehler durch den Kauf einer preisgünstigen Aktie rückgängig machen zu können. Der Betrug beginnt in der Regel mit einem Angebot, Ihnen einen verlockend hohen Preis für wertlose Aktien zu zahlen. Um das Angebot anzunehmen, müssen Sie eine Gebühr im Voraus überweisen, um die Dienstleistung zu bezahlen. Wenn Sie dies jedoch tun, sehen Sie dieses Geld - oder irgendetwas von dem Geld aus dem Geschäft - nie wieder..

Wie Sie vermeiden, Opfer eines Anlagebetrugs zu werden:

1. Überprüfen Sie die Lizenz der Person, die die Anlage verkauft
2. Prüfen Sie, ob die Investition registriert ist
3. Hüten Sie sich vor Versprechungen von hohen Renditen und/oder schnellen Gewinnen
4. Seien Sie misstrauisch bei Verkäufen unter hohem Druck

5. Hüten Sie sich vor unaufgeforderten Angeboten
6. Verlangen Sie einen Prospekt oder ein Emissionsprospekt
7. Sprechen Sie mit einer dritten Person
8. Achten Sie auf Online-Betrügereien

4.7. Fake News und Propaganda

Propaganda wird definiert als bewusste und konsequente Verbreitung von Theorien und Ideen in Philosophie, Wissenschaft, Religion usw., um die Menschen zu erziehen, ihre Ansichten und Stimmungen zu beeinflussen, sie zu manipulieren und bestimmte Handlungen zu fördern, die zu den vom Propagandisten verfolgten Zielen beitragen würden. Propaganda zielt darauf ab, die Gefühle und Meinungen der Zielgruppe zu beeinflussen.

Die Wirksamkeit der Propaganda wird dadurch erhöht, dass sie teilweise die Wahrheit sagt, aber nicht alle Informationen liefert und Fakten verschleiert. Daher kann es manchmal schwierig sein, Propaganda zu erkennen. Propaganda stellt bestimmte korrekte Fakten dar, verändert oder verzerrt aber den gesamten Kontext. Die Richtigkeit der dargestellten Fakten kann überprüft werden, so dass die von der Propaganda vermittelte Botschaft wahr zu sein scheint. Dies soll jedoch irreführend sein.

Propaganda wird häufig in einem negativen Kontext als ein inakzeptables, auf Desinformation basierendes Mittel zur Beeinflussung der öffentlichen Meinung definiert. Synonyme zur Beschreibung von Propaganda sind unter anderem Lüge, Täuschung, Verzerrung, Manipulation, Gehirnwäsche, Gedankenkontrolle und psychologische Kriegsführung.

Propaganda wird jedoch auch zu Marketing-, sozialen und erzieherischen Zwecken eingesetzt, d. h. Propaganda kann auch in einem positiven Kontext funktionieren, und das Wichtigste ist, wofür sie eingesetzt wird. Ein Beispiel dafür sind die Darstellungen der Schädlichkeit des Rauchens auf Zigarettenschachteln. Sie ist auch Propaganda, weil sie versucht, Menschen mit Emotionen zu beeinflussen und ihr Verhalten zu ändern, d. h. sie zu zwingen, mit dem Rauchen aufzuhören. Am häufigsten wird Propaganda jedoch für negative Zwecke eingesetzt, um Hass und Feindseligkeit zu schüren.

Propaganda wird ständig von sozialen, technologischen, kulturellen und wirtschaftlichen Veränderungen beeinflusst. Sie muss sich daher anpassen und in einer Weise handeln, die der Persönlichkeit des modernen Menschen entspricht. Propaganda wird oft mit den Plakaten des Zweiten Weltkriegs in Verbindung gebracht, aber sie hat inzwischen eine Vielzahl subtilerer Formen angenommen. Die Art und Weise, wie sie funktioniert, kann so offensichtlich sein wie ein Hakenkreuz oder so subtil wie ein Kommentar in einem Nachrichtenportal.

Je nach Objektivität lässt sich Propaganda in weiß, grau und schwarz einteilen.

Weiße Propaganda ist die transparenteste und offenste Darstellung von Fakten. Sie wird für verschiedene soziale Programme und Initiativen verwendet. Weiße Propaganda versucht, die Ergebnisse unabhängiger Experten zu präsentieren, die die wichtigsten Ansichten widerspiegeln.

Angesichts des rasant zunehmenden Wettbewerbs zwischen verschiedenen öffentlichen und wirtschaftlichen Organisationen wird es jedoch immer schwieriger, die Fairness des Ansatzes zu bestimmen, und die Ansichten von Experten zu denselben Themen unterscheiden sich immer mehr. Wir bezeichnen daher als weiße Propaganda die Absicht, begründete Erklärungen zu liefern, ohne dabei die Tatsachen zu verfälschen.

Meistens wird in der weißen Propaganda über die Errungenschaften eines Landes, eines Unternehmens oder einer Organisation gesprochen, und sie ist positiv. Beispielsweise wirbt die Republik Litauen für sich selbst und stellt sich als Brücke zwischen dem Westen und dem Osten dar, in der ein investitionsfreundliches Klima herrscht und finanzielle Sicherheit gewährleistet ist. Dies ist Propaganda, obwohl sie auf korrekten Informationen aus offiziellen Quellen beruht.

Graue Propaganda. Ihre Vertreter verbinden absichtlich die bestätigten Fakten mit den unbestätigten, präsentieren nur eine Interpretation zu ihren Gunsten und verzerren absichtlich den Kontext des Ereignisses. Graue Propaganda wird intensiv bei gelenkten informatorischen, politischen oder wirtschaftlichen Konflikten eingesetzt.

Graue Propaganda stellt eine einseitige Annäherung an das Thema dar und vermeidet Kritik. Eine solche Propaganda behauptet zum Beispiel, dass die eigene Armee immer Recht hat. Vertreter dieser Propaganda vermeiden den offenen Dialog, der in einer Enthüllung enden könnte, halten aber dennoch nicht an einer einseitigen Lüge fest und lassen ihrer Haltung die Möglichkeit, sich zu ändern.

Graue Propaganda ist in den russischen Fernsehkanälen ORT und RTV während der Präsidentschaft Wladimir Putins weit verbreitet, wenn jede Information über Putin und Russland positiv dargestellt wird, auch wenn das internationale Forum Russland für bestimmte Entscheidungen scharf kritisiert.

Schwarze Propaganda beruht auf der absichtlichen Verfälschung von Ereignissen und Fakten, d. h. auf Lügen. Besonders verbreitet war sie in Nazi-Deutschland, wo Methoden der Ereignisinszenierung eingesetzt wurden. Die Nazis z. B. zogen in Uniformen sowjetischer Soldaten verkleidet durch polnische Dörfer und schüchterten die Einwohner mit der drohenden kommunistischen Herrschaft und deren Folgen ein.

Schwarze Propaganda stützt sich auch auf schwarze Technologie. So werden z. B. während einer Wahl Informationen im Namen des Gegners verbreitet oder Ereignisse so inszeniert, dass sie später die Wahlchancen des Gegners erheblich erschweren. Schwarze Propaganda und schwarze Technologie werden in vielen Demokratien verfolgt.

Die Propagandakommunikation ist daher in der Regel nicht völlig objektiv und stellt Fakten selektiv dar, um Einstellungen zu beeinflussen. Oft wird eine überladene Sprache verwendet, um eine emotionale Reaktion auf die dargebotenen Informationen hervorzurufen und nicht den Verstand.

Im digitalen Zeitalter, in dem wir heute leben, findet dieser bewusste Versuch, parteiische Informationen zu verbreiten, auch auf digitalen Plattformen statt. Sein Ziel ist es, in die Irre zu führen und zu täuschen. Wir können also getrost von "digitaler Propaganda" sprechen (Bjola, 2018, S. 307).

Als sich der Propagandaprozess in den Online-Raum verlagerte, entstanden neue Formen der Propaganda, die als **Trolle und Bots** bekannt sind. Ihr Ziel ist es, Wahlergebnisse zu beeinflussen, politische Gegner zu demoralisieren, zu diskreditieren

oder zu isolieren, an Meinungsumfragen teilzunehmen und Propaganda und falsche Nachrichten zu verbreiten.

