

Handout zur Veranstaltungsreihe „Digitallotsen von und für Bürger“

Was sind Digitallotsen?

Unter „Digitallotsen“ werden interessierte und engagierte Personen verstanden, welche bereit sind, ihr durch Veranstaltungen beim Regionalmanagement gewonnenes Wissen an interessierte Bekannte, Freunde, Firma etc. in ihrem Umfeld weiterzugeben. Durch die gezielte Ausbildung in verschiedenen Themenbereichen der Digitalisierung von Digitallotsen, die ihr gewonnenes Wissen mit ihren Mitmenschen teilen, gewinnt der ganze Landkreis an Wissen. Diese Mitmenschen sollen die Wissensweitergabe durch eine kurze Umfrage bestätigen.

Wer kann Digitallotse werden?

Digitallotsen können alle Personen im Landkreis Dillingen a.d. Donau werden, die sich für die Thematik interessieren und ihr Wissen gerne weitergeben möchten, sodass auch andere Personen davon profitieren können.

An wen kann man das Wissen als Digitallotse weitergeben?

Die Digitallotsen können ihr gewonnenes Wissen an ihre Mitmenschen weitergeben. Zum Beispiel an:

- Familie, Bekannte, Freunde
- Arbeitskollegen
- Vereine
- andere Organisationen

Wer ist Ihr Ansprechpartner im Projekt Digitallotsen?

Erik Laznik und Carolin Bucher

Landratsamt Dillingen a.d. Donau
Regionalmanagement
Große Allee 24
89407 Dillingen a.d. Donau
Tel: 09071 / 514778
E-Mail: Regionalmanagement@landratsamt.dillingen.de
Internet: <http://www.landkreis-dillingen.de>



Link und QR-Code zur Umfrage bzgl. Wissensweitergabe:

<https://docs.google.com/forms/d/e/1FAIpQLSfHT4c8C82QBCcpWmLqOrvd3fT3LpFfO0HJd8i6buFTH2oDqQ/viewform?vc=0&c=0&w=1&flr=0>

Das vorliegende Handout dient als inhaltliche Orientierung der insgesamt 8-teiligen Veranstaltungsreihe „Digitallotsen von und für Bürger“, die zwischen Oktober 2023 und Mai 2025 durch das Regionalmanagement des Landkreises Dillingen a.d.Donau organisiert und durchgeführt wurde. Das Regionalmanagement dankt allen beteiligten Referenten für Ihre lehrreichen Vorträge.

Die kostenfreie Veranstaltungsreihe richtete sich an alle interessierten Bürgerinnen und Bürger, Unternehmerinnen und Unternehmer, insbesondere aus dem Landkreis Dillingen a.d.Donau. Bei Fragen, Anregungen und Wünschen können Sie sich gerne jederzeit an das Regionalmanagement des Landkreises Dillingen a.d.Donau unter regionalmanagement@landratsamt.dillingen.de wenden. Bei inhaltlichen Fragen stehen Ihnen ebenfalls die Referentinnen und Referenten der einzelnen Veranstaltungen zur Verfügung.

Das Regionalmanagement Dillingen a.d.Donau existiert seit Februar 2018 und wird gefördert durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie.



Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie

Inhalt

1. Veranstaltung: „ Trickbetrug und wie Sie sich und andere davor schützen können “ (04.10.2023) mit Sandra Gartner, Kriminalpolizeiinspektion Dillingen	4
2. Veranstaltung: „ Internetgefahren für Erwachsene und Erziehungsberechtigte – Tipps und Tricks “ (20.11.2023) mit Sandra Gartner, Kriminalpolizeiinspektion Dillingen	6
3. Veranstaltung: „ 3D-Druck “ (15.02.2024, 21.05.2024) mit BayernLab Dillingen	10
4. Veranstaltung: „ Bayernatlas “ (14.03.2024, 24.07.2024) mit Franziska Berger, Vermessungsamt Dillingen	17
5. Veranstaltung: „ Künstliche Intelligenz “ (07.05.2024, 17.06.2024 und 20.06.2024) mit Kilian Modl, BayernLab Dillingen	22
6. Veranstaltung: „ Digitaler Kompass: Internetsicherheit und Medienkompetenz für (Groß)-Eltern und Pädagogen “ (28.01.2025) mit Kilian Modl, BayernLab Dillingen	26
7. Veranstaltung: „ Mikrotransaktionen – In-App-Käufe & andere Verkaufsstrategien der Spieleindustrie “ (04.02.2025) mit Kilian Modl, BayernLab Dillingen	30
8. Veranstaltung: „ Kryptowährung “ (09.04.2025, 14.05.2025 und 26.05.2025) mit Kilian Modl, BayernLab Dillingen	32

1.Veranstaltung: „Trickbetrug und wie Sie sich und andere davor schützen können“ (04.10.2023) mit Sandra Gartner, Kriminalpolizeiinspektion Dillingen

„Ein gesundes Misstrauen schadet niemanden und hat nichts mit Unhöflichkeit zu tun.“ Dieses Zitat gilt für alle Arten von Trickbetrug. Die meisten Opfer sind statistisch gesehen älter als 70 Jahre alt, leben alleine und sind gebrechlich.