Trolle sind Zehntausende von Menschen, die von Propagandisten angeheuert werden, um den ganzen Tag (oder die Nacht) auf den Nachrichtenportalen der Zielgruppe und in den sozialen Netzwerken zu arbeiten, um die neuesten Nachrichten und Beiträge zu kommentieren und einen Hengst unter den Internetnutzern aufzuziehen, Fehlinformationen zu verbreiten und die vorherrschenden Werte und Einstellungen zu verachten (Grigaliūnas, 2016).

Wie erkennt man einen Troll?

Einträge oder Nachrichten mit pro-russischem Inhalt;

● Rechtschreibfehler;

● Oft ein weibliches Benutzerkonto;

● Geringe Anzahl von Followern;

● Teilen von Nachrichten unter dem Namen einer bestimmten Person, wie z. B. @putin_leader;

● Behauptet, sich auf alternative Quellen zu beziehen, gibt diese aber nicht an;

● Kommentiert oder teilt Beiträge, Beiträge nur zu einem bestimmten Thema.

Ein Bot ist ein Computerprogramm, das automatisch bestimmte Aktionen ausführt, die ein Mensch am Computer ausführen kann. In der Propaganda werden Bots eingesetzt, um Propagandakommentare auf Nachrichtenportalen und Beiträge in sozialen Netzwerken zu schreiben. Diese Programme generieren verschiedene Kommentare: Es wird eine Vorlage erstellt und ein neuer Kommentar wird aus dieser Vorlage generiert. Proxy-Server liefern verschiedene IP-Adressen, so dass es den Anschein hat, dass viele verschiedene Personen Kommentare schreiben. Zum Beispiel sind etwa 15 Prozent der Nutzer des sozialen Netzwerks Twitter Bots.

Wie erkennt man einen Bot?

● Achten Sie auf das Profilfoto. In der Regel handelt es sich dabei um Zeichnungen, Bilder aus der Natur, Fotos von Politikern oder Prominenten oder gar keine Profilfotos. Sie können die Herkunft eines Profilfotos mit der Google-Bildersuche herausfinden.

● Langer Nutzername. Der Nutzername vieler Bots ist ungewöhnlich, mit Zahlen oder ohne jegliche Bedeutung.

● Generische Inhalte oder doppelte Beiträge oder Nachrichten. Bots sind darauf ausgelegt, ein bestimmtes Thema oder Tag # in sozialen Netzwerken zu dominieren. Um dies zu erreichen, wird eine Nachricht oder ein Beitrag viele Male geteilt.

● Das Benutzerkonto ist leer. Von Menschen erstellte Benutzerkonten enthalten viele persönliche Informationen, von Bots erstellte - keine oder nur grundlegende Informationen.

● Bots folgen weit mehr Personen in sozialen Netzwerken, als sie selbst Follower haben.

● Bots teilen viele Beiträge und Nachrichten. Wenn ein Nutzer ständig viele Einträge teilt, auch nachts, besteht eine gute Chance, dass es sich um einen Bot handelt.

● Bots teilen Beiträge oder Nachrichten mit radikalen politischen Inhalten. Dabei handelt es sich in der Regel um ideologische Klischees, patriotische und militaristische Texte, die sich gegen die herrschenden Werte und Einstellungen richten.

● Viele stereotype Aufnahmen, wie z. B. Stimmungen, Videos mit Tieren usw., im Nachrichten-Feed des Nutzers. Solche Inhalte werden von Bots in den Pausen zwischen Wahlen oder anderen relevanten Ereignissen verwendet.

Sie können hier überprüfen, ob Sie keine Bots im sozialen Netzwerk Twitter verfolgen: https://botcheck.me

Übrigens: Es gibt nicht nur Trolle, sondern auch Elfen. Dabei handelt es sich in der Regel um aktive und bürgerliche Personen, die verschiedene Fehlinformationen und Manipulationen aufdecken und die Verbreiter von Falschnachrichten und Propaganda im Online-Raum bekämpfen.

Beeinflussungsmittel, die als Propaganda verwendet werden können

Die Verallgemeinerung ist ein Versuch, durch Abstraktionen Gefühle zu beeinflussen; sie ist eine der einfachsten Formen der Propaganda. Diese Methode wird häufig im Wahlkampf von Politikern eingesetzt. Besonders wirksam ist diese Methode in schwierigen Zeiten, z. B. in einer Wirtschaftskrise. Häufig werden emotionale, zusammenfassende Aussagen verwendet, wie z. B. Wir verdienen es, besser zu leben, Für die Zukunft wird Ordnung sein, Jeder Mensch ist von größter Bedeutung usw.

Symbole helfen dabei, das eigene Image zu verbessern. So ist beispielsweise eine Person auf einem Foto von bestimmten symbolischen Gegenständen umgeben, die das Bild vermitteln, dass diese Person die symbolisierten Werte vertritt.

Etikettierung bedeutet, dass eine negative Idee, Handlung oder ein Begriff mit einer bestimmten Person, Organisation usw. in Verbindung gebracht wird. Oft wird Sarkasmus oder Spott verwendet. Dies ist ein wirksames Propagandamittel, denn hartnäckige Etikettierungen - Lügner, Terroristen, Korrupte - lassen sich nur schwer wieder loswerden.

Das Gefühl der Herde vermittelt den Eindruck, dass die Idee weit verbreitet ist, so dass eine Ablehnung das Risiko birgt, isoliert und deplatziert zu sein.

Emotionale Erregung versucht, starke Gefühle wie Angst, Wut, Traurigkeit und Groll hervorzurufen. Am häufigsten wird versucht zu zeigen, dass das eine oder andere Phänomen negative Folgen haben wird, wobei eine Vielzahl menschlicher Ängste verwendet wird.

Beim Kartenstapeln werden nur positive Fakten erzählt und negative Fakten unterdrückt. Obwohl die bei dieser Technik verwendeten Argumente in der Regel stichhaltig sind, werden oft Statistiken präsentiert, die die Situation verzerren können, weil Informationen aus dem Zusammenhang gerissen oder wichtige Fakten weggelassen werden. In politischen Kampagnen wird ein Kandidat nur auf der positiven Seite dargestellt, während die negativen Fakten weggelassen werden.

C.R.A.P. test

Eine schnelle Überprüfung der Richtigkeit der Informationen auf der Website kann mit dem C.R.A.P.-Test (Currency, Reliability, Authority, and Purpose / Point of View) durchgeführt werden. Dieser Test ermöglicht es, herauszufinden, wann und unter welchen Umständen der veröffentlichte Text geschrieben wurde, wie zuverlässig sein Autor ist und schließlich den Zweck und die Einstellung dieser Informationen (CyberWise, 2019).

Währung ● Wie aktuell sind die Informationen? ● Wie kürzlich wurde die Website aktualisiert? ● Ist sie aktuell genug für Ihr Thema?
Verlässlichkeit ● Welche Art von Informationen sind in der Ressource enthalten? ● Ist der Inhalt der Ressource hauptsächlich Meinung? Ist er ausgewogen? ● Gibt der Ersteller Referenzen oder Quellen für Daten oder Zitate an?
Autorität ● Wer ist der Ersteller oder Autor? ● Was sind die Referenzen? Können Sie Informationen über den Hintergrund des Autors finden? ● Wer ist der Herausgeber oder Sponsor? ● Ist er seriös? ● Welches Interesse hat der Herausgeber (wenn überhaupt) an diesen Informationen? ● Gibt es Werbung auf der Website? Wenn ja, sind sie klar gekennzeichnet?
PZweck/Standpunkt ● Handelt es sich um Fakten oder Meinungen? Führt der Autor Quellen oder Verweise auf? ● Ist er parteiisch? Scheint der Autor zu versuchen, eine Agenda oder eine bestimmte Seite zu unterstützen? ● Versucht der Ersteller/Autor, Ihnen etwas zu verkaufen? Wenn ja, wird dies deutlich gemacht?

Wege zum Gegensteuern

Bei so vielen Informationen, die auf allen digitalen Plattformen verfügbar sind, ist es leicht, getäuscht zu werden. Studien zeigen, dass ca. 75 % der Menschen, die Fake News sehen, nicht in der Lage sind, zu erkennen, dass diese tatsächlich gefälscht sind. Eine schnelle Möglichkeit zu überprüfen, ob eine Information echt ist oder nicht, ist daher der C.R.A.P.-Test. Finden Sie

heraus, ob der Artikel aktuell und seriös ist, ob der Autor glaubwürdig ist und schließlich den Zweck und die Sichtweise des Artikels (CyberWise, 2019). Auf jeden Fall ist immer gesunder Menschenverstand gefragt. Einige Möglichkeiten, Fake News zu erkennen, werden im Folgenden kurz dargestellt (How to Spot Fake News, n.d.).

1. Betrachten Sie die Quelle: Versuchen Sie, mehr über die Quelle zu erfahren und überlegen Sie, ob sie glaubwürdig ist.

2. Lesen Sie weiter: Schlagzeilen können skandalös sein, um mehr Klicks zu erhalten. Suchen Sie weitere Informationen über die erzählte Geschichte und versuchen Sie, die Wahrheit herauszufinden.

3. Überprüfen Sie den Autor: Hat der Autor außer dem aktuellen Beitrag noch weitere Beiträge verfasst? Hat er irgendwelche Kommentare oder Urteile über seine Glaubwürdigkeit erhalten?

4. Unterstützende Quellen: Normalerweise listet eine Website andere Links auf, die sich auf das Thema des angegebenen Artikels beziehen. Prüfen Sie, ob diese Links wirklich mit dem ursprünglichen Artikel in Verbindung stehen oder ob sie nur irreführend sind.

5. Prüfen Sie das Datum: Ist die Information aktuell oder wurde sie neu veröffentlicht?

6. Ist es ein Scherz? Falls die Informationen wirklich skurril sind, könnte es sich um Satire handeln. Prüfen Sie noch einmal den Autor und die Quelle, um sicher zu gehen.

7. Überprüfen Sie Ihre Vorurteile: Überlegen Sie, ob die Nachrichten, die Sie lesen, Ihre eigenen Vorurteile beeinflussen. Möglicherweise lehnen Sie sie ab, weil Sie nicht einverstanden sind. Aber das macht die Nachricht nicht zu einer Fälschung.

8. Fragen Sie die Experten: Es gibt einige Fact-Checking-Seiten, die Sie besuchen können, um sicher zu sein, dass die Informationen stimmen.

Es gibt zwei weitere wesentliche Bereiche, die wir beachten müssen, wenn wir Fake News erkennen wollen. Der erste ist die Faktizität und der zweite ist die unmittelbare Intention des Autors. Faktizität bezieht sich auf den Grad, in dem Nachrichten die Realität widerspiegeln. Satire zum Beispiel präsentiert reale Fakten, aber in einem differenzierten Kontext, während Parodien fiktive Inhalte präsentieren (Tandoc et al., 2017, S. 142). Die unmittelbare Absicht des Autors bezieht sich auf den Grad, in dem der Autor beabsichtigt, das Publikum falsch zu informieren und in die Irre zu führen. Er könnte das Publikum wirklich täuschen und in die Irre führen wollen, aber er könnte auch düpiert sein und somit Fake News übertragen.

Case studies

Ein Beispiel für eine Propagandakampagne ist die zwischen Russland und den Vereinigten Staaten von Amerika in Bezug auf die Präsidentschaftswahlen von 2016. Der Hauptgrund für die Gestaltung der Wahlergebnisse war das Erscheinen einer Vielzahl von Fake News, um die amerikanischen Bürger dazu zu bringen, für Trump zu stimmen. Cambridge Analytica, ein Unternehmen, das sich auf die Analyse von Daten und die Erstellung von psychologischen Profilen für politische Zwecke unter Verwendung von Daten amerikanischer Facebook-Nutzer spezialisiert hat, stellte im Vorfeld der Präsidentschaftswahlen die Wahlprofile von Tausenden von Menschen zusammen, um Donald Trumps Wahlkampf zu unterstützen. Facebook-Nutzer, die analysiert wurden, wurden in zwei Kategorien eingeteilt. Die erste

umfasste Wähler, die beabsichtigten, für Trumps Gegner zu stimmen, während die zweite diejenigen umfasste, die beabsichtigten, sich zu enthalten. Danach folgte eine gezielte Fake-News-Kampagne über Hillary Clinton. Die "Nachrichten", die den Wählern der ersten Klasse präsentiert wurden, sollten sie davon überzeugen, nicht zu wählen, während diejenigen, die auf dem Handy der zweiten Klasse zu sehen waren, sie dazu bringen sollten, für Trump zu stimmen. Laut einer Studie der Stanford University gingen 41 % der Fake News im letzten Monat vor der Wahl viral. Facebook hat offiziell zugegeben, dass 126 Millionen Amerikaner, etwa 40 % der gesamten US-Bevölkerung, Nachrichten und Beiträge in sozialen Netzwerken gesehen haben, die von der inzwischen berüchtigten Internet Research Agency mit Sitz in St. Petersburg "gepflanzt" wurden (Tsompanidis, 2018).

Ein Beispiel für die Leichtigkeit, mit der heutzutage Fake News verbreitet werden, ist die Entdeckung neuer hausgemachter Rezepte, die angeblich das neue Coronavirus Covid-19 abtöten sollen. Wir hörten Dinge wie "Alkohol trinken tötet das Virus", "Chlordioxid trinken stärkt das Immunsystem". Diese Ansichten sind zumindest gefährlich. Aber ein Rezept, das schnell in den sozialen Medien zirkulierte, war die Behauptung, dass gekochter Knoblauch Covid-19 tötet: "Gute Nachrichten, das Coronavirus von Wuhan kann durch eine Schüssel mit frisch gekochtem Knoblauchwasser geheilt werden. Ein alter chinesischer Arzt hat seine Wirksamkeit bewiesen. Auch viele Patienten haben die Wirksamkeit bewiesen. Acht (8) gehackte Knoblauchzehen fügen Sie sieben (7) Tassen Wasser hinzu und bringen es zum Kochen. Essen und trinken Sie das gekochte Knoblauchwasser, über Nacht tritt Besserung und Heilung ein. Ich bin froh, dies zu teilen" (Spencer, 2020). Dieses Gerücht wurde so verbreitet, dass die Weltgesundheitsorganisation (WHO) es niederschlug und berichtete: "Knoblauch ist ein gesundes Lebensmittel, das einige antimikrobielle Eigenschaften haben kann. Es gibt jedoch keine Hinweise aus dem aktuellen Ausbruch, dass der Verzehr von Knoblauch Menschen vor dem neuen Coronavirus geschützt hat" (Spencer, 2020).

Weitere Informationen zu Propaganda im digitalen Zeitalter und Fake News finden Sie unter:

https://www.youtube.com/watch?v=5__dZBZuzZc&ab_channel=OsloFreedomForum

https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise

https://www.cyberwise.org/fake-news

https://www.cybercivics.com/

Die besten Möglichkeiten, Propaganda abzuwehren:

- Verantwortungsvolle, unabhängige Medien;
- Dekonstruktion von Mythen und strategische Kommunikation;
- Freie, gebildete Gesellschaft;
- Kontinuierliche Entwicklung der Fähigkeit, Informationen kritisch zu bewerten;
- Bildung und Stärkung der nationalen Erzählung und des historischen Gedächtnisses.

BEISPIEL: Die litauische Bayraktar-Geschichte

Russische Propagandalüge: Bayraktar, für den Litauer Geld gesammelt haben, ist bereits abgeschossen worden

, Hunderte von Litauern sammelten in dreieinhalb Tagen 4,7 Millionen Dollar, um den unbemannten Bayraktar in der Ukraine zu kaufen. Er wurde 3,5 Minuten nach seinem ersten Aufstieg abgeschossen".

Er wird als "anonymer Twitter-Kanal, der fiktive Nachrichten veröffentlicht", vorgestellt. Die Kommentatoren schienen diesem Detail keine Beachtung zu schenken und nahmen die Nachricht ernst.