1. Gefahren an der Haustür

Fremde an der Haustüre bergen oftmals Gefahren, da Kriminelle sich unter einem Vorwand Eintritt verschaffen wollen. Die Kriminelle geben sich beispielsweise als Polizisten oder andere Amtspersonen aus, um an Geld oder Wertgegenstände zu gelangen. Dabei wird meist ein gefälschter Dienstausweis gezeigt, um hereingelassen zu werden. Ebenfalls gibt es Kriminelle, die eine Notlage oder eine persönliche Beziehung (angeblich Bekannte sollen besucht werden) vortäuschen, um so in Ihre Wohnung zu gelangen. Manche Täter suchen gezielt ältere Menschen auf, um sie an der Haustüre dazu zu überreden, einen Vertrag zu unterschreiben. In diesem Fall ist es wichtig zu wissen, dass Sie Verträge, die Sie bei solchen Haustürgeschäften abschließen, innerhalb von 14 Tagen ohne Angaben von Gründen schriftlich widerrufen können.

Tipps:

- Lassen Sie keine Unbekannten in Ihre Wohnung. Sie sind grundsätzlich nicht verpflichtet, jemanden unangemeldet einzulassen.
- Benutzen Sie die Türsprechanlage falls möglich.
- Falls Zweifel bestehen, rufen Sie bei der Behörde an, von der die angebliche Amtsperson kommt. Suchen Sie dabei die Telefonnummer der Behörde selbst heraus.
- Lassen Sie nur Handwerker rein, die Sie selbst bestellt haben oder von der Hausverwaltung angekündigt wurden.
- Zeigen oder erklären Sie niemanden, wo Sie ihr Geld oder Wertgegenstände aufbewahren.
- Kaufen oder unterschreiben Sie niemals etwas an der Haustür.
- Lassen Sie die Besucher währenddessen vor der verschlossenen Tür warten.
- Informieren Sie sofort die Polizei, wenn Ihnen eine Kontaktaufnahme verdächtig vorkommt: Notrufnummer 110.

2. Gefahren am Telefon

Viele Kriminelle melden sich per Telefon und nutzen dabei die Gutgläubigkeit ihrer Opfer aus, um an Geld zu kommen. Die Betrüger rufen meist bei älteren und alleinlebenden Personen an und geben sich als Verwandte, Enkelkinder oder auch Bekannte aus und bitten kurzfristig um Bargeld. Als Grund wird meist ein finanzieller Engpass oder eine Notlage vorgetäuscht (beispielweise ein Autokauf oder ein Unfall). Durch die Dringlichkeit wird das Opfer enorm unter Druck gesetzt und zur Verschwiegenheit verpflichtet. Relativ neu ist beim Enkeltrick die Variante des Messenger-Betrugs. Hier geben sich Kriminelle als Kinder aus, die ihre Handynummer gewechselt haben. Ziel ist auch hier mit erfundenen Geschichten Geld zu erbeuten. Falls die Opfer das Geld nicht parat haben, werden sie gebeten, unverzüglich zur Bank zu gehen und dort den Betrag abzuheben.

Immer wieder sind Kriminelle unterwegs, welche sich als Polizisten ausgeben, um in den Besitz von Geld und Wertgegenständen zu gelangen. Beispielsweise wird behauptet, dass diese Dinge zu Hause nicht mehr sicher sein oder auf Spuren untersucht werden müssen. Mittlerweile können die Täter eine spezielle Technik anwenden, sodass auf der Telefonanzeige der Angerufenen die Polizei Notrufnummer 110 oder eine örtliche Telefonnummer angezeigt wird.

Betrugsversuche durch Gewinnversprechen gibt es in zahlreichen Varianten. Bei dieser Masche meldet sich ein vermeintlicher Notar oder Rechtsanwalt per Telefon. Es wird behauptet, dass sie einen hohen Geldbetrag oder Ähnliches gewonnen haben. Vor der Übergabe muss aber eine „Verwaltungsgebühr“ bezahlt werden, welche die Opfer per Internet-Bezahlsystem oder am Postschalter mittels Bargeldtransfer ins Ausland überweisen sollen.

Tipps:

- Lassen Sie sich nicht unter Druck setzen. Legen Sie den Hörer auf, wenn Ihnen etwas merkwürdig vorkommt.
- Sprechen Sie am Telefon nicht über finanzielle oder persönliche Verhältnisse.
- Geben Sie niemals Wertgegenstände oder Geld an Unbekannte Personen.

- Machen Sie sich bewusst: Wenn Sie nicht an einer Lotterie teilgenommen haben, können Sie auch nichts gewonnen haben!
- Geben Sie niemals Geld aus, um vermeintliche Gewinne einzufordern.
- Machen sie keinerlei Zusagen am Telefon und weisen Sie unberechtigte Geldforderungen zurück.
- Fragen Sie die Anrufer nach Namen, Adresse und Telefonnummer der Verantwortlichen, um welche Art von Gewinnspiel es sich handelt.
- Kontrollieren Sie mindestens einmal im Monat Ihre Kontoauszüge und Ihre Telefonrechnung.
- Wenn Sie unsicher sind: Rufen Sie die Polizei unter der Notrufnummer 110 oder Ihre örtliche Polizeidienststelle an. Sobald Unsicherheit bei solchen Angelegenheiten besteht, kann man bei jeder Polizeidienststelle oder auch bei der Verbraucherzentrale anrufen. Diese sind immer auf dem aktuellen Stand bezüglich Trickbetrug und hätten für den Notfall auch Muster für Widerrufsschreiben für bestimmte Fälle.