Im Mai 2022 haben sich Hunderte von Litauern zusammengetan, um aus Solidarität mit einem anderen Land der ehemaligen Sowjetunion eine fortschrittliche Militärdrohne für die Ukraine in ihrem Krieg gegen Russland zu kaufen.

Die angestrebten 5 Millionen Euro wurden in nur dreieinhalb Tagen gesammelt - größtenteils in kleinen Beträgen zwischen 5 und 100 Euro - um den Kauf einer Militärdrohne vom Typ Byraktar TB2 zu finanzieren, wie der litauische Internetsender Laisves TV berichtet, der die Aktion ins Leben gerufen hat.

Die Drohne hat sich in den letzten Jahren bei Konflikten in Syrien und Libyen gegen russische Streitkräfte und deren Verbündete bewährt und wird vom litauischen Verteidigungsministerium angeschafft.

Zum weiteren Lesen hier https://lithuania.postsen.com/news/7172/Russian-propaganda-lie-Bayraktar-for-whom-Lithuanians-raised-money-has-already-been-shot-down.html

PRAKTISCHE AUFGABE. Wag the Dog

Ermutigen Sie die Schulungsteilnehmer, Wag the Dog zu sehen, eine schwarze Komödie aus dem Jahr 1997, eine amerikanische politische Satire, produziert und inszeniert von Barry Levinson und mit Dustin Hoffman und Robert De Niro in den Hauptrollen.

Ziel der Aktivität: Üben und Analysieren der persönlichen Beobachtung / kritischen Denkfähigkeit.

Fähigkeiten, die durch die Aktivität entwickelt werden: kritische Beobachtung.

Für wie viele Personen ist die Aktivität geeignet: Einzelarbeit mit anschließender Gruppendiskussion.

Zeitbedarf für die Aktivität: 97 Minuten für das Ansehen des Films und bis zu 15 Minuten für eine moderierte Diskussion.

Wie viele Lehrkräfte werden benötigt? Eine Person für die Moderation der Diskussion.

Andere Anforderungen für die Aktivität (Raum, Ausrüstung...): zu Hause/im Auditorium/ online.

Beschreibung der Aktivität: Bitten Sie die TeilnehmerInnen, während des Films zu beobachten, wie die Dinge vor sich gehen.

Fordern Sie die Gruppenmitglieder auf, über verschiedene Aspekte der politischen Phrase "mit dem Hund wedeln" nachzudenken.

Erstens kann er verwendet werden, um anzuzeigen, dass die Aufmerksamkeit absichtlich von etwas Wichtigerem auf etwas weniger Wichtiges gelenkt wird.

Zweitens, wenn man sagt, dass der Schwanz mit dem Hund wedelt, bedeutet das, dass ein kleiner oder unwichtiger Teil von etwas zu wichtig wird und das Ganze kontrolliert.

Referenzen

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Bjola, C. (2018). The Ethics of Countering Digital Propaganda. Ethics & International Affairs, 32(3), 305–315. https://doi.org/10.1017/s0892679418000436

CyberWise. (2019, August 10). What Is Fake News? YouTube. https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise

How to spot fake news. n.d. [Illustration]. https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps

Spencer, S. H. (2020, February 11). Fake Coronavirus Cures, Part 2: Garlic Isn't a "Cure." FactCheck.Org.

https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/

Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). Defining "Fake News." Digital Journalism, 6(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143

Tsompanidis, G. (2018) "Translated bibliography". Propaganda from the point of view of modern international law.

Wikipedia contributors. (2020b, December 20). Propaganda. Wikipedia. https://en.wikipedia.org/wiki/Propaganda

4.8. Betrügerische Werbung (fake Produkte, Nachträge)

Wann immer Geld im Spiel ist, gibt es immer eine Gelegenheit für einen Betrug. Aus technischer Sicht war Online-Werbebetrug ein relativ einfaches (und ja - lukratives) Geschäft für Betrüger und ein finanzielles Desaster für Werbetreibende, Publisher und Online-Werbeplattformen selbst. Das Online-Werbegeschäft wurde auf einer Reihe von offenen Internet-Standard-Technologien aufgebaut, die nie dazu gedacht waren, betrugs- / betrugs- / stahlsicher zu sein. Infolgedessen hatten Anzeigenbetrüger einen riesigen Vorsprung. Laut Juniper sah sich die Online-Werbebranche im Jahr 2019 mit einem atemberaubenden Verlust von 42 Milliarden US-Dollar aufgrund von Anzeigenbetrug konfrontiert, und leider gibt es keinen Grund zu der Annahme, dass die Zahl in diesem Jahr geringer ausfallen wird.

Zur Verdeutlichung: Digitaler Anzeigenbetrug ist eine absichtliche Aktivität, die verhindert, dass Werbung an die richtige Zielgruppe oder den richtigen Standort ausgeliefert wird. Die böswilligen Risiken, mit denen Vermarkter heute konfrontiert sind, werden immer ausgefeilter und damit größer, als bisher angenommen wurde.
Die digitale Werbeumgebung umfasst mittlerweile Tausende von Zwischenhändlern, die eine Fülle von dunklen Ecken bieten, in denen Betrüger ihre kriminellen Aktivitäten verbergen können. Betrüger wissen, wenn sie beobachtet werden und sind noch gefährlicher geworden, was es umso schwieriger macht, Anzeigenbetrug zu verhindern.
Infolgedessen sagen 96 Prozent der Verbraucher, dass sie wenig Vertrauen in digitale Werbung haben - was es für Vermarkter noch schwieriger macht, nachzuweisen, dass ihre Werbung legitim ist. Welche Schritte sollten Unternehmen also unternehmen, um zu verhindern, dass sie einen Großteil ihres Budgets durch Betrug verlieren und damit auch das Vertrauen der Verbraucher?
Selbst wenn nur ein kleiner Prozentsatz der Verbraucher auf die betrügerischen Anzeigen klickt und gefälschte Produkte oder Dienstleistungen kauft, ist es immer noch eine große geschäftliche und monetäre Absicht, die Techniken und Marketingbemühungen zu entwickeln

Kluge Verbraucher müssen teilweise die Verantwortung übernehmen, den Betrug in der Werbung einzudämmen, indem sie gefälschte Anzeigen melden und die weniger geschickten Menschen in ihrem Umfeld davon abhalten, sich mit solchen Anzeigen zu beschäftigen.

Wie erkennt man gefälschte Werbung?
Es ist relativ einfach, wenn Sie das Muster verstehen und kennen:

1. Die Qualität von Online-Anzeigen ist in der Regel schlecht und die Inhalte wiederholen sich;

2. Riesige und unrealistische Ansprüche und Versprechungen zu liefern eher unmöglich Ergebnisse entweder schnell reich zu werden oder wachsen wieder die verlorenen Haare;
3. Landing Pages werden unter seltsamen Domainnamen gehostet, unbekannte Marken, Fotos von entweder Prominenten oder nicht existierenden Fachleuten werden verwendet;
4. Die in den Landing Pages verwendete Schriftart ist auffällig bunt, sehr anreizend zum Handeln und es werden große Rabatte angeboten;
5. Die Landing Page und die Produktbeschreibungsseite können eine große Menge an gefälschten und meist sehr positiven Rezensionen enthalten.

4.9. PC/Online-Gaming, Casino, Sucht

Spielen ist ein angeborener menschlicher Trieb, der in der frühen Kindheit auftritt (Kuss & Griffiths, 2012, S. 5). Nach der Jahrtausendwende hat das Spielen im Internet aufgrund der enormen technologischen Entwicklung stark zugenommen. PC-Gaming und generell Online-Gaming gibt den Spielern die Möglichkeit, verschiedene Spielumgebungen gleichzeitig zu erleben, virtuelle Charaktere zu entwerfen und zu entwickeln, mit denen sie sich identifizieren können, und auch mit anderen Spielern auf der ganzen Welt zu jeder Zeit zu spielen (Kuss & Griffiths, 2012, S. 5). Darüber hinaus ermöglicht das Online-Gaming den Spielern, über Chats mit anderen zu kommunizieren und so neue Beziehungen aufzubauen (Kuss, 2013, S. 125). Ein weiterer Grund, warum Internet-Gaming für manche Menschen so attraktiv erscheint, ist, dass es die Möglichkeit bietet, den Problemen des realen Lebens zu entfliehen und auf diese Weise wird Online-Gaming zu einer Bewältigungsstrategie. (Kuss, 2013, S. 125).

Eine der bekanntesten Kategorien von Online-Spielen sind die Massively Multiplayer Online Role-Playing Games (MMORPGs), wie z. B. "World of Warcraft". Diese Art von Spielen erlaubt es den Spielern, sich Ziele zu setzen und diese zu erreichen, wie z. B. den Levelaufstieg, wodurch sie einen höheren virtuellen Status und Macht in der Spielumgebung erlangen. Spieler können auch durch die Bewunderung motiviert werden, die sie von der Gaming-Community erhalten können (Kuss, 2013, S. 125).

Auf der anderen Seite können die Aspekte des Sozialisierens und des Entkommens eine Sucht nach Online-Spielen begünstigen (Kuss, 2013, S. 125). Weitere negative Folgen sind die Vernachlässigung von Beziehungen im realen Leben, die Verweigerung von Schlaf, Arbeit und Studium, die Besessenheit vom Spielen, mangelnde Aufmerksamkeit mit der Folge von Aggression und Stresssteigerung als Konsequenz, Schwierigkeiten mit dem verbalen Gedächtnis und ein hohes Maß an Einsamkeit (Kuss, 2013, S. 125). In einigen Ländern, wie z. B. in südostasiatischen Ländern, waren die negativen Folgen des Online-Gamings so gravierend, dass die Regierungen Maßnahmen ergriffen, um diese negativen Auswirkungen zu reduzieren. In Japan zum Beispiel hat die Regierung die Schwere der Folgen erkannt, was zur Entwicklung von "Fastencamps" führte, in denen Personen, die süchtig nach Online-

Spielen sind, geholfen wird, indem sie von der Technologie völlig abgeschnitten werden (Kuss, 2013, S. 125).

Casino Sucht

Casino-Glücksspiele sind weltweit eine sehr beliebte Aktivität. In den letzten fünfzehn Jahren hat sich das Glücksspielumfeld durch die zunehmende Verfügbarkeit von Online-Glücksspielen erheblich verändert (Gainsbury, 2015, S. 190). Heutzutage ist ein internetfähiges Gerät und ein Klick auf einen Knopf alles, was man braucht, um Zugang zu einer Glücksspielumgebung zu haben. Darüber hinaus wird der Zugang auch dadurch ermöglicht, wie einfach Geld durch Kreditkarten, elektronische Banküberweisungen und E-Wallets ausgegeben werden kann.

Online-Casino und -Glücksspiel haben eine Kontroverse über die mögliche daraus resultierende Sucht ausgelöst (Gainsbury, 2015, S. 190). Die fünfte Ausgabe des Diagnostic and Statistical Manual of Mental Disorders (DSM-5) fügte eine neue Kategorie der Non - Substance Behavioural Addiction im Rahmen der Kategorie Substance Addiction hinzu. Um eine Glücksspielsucht zu diagnostizieren, muss die Person vier oder mehr der folgenden Punkte angeben (DSM-5):

1. Muss mit immer höheren Geldbeträgen spielen, um die gewünschte Erregung zu erreichen.
2. Ist unruhig oder reizbar, wenn er versucht, das Spielen zu reduzieren oder zu beenden.
3. Hat wiederholt erfolglose Versuche unternommen, das Glücksspiel zu kontrollieren, einzuschränken oder zu beenden.
4. Beschäftigt sich häufig mit dem Spielen (z. B. anhaltende Gedanken an vergangene Glücksspielerlebnisse, Planung des nächsten Spiels, Überlegungen, wie man an Geld zum Spielen kommen kann).
5. Spielt oft, wenn er sich verzweifelt fühlt (z. B. hilflos, schuldig, ängstlich, deprimiert).
6. Lügt, um das Ausmaß der Beteiligung am Glücksspiel zu verbergen.
7. Hat eine wichtige Beziehung, einen Arbeitsplatz oder eine Ausbildungs- und/oder Karrieremöglichkeit wegen des Glücksspiels gefährdet oder verloren.
8. Verlangt von anderen Geld, um die durch das Spielen verursachte verzweifelte finanzielle Lage zu erleichtern.

Risikofaktoren für Internet-Glücksspiel (Gainsbury, 2015, S. 190)

1. Jüngere Erwachsene und ältere Heranwachsende
2. Männlich
3. Alkohol- oder Drogenmissbrauch
4. Irrationale Kognitionen

5. Willenskraft, schnell und einfach Geld zu verdienen

Dennoch gibt es in den bisher durchgeführten Studien kein spezifisches Persönlichkeits- und Verhaltensmuster, um zwischen Internet- und Nicht-Internet-Problemspielern zu unterscheiden.

Im folgenden Link finden Sie die Geschichte eines Mannes namens Justyn Rees Larcombe, der £ 750.000 verspielte und dabei auch seine Familie verlor.

https://www.youtube.com/watch?v=7AN3VLLlkdI&ab_channel=TEDxTalks

Quellenangaben

Gainsbury, S. M. (2015). Online Gambling Addiction: The Relationship Between Internet Gambling and Disordered Gambling. Current Addiction Reports, 2(2), 185–193. https://doi.org/10.1007/s40429-015-0057-8

Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework. Journal of Substance Use, 10(4), 191–197.

Kuss, D. J. (2013). Internet gaming addiction: current perspectives. Psychology research and behavior management, 6, 125.

Kuss, D. J., & Griffiths, M. D. (2012). Online gaming addiction in children and adolescents: A review of empirical research. Journal of behavioral addictions, 1(1), 3-22.

5. Rolle der Regierung und Institutionen, bei denen Sie sich bewerben können

5.1. E-Privacy-Regelung in der EU

Die ePrivacy-Verordnung (ePR) ist ein Vorschlag zur Regelung verschiedener datenschutzrelevanter Themen, hauptsächlich in Bezug auf die elektronische Kommunikation innerhalb der Europäischen Union. Ihr vollständiger Name lautet "Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Datenschutzverordnung für elektronische Kommunikation)". Sie würde die Richtlinie über den Schutz der Privatsphäre und der elektronischen Kommunikation von 2002 (Datenschutzrichtlinie für elektronische Kommunikation) aufheben und wäre lex specialis zur Allgemeinen Datenschutzverordnung. Sie würde letztere in Bezug auf datenschutzrelevante Themen präzisieren und ergänzen. Schlüsselbereiche der vorgeschlagenen Verordnung sind die Vertraulichkeit der Kommunikation, Datenschutzkontrollen durch elektronische Einwilligung und Browser sowie Cookies.

Der Anwendungsbereich der ePrivacy-Verordnung ist noch in der Diskussion. Einigen Vorschlägen zufolge würde sie für jedes Unternehmen gelten, das Daten im Zusammenhang mit irgendeiner Form von Online-Kommunikationsdienst verarbeitet, Online-Tracking-Technologien einsetzt oder elektronisches Direktmarketing betreibt.

Die vorgeschlagenen Strafen für die Nichteinhaltung würden bis zu 20 Millionen Euro betragen oder, im Falle eines Unternehmens, bis zu 4 % des gesamten weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Die ePrivacy-Verordnung sollte ursprünglich am 25. Mai 2018 zusammen mit der GDPR in Kraft treten, ist aber noch nicht verabschiedet worden.

Video: The impact of the European ePrivacy regulation

https://www.youtube.com/watch?v=Q8YFLkvEcLE

Unterschied zwischen Verordnung und Richtlinie

1. Die (neue) Datenschutzverordnung für die elektronische Kommunikation wird die (derzeitige) Datenschutzrichtlinie für die elektronische Kommunikation aufheben.

2. Im Gegensatz zu einer EU-Richtlinie ist eine EU-Verordnung ein Rechtsakt der Europäischen Union, der sofort als Gesetz in allen Mitgliedsstaaten gleichzeitig in Kraft tritt.