3. Rat und Hilfe

Oft kümmert sich niemand darum, was auf dem Nachbargrundstück oder an der Wohnungstür passiert. Darauf vertrauen viele Kriminelle. Reden Sie mit Ihren Nachbarn, denn wer sich kennt, achtet auch mehr aufeinander und spürt, wenn etwas nicht stimmt. Mit gegenseitiger Aufmerksamkeit und Hilfe gewinnen Sie und Ihre Nachbarschaft deutlich an Sicherheit. Die Polizei steht Ihnen auch immer hilfsbereit zur Seite. Sollten Sie doch einmal Opfer einer Straftat geworden sein, bleiben Sie bitte nicht (vielleicht aus unbegründeter Scham) tatenlos, sondern erstatten Sie so schnell wie möglich Anzeige bei der Polizei. Wenn Sie eine Straftat beobachten, dann schauen Sie nicht weg, sondern reagieren Sie. Wichtig ist, den Betroffenen je nach Möglichkeit zu helfen, zum Beispiel einen Notarzt zu rufen oder Erste Hilfe zu leisten.

Weitere Informationen finden Sie auf der Internetseite www.polizei-beratung.de. Neben Informationen zu den unterschiedlichsten Themen finden Sie auch eine ganze Reihe von Broschüren und Informationsblättern.

Wenn Sie durch eine vorsätzlich begangene Gewalttat gesundheitliche Schäden erleiden, können Ihnen nach dem Opferentschädigungsgesetz (OEG) Versorgungsansprüche zustehen. Auf der Homepage der Opferhilfeeinrichtung WEISSE RING können Sie sich bundesweit und kostenlos unter www.weisser-ring.de informieren.

2. Veranstaltung: „Internetgefahren für Erwachsene und Erziehungsberechtigte – Tipps und Tricks“ (20.11.2023) mit Sandra Gartner, Kriminalpolizeiinspektion Dillingen

Medienerziehung bedarf eines frühzeitigen Beginns. Dabei spielen Kontrolle, Verantwortung und Vertrauen eine zentrale Rolle. Die gemeinsame Nutzung neuer Medien bietet eine wertvolle Gelegenheit, Wissen zu vermitteln und zu erklären. Es ist ratsam, dass Erziehungsberechtigte bestimmte Apps oder Anwendungen selbst ausprobieren und testen, um eine fundierte eigene Meinung zu entwickeln.

Das Internet, als schier unerschöpfliche Quelle ohne Grenzen, vergisst nichts. In den letzten fünf Jahren hat sich der Internetkonsum vervielfacht. Es ist daher von großer Bedeutung, Kinder unter 3 Jahren keinerlei Bildschirmkonsum auszusetzen.

Die Auseinandersetzung mit Medien sollte bereits in jungen Jahren beginnen, insbesondere angesichts der Tatsache, dass viele Kinder bereits in der Grundschule im Besitz eines eigenen Smartphones sind. Bei der Wahl von Kommunikationsplattformen bieten Threema und Signal sichere Alternativen zu WhatsApp an.

Wichtige Maßnahmen zur Sicherung des Medienkonsums umfassen die individuelle Konfiguration des Handys, die Einrichtung einer Premium SMS-Sperre, die Aktivierung einer Drittanbietersperre beim Telefonanbieter sowie die Deaktivierung von In-App-Käufen.

1. Verbreitung verbotener Inhalte

Gewaltverherrlichende oder pornografische Inhalte sind aufgrund ihrer jugendgefährdeten Wirkung meist verboten. Auch die Herstellung und Verbreitung von solchen Inhalten ist strafbar. Zuständig für die Verfolgung solcher Verstöße sind – neben den Polizeibehörden – zwei im staatlichen Auftrag handelnde Institutionen: die Internet-Beschwerdestelle sowie www.jugendschutz.net. Während die Meldestellen mit Abmahnungen und Bußgeldern beim Seitenbetreiber die Inhalte löschen lassen können, verfolgt die Polizei die Verfasser verbotener Inhalte.

Kinderpornografische Inhalte:

Es sind über 750.000 Pädophile täglich im Internet unterwegs. Unter Kinderpornografie (Missbrauchsdarstellungen) werden Bilder und Videos verstanden, die den Missbrauch von Kindern unter 14 Jahren zeigen. Gemeint sind damit auch Aufnahmen, die Kinder in unnatürlicher geschlechtsbetonter Körperhaltung wiedergeben oder ihre unbedeckten Geschlechtsteile in sexuell aufreizender Art zur Schau stellen. Strafbar ist der Besitz, das sich Verschaffen, das Herstellen oder Verbreiten von Bildern, Filmen, aber auch von Zeichnungen oder Schriften.

Tipps:

- Sichern Sie Beweise für strafbare Inhalte im Internet oder in Messengerdiensten (WhatsApp) und wenden Sie sich damit an die Polizei oder die Meldestellen unter www.jugendschutz.net oder www.internet-beschwerdestelle.de. Wichtig: Notieren Sie sich den Fundort der verbotenen Inhalte (z. B. Facebook, Youtube) sowie die dazugehörige URL.
- Im Falle von Kinderpornografie im Netz dürfen Sie nicht selbst nach einschlägigen Seiten suchen und diese sichern, dadurch können Sie sich strafbar machen. Wenn Sie zufällig einen solchen Inhalt entdecken, melden Sie diesen sofort der Polizei oder weisen die Internet-Beschwerdestelle daraufhin.
- Kampagne gegen Missbrauchsdarstellungen: Die polizeiliche Kampagne unter www.soundswrong.de klärt Erwachsene und Kinder über die strafbare Verbreitung von Missbrauchsdarstellungen auf.

2. Verletzung von Persönlichkeits- und Urheberrechten

Schnell ist ein Bild aus dem Netz gezogen, das Lieblingslied heruntergeladen oder das selbstgedrehte Video ins eigene Profil bei Facebook, Instagram und Co. eingestellt. Diese Freiheit hat jedoch Grenzen, da nicht alle Daten von jedem in jeder Form genutzt werden dürfen. Problematisch ist neben illegalen Downloads von Bildern, Videos, Software oder Musik vor allem auch der Umgang mit selbst erstellten Inhalten. Vielen ist kaum bewusst, dass Sie beispielsweise Aufnahmen von Dritten nicht einfach weiterverwenden dürfen. Wenn auf den Aufnahmen Bekannte, Familienmitglieder oder Kolleginnen und Kollegen zu sehen sind, dürfen sie nicht ohne deren Erlaubnis im Internet verbreitet werden. Gerade

wenn Dritte in peinlichen oder erniedrigenden Situationen gezeigt werden, wird aus dem scheinbar harmlosen Spaß schnell strafbares Verhalten. Auch wer Aufnahmen von Verkehrsunfällen mit Verletzten oder Toten erstellt, macht sich strafbar.

Tipps:

- Heimliche Film- und Bildaufnahmen von Dritten sind nicht erlaubt – deren Veröffentlichung im Internet ist strafbar.
- Nutzen Sie Inhalte von Dritten ausschließlich in der zugelassenen Form. Beachten Sie dabei, dass Veränderungen der Inhalte ausgeschlossen sind.
- Setzen Sie Verlinkungen zu den Webseiten anderer, statt Inhalte zu kopieren. Holen Sie dazu die Zustimmung des Seitenbetreibers ein und geben Sie eine Quelle an.
- Nutzen Sie ausschließlich legale Musik- und Videoportale, um Filme im Internet anzuschauen oder um Musik zu hören. Illegale Downloads können Schadsoftware enthalten oder zivilrechtliche Forderungen der Rechteinhaber nach sich ziehen.
- Das Online-Streaming von illegalen Inhalten kann strafbar sein.
- Wenn Ihre persönlichen Daten, Bilder oder Texte unerlaubt verbreitet werden: Sichern Sie alle Seiten durch Screenshots und machen Sie denjenigen auf Verletzung Ihrer Rechte aufmerksam. Setzen Sie ihm Fristen, innerhalb derer die Inhalte entfernt werden sollen. Beantragen Sie dann eine Löschung der Daten beim Provider der Website. Je nach Seitenbetreiber sind die Voraussetzungen dafür unterschiedlich. Wenden Sie sich bei Verdacht auf eine Straftat an die Polizei.

3. Straftaten in sozialen Netzwerken

Das Risiko, in einem sozialen Netzwerk Opfer einer Straftat zu werden, steigt mit jeder persönlichen Information im eigenen Profil. Betrug, Cybermobbing oder Phishing sind Straftaten, die meist erst möglich werden, weil Nutzerinnen und Nutzer leichtfertig mit ihren Daten umgehen und allgemeine Sicherheitshinweise ignorieren. Während ein materieller Schaden beispielsweise durch einen Betrug meist noch zu verkraften ist, sind die Folgen von Beleidigungen, übler Nachrede oder Verleumdungen gravierender. Solche Straftaten tauchen oft in Verbindung mit (Cyber) Mobbing oder Cyberstalking (Nachstellung mittels moderner Kommunikationsmittel) auf. Neben dem unbedachten Umgang mit den eigenen Daten sind mangelnde Schutzeinstellungen der jeweiligen Profile ein Anreiz für Täter. Kriminelle nutzen die sozialen Netzwerke für Betrug, beispielsweise indem sie Profile übernehmen, um von Freunden der realen Person Geld zu erpressen oder um Daten auszuspähen.

Romance Scamming:

Besonders perfide gehen Betrüger beim Romance Scamming vor. Sie täuschen ihren Opfern über Wochen und Monate eine Online-Beziehung vor und bitten diese um Geld und andere Gefälligkeiten. Dabei üben sie nicht selten immensen Druck aus, damit Betroffene weiterzahlen. Auf diese Weise haben viele Geschädigte bereits ihre gesamten Ersparnisse an die Kriminellen verloren.

So sichern Sie Online-Accounts:

- Bevor Sie ein Profil bei einem Dienst einrichten: Achten Sie auf die AGB und den Datenschutz.
- Nutzen Sie wenn möglich die 2-Faktor-Authentisierung für die Account-Anmeldung, auch bei Messenger-Diensten oder Netzwerk-Konten. Dabei wird neben dem Passwort zusätzlich z. B. die Eingabe eines Codes (verschickt auf ein anderes Gerät in Ihrem Besitz), ein Fingerabdruckscan oder ein USB-Token zur Identifikation gefordert.
- Wählen Sie sichere Passwörter. Nutzen Sie einen Passwort-Manager, damit Sie Passwörter für viele Accounts verwalten können. - Teilen Sie nie Ihre Login-Daten mit Dritten.
- Überprüfen Sie regelmäßig die Sicherheitseinstellungen Ihrer Netzwerk-Accounts: Machen Sie so viele Bereiche wie möglich ausschließlich für Ihre Freunde sichtbar, z. B. Daten wie Telefonnummern, E-Mail oder auch die Chronik.
- Geben Sie nie Ihre Ausweis- oder Kontodaten in sozialen Netzwerken an.
- Beschränken Sie den Zugriff von anderen Apps z. B. auf Ihr Facebook-Konto. Sie können App-Verknüpfungen nur auf Kontodaten zulassen.
- Klicken Sie nicht auf verdächtige Links.
- Melden Sie Personen, die Sie andauernd unaufgefordert kontaktieren, dem Netzbetreiber. Erstellen Sie Anzeige bei der Polizei in schweren Fällen.