3. Die aktuelle ePrivacy-Richtlinie ist ein Rechtsakt der Europäischen Union, der die Mitgliedsstaaten verpflichtet, ein bestimmtes Ergebnis zu erreichen, ohne die Mittel zur Erreichung dieses Ergebnisses vorzuschreiben. Sie ist daher in nationale Gesetze und Verordnungen umgesetzt worden.

4. Wenn die vorgeschlagene ePrivacy-Verordnung in Kraft treten würde, würden diese Gesetze überholt und (aus Gründen der Klarheit) wahrscheinlich aufgehoben werden. Die

Datenschutzverordnung für die elektronische Kommunikation wäre selbstausführend und würde nicht viele Durchführungsmaßnahmen erfordern.

5.2. GDPR und CCPA

Die General Data Protection Regulation (GDPR) ist ein Datenschutz- und Sicherheitsgesetz, das den Schutz von personenbezogenen Daten betrifft. Als personenbezogene Daten gelten alle Informationen, die direkt oder indirekt zur Identifizierung einer Person führen können (Goddard, 2017, S. 703). Zu den personenbezogenen Daten gehören Informationen über den Standort, die ethnische Zugehörigkeit, das Geschlecht, biometrische Daten, religiöse Überzeugungen oder Web-Cookies. Auch pseudonyme Daten können in den Kontext personenbezogener Daten fallen, wenn die Identität einer Person leicht zu ermitteln ist. Die GDPR wurde von der Europäischen Union (EU) ausgearbeitet und verabschiedet, verpflichtet aber Organisationen weltweit, solange sie mit Bürgern in der EU interagieren und Daten sammeln (Wolford, 2019). Auf diese Weise werden alle EU-Bürger vor dem Ort der Datenverarbeitung geschützt.

Kurzer historischer Rückblick

1950 Die Europäische Menschenrechtskonvention besagt, dass "jeder das Recht hat, sein Privat- und Familienleben zu schützen"	**1995** Europäische Datenschutzrichtlinie umgesetzt Mindeststandards für Datenschutz und -sicherheit	**2000** Viele Finanzorganisationen boten Online-Transaktionen an
2006 Facebook hatte seinen ersten Auftritt	**2011** Eine Google-Benutzerin hat das Unternehmen angeklagt, ihre E-Mails zu überprüfen	**2016** Europäisches Parlament setzt GDPR in Kraft

Strafmaßnahmen

Wenn gegen die GDPR verstoßen wird, dann sind die Geldstrafen wirklich hoch. Es gibt zwei Arten von Bußgeldern. Die erste ist eine Geldstrafe von etwa 20 Millionen Euro oder 4 % des weltweiten Umsatzes, und die zweite ist, dass Menschen, deren Daten nicht geschützt wurden, das Recht haben, eine Entschädigung zu verlangen (Wolford, 2019)).

Grundlagen des Datenschutzes (Wolford, 2019).

Die Verarbeitung personenbezogener Daten sollte nach sieben Grundprinzipien erfolgen:

1. Transparenz - Rechtmäßigkeit - Fairness

2. Zweckbindung: Daten sollten nur für die Zwecke verwendet werden, über die das Subjekt informiert wurde
3. Datenminimierung: Sie sollten nur die Daten sammeln, die für Ihren Zweck absolut notwendig sind.
4. Korrektheit: Daten müssen genau und aktuell gehalten werden.
5. Speicherbegrenzung: Sie können die Daten so lange speichern, wie es Ihr Zweck erfordert
6. Integrität und Vertraulichkeit: Die Verarbeitung von Daten muss so erfolgen, dass Schutz und Vertraulichkeit gewährleistet sind.
7. Rechenschaftspflicht: Die Person, die die Daten verarbeitet, ist für den Nachweis der Einhaltung aller oben genannten Grundsätze der GDPR verantwortlich.

Einverständnis

Es ist zwingend erforderlich, dass die betroffenen Personen ihre Einwilligung geben, um die Verarbeitung ihrer Daten zu erlauben. Doch was ist eine Einwilligung?
1. Die Einwilligung sollte frei gegeben werden, spezifisch und unmissverständlich sein.
2. Die Aufforderung zur Einwilligung sollte klar, unterscheidbar und in einfachen Worten formuliert sein.
3. Die betroffenen Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen, wenn sie es wünschen.
4. Wenn es sich um Kinder unter 13 Jahren handelt, ist die Zustimmung der Eltern obligatorisch.

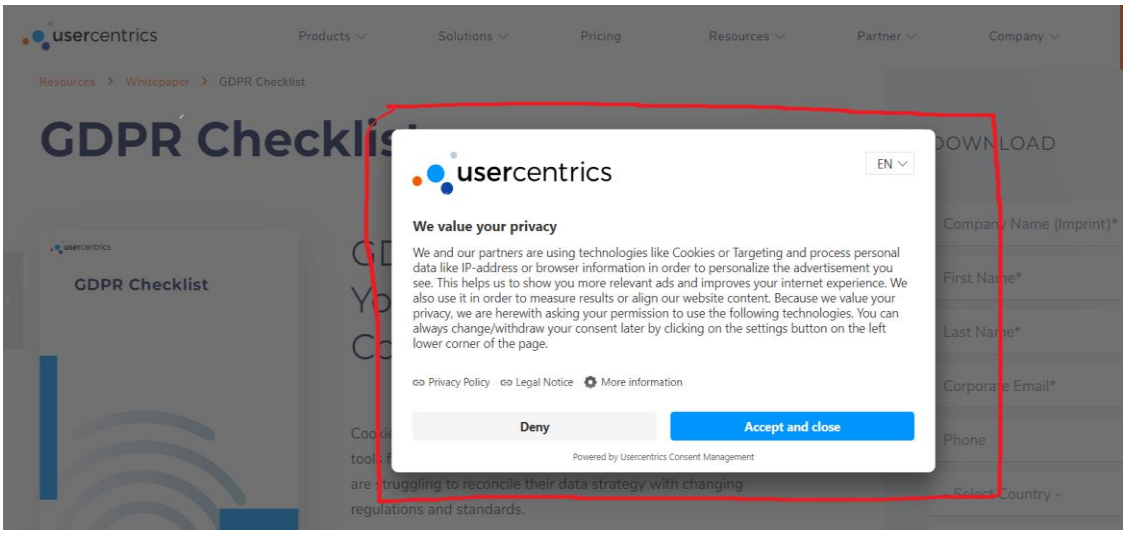
Ein dokumentarischer Nachweis der Einwilligung muss aufbewahrt werden

Datenschutzrechte

Auch der Einzelne, der in die Preisgabe von personenbezogenen Daten einwilligt, hat Persönlichkeitsrechte. Sie sind im Folgenden aufgeführt (Wolford, 2019):

1. Das Recht, informiert zu werden
2. Das Recht auf Zugang
3. Das Recht auf Korrektur
4. Das Recht auf Löschung
5. Das Recht auf Einschränkung der Verarbeitung
6. Das Recht auf Datenübertragbarkeit
7. Das Recht, Widerspruch einzulegen
8. Rechte in Bezug auf automatisierte Entscheidungsfindung und Profiling.

Abbilung 5.1. Ein Beispiel dafür, wie über das Internet nach dem Zugang zu persönlichen



Daten gefragt wird.

Der California Consumer Privacy Act (CCPA) stärkt die Datenschutzrechte und den Verbraucherschutz für die Einwohner Kaliforniens. Es ist ein Gesetz des Bundesstaates Kalifornien, das eigentlich im Juni 2018 verabschiedet wurde, aber erst am 1. Januar 2020 in Kraft trat (Cooman, 2020). Laut CCPA gelten als personenbezogene Daten alle Informationen, die zur Identifizierung einer Person führen können (z. B. Name, Adresse, E-Mail, Passnummer, Sozialversicherungsnummer usw.), kommerzielle Informationen (z. B. gekaufte Produkte), elektronische Netzwerkaktivitäten, Audio- oder visuelle Daten und Schlussfolgerungen, die aus einer der oben genannten Informationen gezogen werden, um ein Profil über einen Verbraucher zu erstellen, das seine Präferenzen widerspiegelt.

Zielsetzung der CCPA

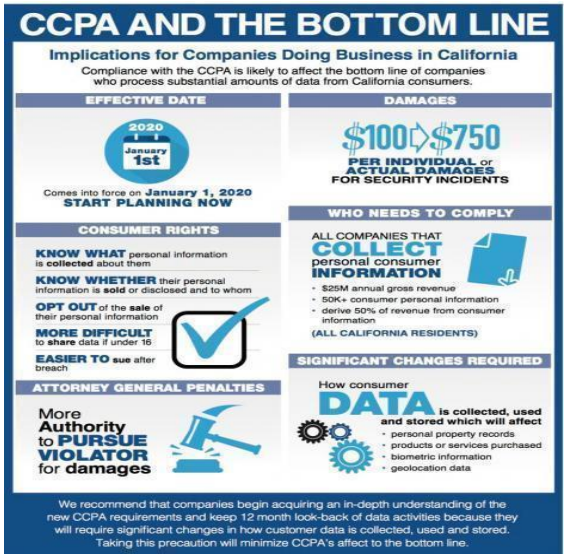
1. *Besitzen Sie Ihre persönlichen Daten*

2. *Kontrollieren Sie Ihre persönlichen Daten*

3. *Schützen Sie Ihre persönlichen Daten*

4. *Halten Sie große Unternehmen haftbar*

Abbildung 5.2. Die Grundelemente des CCPA



Hauptunterschiede zwischen GDPR und CCPA

Obwohl GDPR und CCPA gemeinsame Punkte haben, sind sie nicht austauschbar. Ihre Hauptunterschiede beziehen sich auf den territorialen Geltungsbereich und die Anwendung des Gesetzes, auf Sanktionen - im Falle eines Verstoßes - auf die Art und die Erfassungsbeschränkungen und auf die Tatsache, dass die DSGVO eine rechtmäßige Grundlage für jede Verarbeitung personenbezogener Daten verlangt (A., 2021). Die vorgenannten Punkte sind in der folgenden Abbildung dargestellt (A., 2021).

Abbildung 5.3. Die Unterschiede zwischen GDPR und CCPA

Quellenangaben

2019 is the Year of . . . CCPA? [Infographic]. (2019). The National Law Review. https://www.natlawreview.com/article/2019-year-ccpa-infographic

A. (2021, January 7). CCPA vs. GDPR – differences and similarities. Data Privacy Manager. https://dataprivacymanager.net/ccpa-vs-gdpr/

Cooman, G. (2020, January 28). What is CCPA and why should it matter to you? Proxyclick. https://www.proxyclick.com/blog/what-is-ccpa-and-why-does-it-matter-to-you#DDP

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 59(6), 703–705. https://doi.org/10.2501/ijmr-2017-050

Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? GDPR.Eu. https://gdpr.eu/what-is-gdpr/

5.3. Staatliche Datenschutzbehörden

Staatliche Datenschutzbehörden (DPAs) sind unabhängige öffentliche Behörden, die für die Überwachung der Umsetzung der Datenschutzgesetze zuständig sind und über Ermittlungs- und Korrekturbefugnisse verfügen (What Are Data Protection Authorities (DPAs)? 2018). DPAs bieten fachkundige Beratung in Datenschutzfragen und sind für die Bearbeitung von Anzeigen aufgrund von Verstößen gegen die Datenschutzgrundverordnung (GDPR) und die jeweiligen nationalen Gesetze zuständig. Im Rahmen der GDPR sollten alle EU-Mitgliedstaaten über eine Datenschutzbehörde verfügen, die als Vermittler zwischen den Beteiligten innerhalb des jeweiligen Mitgliedstaates fungiert (Clerck, 2019).

Liste der Datenschutzbehörden in verschiedenen EU-Mitgliedstaaten (Wikipedia-Mitarbeiter, 2020b)

Litauen: Staatliche Datenschutzaufsichtsbehörde

Österreich: Österreichische Datenschutzbehörde

Spanien: Spanische Datenschutzbehörde

Griechenland: Hellenische Datenschutzbehörde

Zypern: Amt des Beauftragten für den Schutz personenbezogener Daten

Italien: Italienische Datenschutzbehörde

Quellenangabe

What are Data Protection Authorities (DPAs)? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

Clerck, J. (2019, November 25). Supervisory authorities: consistency and Data Protection Authorities (DPAs) under GDPR. I-SCOOP.

https://www.i-scoop.eu/supervisory-authorities-consistency-and-data-protection-authorities-dpas/

Wikipedia contributors. (2020b, December 2). National data protection authority. Wikipedia. https://en.wikipedia.org/wiki/National_data_protection_authority

5.4. Staatliche Behörden zum Schutz der Verbraucherrechte

In jedem EU-Mitgliedstaat gibt es eine nationale Behörde, die für den Schutz der Verbraucherrechte zuständig ist, wenn sie mit Kredit- oder Finanzinstituten zu tun haben (National Competent Authorities for Consumer Protection - European, 2020). Die Verbraucherschutzpolitik sorgt dafür, dass der Binnenmarkt ordnungsgemäß und erfolgreich funktionieren kann (Fact Sheets on the European Union: European Parliament, n.d). Das Hauptziel der Verbraucherschutzbehörden ist es, die Rechte der Verbraucher gegenüber Gewerbetreibenden zu schützen und einen verbesserten Schutz für gefährdete Verbraucher zu bieten (Fact Sheets on the European Union: Europäisches Parlament, n.d.).

Verbraucherschutzvorschriften zielen darauf ab, die Marktergebnisse für die gesamte Wirtschaft zu verbessern, den Markt fairer zu machen und so zu umweltfreundlicheren und sozialen Marktergebnissen zu führen. Der Verbraucherschutz ist zu einem Ziel von entscheidender Bedeutung für die EU geworden (Fact Sheets on the European Union: European Parliament, n.d).

Ein Verbraucher hat das Recht, sich bei einer Kredit- oder Finanzorganisation zu beschweren, wenn er mit den erhaltenen Produkten oder Dienstleistungen nicht zufrieden ist (How to Complain, 2020). Im Folgenden finden Sie einige Vorschläge zur Einreichung von Beschwerden:

1. Wenden Sie sich an die Kredit- oder Finanzorganisation: Wenn Sie mit den Leistungen eines bestimmten Finanzinstituts nicht zufrieden sind, müssen Sie sich an den Kundendienst dieses Instituts wenden. Die Kontaktdaten finden Sie auf deren Website. Es ist sehr hilfreich, wenn Sie einige relevante Dokumente haben, um Ihren Anspruch zu unterstützen.

2. Reichen Sie eine offizielle Beschwerde ein: Wenn die Kundendienstabteilung Ihnen nicht in der von Ihnen gewünschten Weise geholfen hat, können Sie eine offizielle Beschwerde einreichen. Jedes Finanzinstitut hat ein spezielles Verfahren für die Bearbeitung von Beschwerden. Die Schritte für dieses Verfahren sind normalerweise auf der Website angegeben. Auch hier sind unterstützende Dokumente hilfreich.

3. Wenden Sie sich an die zuständige nationale Behörde: Falls Sie weder mit dem Verbraucherservice des Finanzinstituts noch mit dessen Antwort auf Ihre Beschwerde zufrieden sind, können Sie sich an die zuständige nationale Behörde Ihres Landes wenden.

Tipps, die auf den Verbraucherschutz abzielen (Persönliche Finanzen auf EU-Ebene, 2019).