- Melden Sie Personen, die Sie oder andere beleidigen oder bedrohen dem Netzbetreiber oder unter www.internet-beschwerdestelle.de
- Melden Sie sich von einem Account nach der Nutzung immer ab. Dies ist besonders wichtig, wenn Sie über fremde Geräte bei Ihrem Account angemeldet waren.

4. Mangelnder Schutz von Smartphone und Tablet-PC

Die Sicherheitsanforderungen an mobile Geräte haben sich verändert. Gerade weil man mit Smartphones und Tablets kinderleicht im Internet surfen kann, bieten sie Angriffspunkte für Schadsoftware und Phishing. Hinzu kommt, dass viele Menschen Smartphones und Tablets dazu nutzen, Haustechnik und andere vernetzte Geräte zu steuern. Auf dem Vormarsch ist auch das Bezahlen per Smartphone – eine bequeme Anwendung, die immer mehr Menschen für sich entdecken. Je mehr Funktionen ein Smartphone im Alltag übernimmt, umso größer die Gefahr für Zugriffe von außen und Datenmissbrauch. Auch aus diesen Gründen vertrauen viele Nutzerinnen und Nutzer Cloud-Diensteanbietern, die Sicherheit bei der Datenverwaltung versprechen. Nutzer einer Cloud sind in der Lage, von jedem Endgerät mit einem Passwort auf die Inhalte und die Dienste der Cloud zurückzugreifen zu können. Doch auch dabei können vertrauliche Daten schnell in falsche Hände geraten.

Tipps:

- Nutzen Sie den Gerätesperrcode, die automatische Displaysperre und aktivieren Sie stets die SIM/USIM-PIN.
- Nutzen Sie nur App-Stores seriöser Anbieter. Bei Android: Verbieten Sie in den Einstellungen, dass Apps aus unbekannten Quellen auf Ihrem Gerät installiert werden können.
- Aktivieren Sie drahtlose Schnittstellen nur bei Bedarf. Tauschen Sie Daten nur mit vertrauenswürdigen Partnern aus.
- Öffnen Sie keine Links oder Dateien, die Sie von Unbekannten über Messenger erhalten haben.
- Nutzen Sie fremde WLANs, z. B. öffentliche Hotspots an Flughäfen oder in Cafés, nur mit einem VPN. Übermitteln Sie aber auch dann keine vertraulichen Daten.
- Nutzen Sie bei Verlust oder Diebstahl mögliche Ortungs-, Fernsperr- oder Löschdienste.
- Richten Sie Drittanbietersperren beim Provider ein, um sich vor Abofallen zu schützen.
- Löschen Sie alle sensiblen Daten, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät dafür auf Werkseinstellungen zurück.

5. Identitätsdiebstahl und Phishing

Identitätsdiebstahl liegt vor, wenn jemand persönliche Informationen einer anderen Person ausspäht und diese Daten zum Vorspielen einer falschen Identität nutzt. An persönlichen Daten gelangen die Betrüger durch Phishing. Dies geschieht oft durch drive-by-downloads: Besuchen Nutzerinnen und Nutzer infizierte Websites, wird im Hintergrund unbemerkt Schadsoftware auf ihrem Rechner installiert, die Daten abfängt. Betrüger fragen auch in E-Mails sensible Daten ab, indem sie sich als vertrauenswürdige Personen oder Institutionen ausgeben. Auch soziale Netzwerke werden genutzt, um Nutzer geschickt auf Seiten mit falschen Gewinnspiel- und Gratisaktionen zu locken und ihren Opfern gaukeln Betrüger vor, ein seriöses Unternehmen zu sein (mehr dazu unter „Straftaten in sozialen Netzwerken“). Beim Identitätsdiebstahl haben es Kriminelle nicht nur auf das Geld abgesehen – sie begehen im Namen ihrer ahnungslosen Opfer auch Straftaten.

Tipps:

- Antworten Sie niemals auf verdächtige E-Mails, Tweets oder Beiträge, in denen sie persönliche Daten preisgeben sollen. Füllen Sie keine Formulare oder Anmeldeseiten aus, auf die in diesen E-Mails verwiesen wird.
- Versenden Sie Passwörter grundsätzlich nie per E-Mail.
- Nutzen Sie Ihren E-Mail-Account nicht auf öffentlich zugänglichen Rechnern. Ihr Passwort kann dort von unberechtigten unbemerkt gespeichert werden.
- Banken oder Bezahl Dienste fordern Sie nie per E-Mail zur Eingabe Ihrer Kundendaten sowie Zugangs- und Bankdaten auf.
- Erstellen Sie in jedem Fall von Identitätsdiebstahl Strafanzeige. Melden Sie verdächtige E-Mails Ihrem E-Mail-Provider.

6. Weiterführende Links:

www.bsi.bund.de

www.sicher-im-netz.de

www.klicksafe.de

www.polizei-praevention.de

www.zivile-helden.de

Filtersoftware:

www.klicksafe.de

www.fsm.de

Suchmaschinen für Kinder:

www.fragfinn.de

www.blinde-kuh.de

Fakenews:

www.mimikama.org

3.Veranstaltung: „3D-Druck“ (15.02.2024, 21.05.2024) mit BayernLab Dillingen

3D-Druck ist ein additives Verfahren, bei dem ein dreidimensionales Werkstück computergesteuert schichtweise aufgebaut wird. Von CAD File zu Computationally Slice File. Die 3D-Druck Aufbereitung erfolgt folgendermaßen: Digitales Modell -> STL-Datei -> Slicing -> Druck -> 3D-Modell; Der 3D-Druck findet in vielen Bereichen Anwendung: Rapid Tooling, Rapid Prototyping, Rapid Manufacturing, Forschung und Entwicklung, Fertigung von Modellen, Hobby, Medizin, Kunst uvm.