Bevor Sie einen Dienst wählen → Erkennen Sie Ihren finanziellen Bedarf

→ Erfahren Sie mehr über den ausgewählten Dienst

Prüfen Sie, ob der Dienst Ihren Anforderungen entspricht

Abbildung 5.4. Bei Abschluss eines Vertrages für eine bestimmte Leistung (Quelle: Persönliche Finanzen auf EU-Ebene, 2019)

Quellenangaben

Consumer policy: Principles and instruments: Fact Sheets on the European Union: European Parliament. (n.d.). Retrieved from https://www.europarl.europa.eu/factsheets/en/sheet/46/consumer-policy-principles-and-instruments

How to complain. (2020, January 14). European Banking Authority. https://www.eba.europa.eu/consumer-corner/how-to-complain

National competent authorities for consumer protection - European. (2020, August 25). European Banking Authority. https://www.eba.europa.eu/consumer-corner/national-competent-authorities-for-consumer-protection

Personal finance at the EU level. (2019, December 10). European Banking Authority. https://www.eba.europa.eu/consumer-corner/personal-finance-at-the-eu-level

6. Werkzeuge zur Selbsteinschätzung

6.1. Umgehen Sie die Mid-Career-"Krise" - bleiben Sie auf dem neuesten Stand der Technik

Die Technologie wird jeden Tag mehr in jeden Aspekt unseres Lebens integriert. Viele Menschen sind besorgt darüber, dass sich die Welt so schnell verändert und sie den Anschluss verlieren könnten. Dies ist ein sehr berechtigter Gedanke, der derzeit häufiger vorkommt, als man annehmen würde. Unabhängig davon, in welchem Bereich Sie tätig sind, ist es besonders wichtig, mit der Technologie auf dem Laufenden zu bleiben, um Ihr persönliches und berufliches Leben zu beeinflussen. Die Technologie hat sich in den letzten Jahrzehnten rasant weiterentwickelt und Dinge, die früher für unmöglich gehalten wurden, werden in einem sehr schnellen Tempo möglich gemacht. Über die Fortschritte in der Technologie Bescheid zu wissen, ist an sich schon ein faszinierendes Vergnügen für den Geist. Es ist auch wichtig, sich mit der neuen Technologie vertraut zu machen, denn die alte Technologie, mit der Sie zu arbeiten gewohnt sind, wird schnell veraltet sein. Sie werden in jedem Bereich im Vorteil sein, wenn Ihr Wissen in der Technologie auf dem neuesten Stand ist. Im folgenden Abschnitt wird dargestellt, wie wichtig es ist, mit den neuen Trends in der Technologieentwicklung, die für das tägliche Leben benötigt werden, Schritt zu halten.

Technologie hält uns verbunden (besonders mit unserer Familie und Freunden)

Wenn Familien weiter wachsen, ziehen die Mitglieder oft von zu Hause weg, um zur Schule zu gehen, zu arbeiten oder ihre eigenen Familien zu gründen. Glücklicherweise war die Kommunikation mit Hilfe der Technologie noch nie so einfach. Ob über Textnachrichten, FaceTime oder Skype oder eine der verschiedenen Social-Media-Seiten, es ist einfach, mit Familie und Freunden aus der Ferne in Verbindung zu bleiben. Moderne Tablets, Computer und Mobiltelefone haben fast alle die Fähigkeit, eine der oben genannten Kommunikationsformen zu nutzen, um Familie und Freunde in Verbindung zu halten, egal wo auf der Welt sie sich befinden.

Technologie hilft Ihnen, informiert zu bleiben

Der schnellste und günstigste Weg, sich über die Geschehnisse im Land oder auf der ganzen Welt zu informieren, ist das "Klicken" und "Scrollen" auf den Nachrichtenportalen im Internet. Sie können auch den Nachrichtenanbieter Ihrer Wahl abonnieren oder die Handy-Applikation herunterladen (in den meisten Fällen kostenlos) und sich so über aktuelle Ereignisse informieren lassen.

Technologie steigert Ihre Produktivität

Es gibt viele Produktivitäts-Apps, die dabei helfen können, produktiv und organisiert zu bleiben. Zum Beispiel ist "Evernote" eine Produktivitäts-App, die wie ein erstaunlicher Aktenschrank funktioniert. Sie hilft, geistiges Durcheinander in Schach zu halten, da sie alles für Sie organisiert.

Nutzung von Jobportalen als effizienteste Technik zur Stellensuche

Wir sind weit davon entfernt, in den Karriereredaktionen jeder Zeitung nach der nächsten Karrieremöglichkeit zu stöbern und unsere Joblosigkeit in geschlossenen Kreisen von Familie und Freunden zu verbreiten, nur in der Hoffnung, früher eine Empfehlung zu bekommen. Doch die neueste digitale Sensation ist unsere rettende Gnade und Zeit, hier werden Karrieren auf Klicks gemacht. Die Jobportale sind die neueste Anlaufstelle für alle Arbeitssuchenden, die gerade erst anfangen, sich beruflich verändern oder einfach nur außerhalb ihrer alten Mauern arbeiten wollen oder generell einen Job finden wollen.

E-Services, die Ihnen das Leben erleichtern (z. B. Online-Banking).

Es besteht kein Zweifel, dass die Digitalisierung zu einer Revolution in Finanzangelegenheiten geführt hat. Onlinebanking wird entweder über einen Laptop, ein Tablet oder eine Telefon-App erledigt und ist heute die Norm. Banknutzer können nun aus der Ferne ihre Zahlungsein- und -ausgänge überprüfen sowie Geldüberweisungen und Rechnungszahlungen veranlassen. Außerhalb der Bankgeschäfte können auch andere finanzielle Angelegenheiten, wie der Kauf und Verkauf von Währungen und Aktien, online abgewickelt werden. Auch bei der Überweisung von Geld zwischen Konten im In- und Ausland hat sich in den letzten Jahren viel getan.

6.2. Interaktive Spiele und Apps

DUOLINGO hilft Ihnen, eine Fremdsprache zu lernen.

STUDYBLUE ist ein mobiler Lernbegleiter, der Ihnen hilft, "Ihren Kurs zu erobern", indem er Flashcards, Notizen, Studienführer und mehr verwendet.

Freckle Rich mit inhaltsbezogenen Bewertungen, druckbaren Arbeitsblättern und Fortschrittsanalysen.

TYPINGCLUB Gamifizierte, datengesteuerte Aktivitäten helfen bei der Beherrschung der Tastaturfertigkeiten.

SEESAW: THE LEARNING JOURNAL Ein leistungsstarkes multimediales Lern- und Kommunikationswerkzeug.

TED Verbreitung von fesselnden oder inspirierenden Gedanken, normalerweise in Videos von 18 Minuten oder weniger

YOUTUBE Geben Sie die Wörter "how to" in die Suchleiste der App ein und Sie werden fündig

QUIZLET Flexible Lernhilfe unterstützt das Lernen zu Hause, in der Schule und unterwegs

Kryptische Kreuzworträtsel lernen Kryptische Kreuzworträtsel sind gar nicht so kryptisch, wenn man erst einmal anfängt, einige der Methoden zu lernen, um sie zu lösen. Diese App macht einen wirklich guten Job, indem sie erklärt, wie man die Rätsel angeht und Sie mit Übungen testet.

ELEVATE: GEHIRNTRAINING Selbstisolation muss nicht gleichbedeutend mit Stagnation sein. Gehirntrainings-Apps wie Elevate sind darauf ausgelegt, Ihren Verstand mit kurzen täglichen Übungen, die Ihr Gedächtnis, Ihre mathematischen und anderen Fähigkeiten testen, scharf zu halten.

KHAN ACADEMY ein globales Klassenzimmer. Kurse zu Mathematik, Informatik, Naturwissenschaften und Wirtschaft bis hin zu Kunst und Geisteswissenschaften, mit einer Mischung aus Videos, Artikeln und Quiz, um Ihr Lernen zu testen.

SKILLSHARE Zeichnen, Fotografie, Grafikdesign und andere kreative Disziplinen

COURSERA bietet Programmieren, Kunst und Design, Naturwissenschaften und Wirtschaft und andere Fächer in 3.500 Online-Lernkursen, komplett mit Videovorträgen und Dozenten, mit denen man chatten kann.

Google Arts and Culture virtuelle Rundgänge durch mehr als 2.000 "Kultureinrichtungen" auf der ganzen Welt, mit Fotos, Videos und virtueller Realität

Erfahren Sie mehr über Spiele und Apps auf:

https://bit.ly/2KOFFiK
https://bit.ly/2NA3Br9
https://bit.ly/39b33