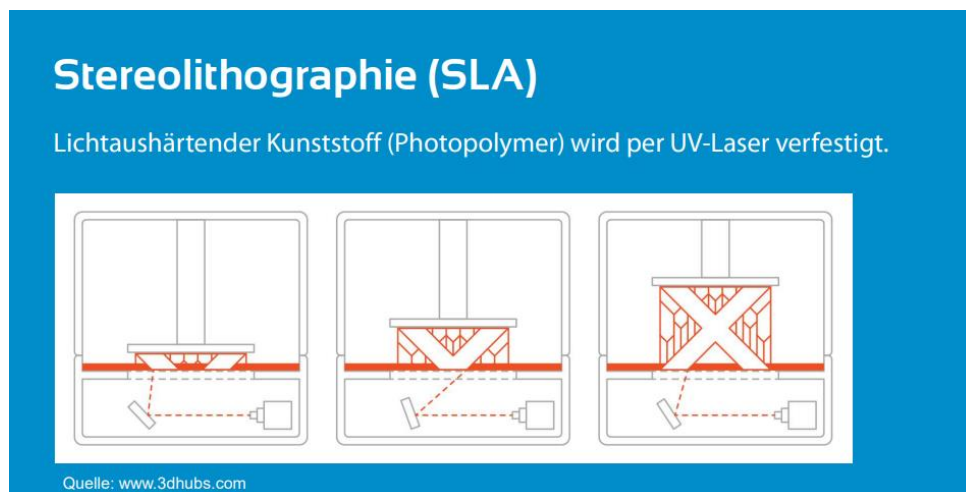
Vorteile:

- Konstruiertes 3D-Modell kann praktisch ohne Vorlaufzeit gefertigt werden
- Fertigung bis auf Losgröße 1 wirtschaftlich, Individuelle Anpassung bei Einzelstücken
- Inzwischen eine Vielzahl an Materialien, welche auch kombiniert werden können
- Geometrisch komplexe Formen herstellbar

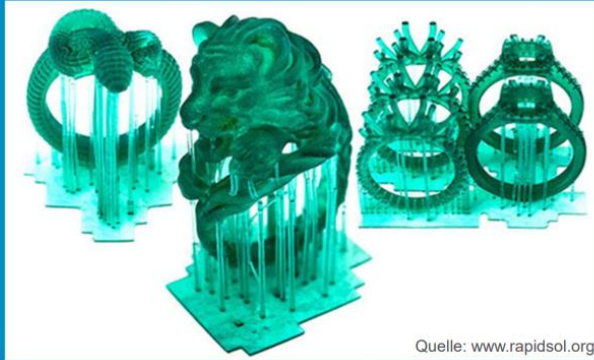
Einschränkungen:

- Bedingt durch den Schichtaufbau gewisse strukturelle Schwäche
- (Aufwändige) Nachbearbeitung bei fast allen Verfahren notwendig
- Kaum Skaleneffekte, daher nur bei geringen Stückzahlen konkurrenzfähig
- Vergleichsweise hohe Fertigungsdauer (objektabhängig)
- Geringere Genauigkeit (je nach Fertigungsverfahren)

1. Druckverfahren:

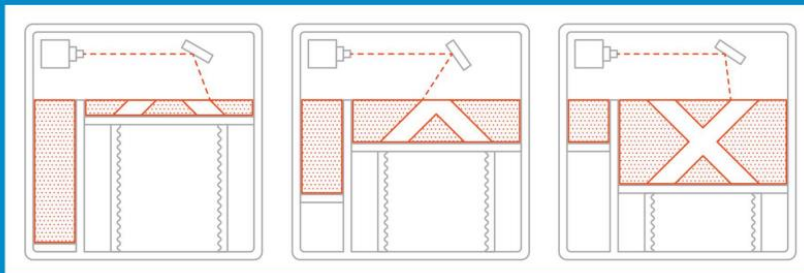


Stereolithographie (SLA)



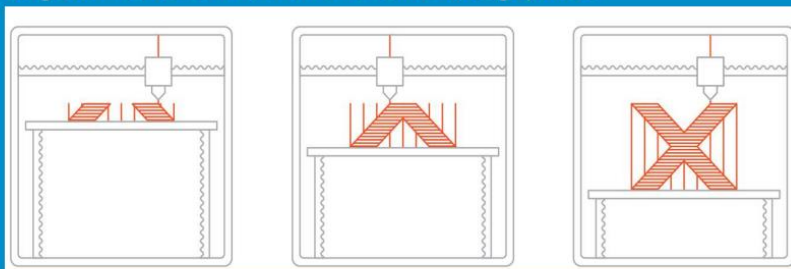
Selektives Laser Sintern (SLS)

Material in Pulverform wird zunächst bis kurz unter den Schmelzpunkt erhitzt und dann per Laser gesintert / verbacken.

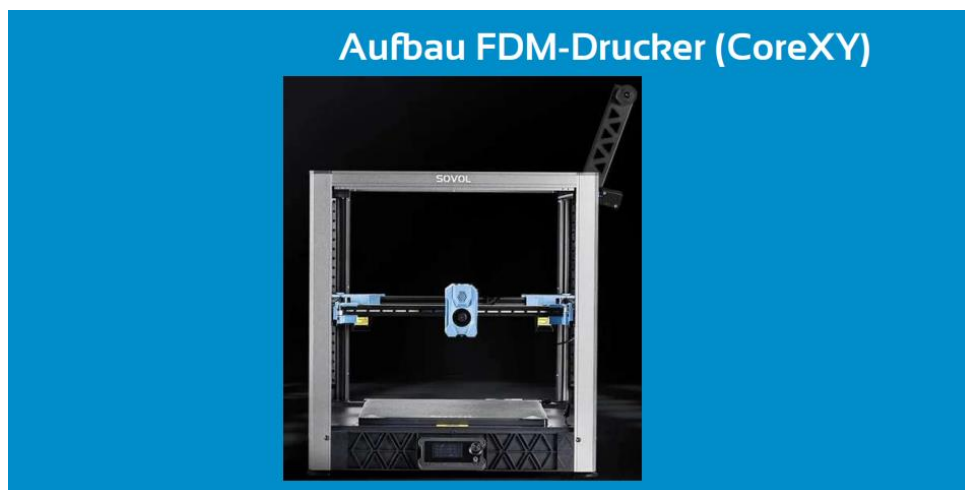
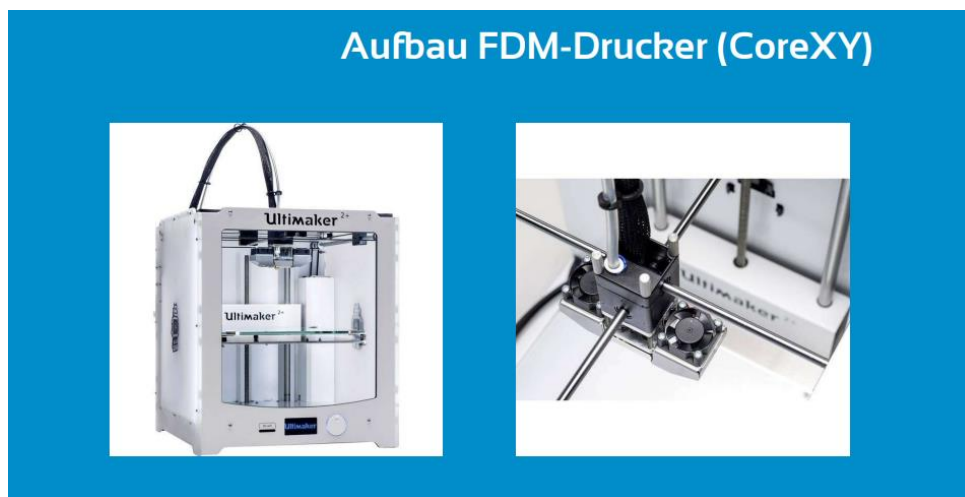
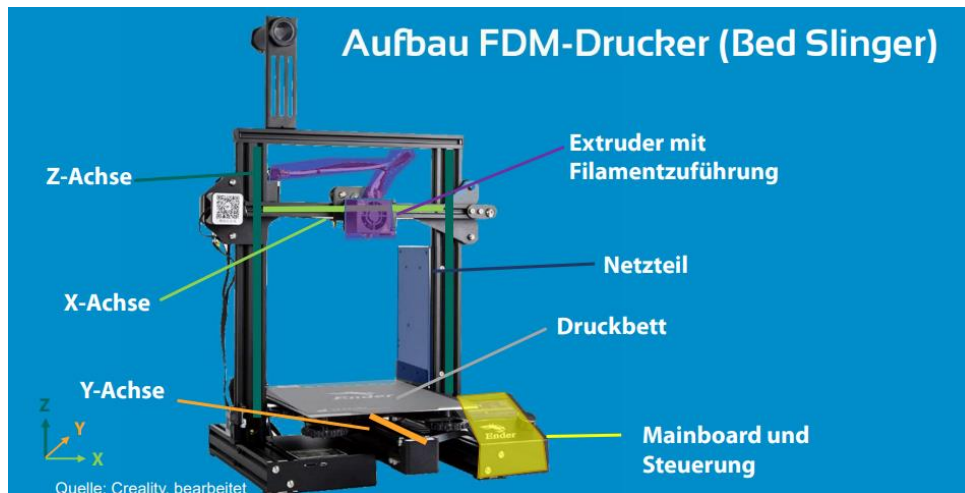


Schmelzschichtverfahren (FDM)

Thermokunststoff auf Filamentspulen wird in einen Extruder gezogen, dort aufgeschmolzen und durch eine feine Düse gepresst



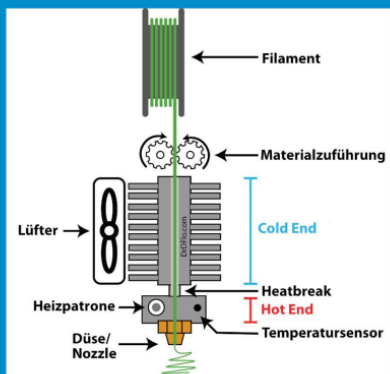
2. Aufbau FDM-Drucker:



Aufbau FDM-Drucker (Toolchanger)



Aufbau FDM-Extruder



Quelle: www.drfllo.com, bearbeitet

Die zwei Extruderarten unterscheiden sich nach Position der Materialzuführung

Direct Extrusion → Direkt am Extruder

- Für alle Filamentarten sehr gut geeignet
- Höheres Gewicht mit entsprechenden Problemen

Bowden → Am Rahmen des Druckers

- Leichter Druckkopf, damit höhere Geschwindigkeit möglich
- Probleme bei flexiblem und rauem Filament

3. Filament:

Im Hobbybereich sind vor allem zwei Materialarten vertreten:

- PLA (Polylactide / Polymilchsäuren)
- PETG (Polyethylenterephthalat)

Die Kosten bei beiden Materialien liegen zwischen 10 bis 30 € je Kilo Filament. Beide Materialien sind vergleichbar einfach zu drucken und einsteigerfreundlich. Durchmesser sind 1,75 mm oder 2,85 mm.

Das Filament PLA ist beinahe geruchsneutral, auf biologischer Basis und industriell kompostierbar, prinzipiell ohne beheiztes Druckbett druckbar, Bauteilkühlung erforderlich, lebensmittelecht, aber nicht spülmaschinenfest. Es ist einfach zu handhaben und somit das beste Material für den Einstieg.

Das Filament PETG ist die Modifizierung von PET mit Glykol, beinahe geruchsneutral, lebensmittelecht, spülmaschinenfest, hohe Schlagzähigkeit und äußert witterungsbeständig.

Das Filament TPU hat ein flexibles und robustes Material, feine Details sind schwer zu drucken, mögliche Probleme bei Filament Zufuhr und Retracting.

Das Filament ABS ist erdölbasiert, starke Geruchsbelastung und mögliche Rauchpartikel, nur druckbar mit beheizbarem Druckbett und Druckraum.

Das Filament Nylon ist sehr strapazierfähig, hohe chemische Beständigkeit und kann gut mit Textilfarbe eingefärbt werden.

Das Filament ASA hat eine hochwertige, kratz und schlagfeste Oberfläche, ist extrem Witterungsbeständig, resistent gegen viele Chemikalien, UV-Licht und vielen Ölen und Fetten.

4. Anschaffung eines 3D-Druckers:

Der Anschaffungspreis liegt zwischen 150 € und 1.000 € im Heimbereich. Bei der Beschaffung sollte der Anwendungsbereich, Druckqualität und Geschwindigkeit, die Größe des Druckers sowie möglicher Standort, Zeitaufwand bis zur Inbetriebnahme und Hilfestellung bei Problemen durch Hersteller oder Community berücksichtigt werden.

Der Standort für einen 3D-Drucker sollte gut bedacht werden. Aufgrund von Geräusch- und Geruchsbelästigung sollte der Raum gut gelüftet werden können. Der Drucker sollte auf einer ebenen, stabilen Fläche stehen. Mögliche Vibrationen sollten durch spezielle Füße oder Matten entgegengewirkt werden. Ein Luftzug sowie Temperaturschwankungen und hohe Feuchtigkeit sollte vermieden werden.

Mögliche Geräte für den Einstieg (FDM)



Anycubic - Kobra 2 / Neo
ab 145,00 EUR



Creality - Ender 3 V3 KE
ab 260,00 EUR



BambuLab – A1 Mini
ab 269,00 EUR

Geräte mit geschlossenem Bauraum (FDM)



Creality K1C
ab 539,00 EUR



BambuLab – P1S
ab 749,00 EUR



BambuLab – X1C
ab 1249,00 EUR

Gerät für den Einstieg mit Schwerpunkt Technik



Ledge iX

Ohne korrekte Kalibrierung ist ein problemloses Drucken kaum möglich. Hierbei ist der gleichmäßige, aber auch der korrekte Abstand zur Druckplatte wichtig. Muss manuell kalibriert werden, kann ein dünnes Blatt Papier (Kassenbon) verwendet werden.

An das 3D-Modell werden folgende Anforderungen gestellt:

- Geschlossener (wasserdichter) Volumenkörper
- Keine Flächenüberschneidungen (self intersection)
- Mindestwandstärke (je nach Material und Druckverfahren zwischen 0,3 und 2 mm)

Slicersoftware:

- Der Slicer wandelt das 3D-Objekt im STL oder OBJ-Format unter Berücksichtigung der Nutzereingaben in G-Code um.
- G-Code ist eine Abfolge von Befehlen, die die Bewegungen des Druckers steuern.
- Es gibt kostenpflichtige und kostenfreie Software.

5. Slicer – Wichtige Einstellungen

Temperatur:

- Die Drucktemperatur muss dem Material angepasst werden, ebenso die Temperatur der Druckplatte (falls beheizbar).
- Faustformel Düse:
 - PLA ~ 210°C, PETG ~ 230°C, ASA ~ 270°
- Faustformel Bett:
 - PLA ~ 50-60°C (oder unbeheizt)
 - PETG ~ 80° C
 - ASA ~ 90-110°C
- Auf Angaben des Herstellers achten, gleiches Material in unterschiedlichen Farben kann verschiedene Temperaturen benötigen.
- Mit einem sog. Temptower kann man die optimale Temperatur ermitteln.

Schichtstärke:

- Bei Objekten mit komplexer Geometrie kann die Qualität erhöht werden.
- Reduzierung der Schichtstärke erhöht die Druckzeit und damit die Kosten und die Fehlerwahrscheinlichkeit.

Wandstärke, obere und untere Schicht:

- Die Mindestwandstärke ist vom Düsendurchmesser abhängig, als Minimum sind 0,8 mm empfehlenswert.
- Die Stärke der obersten und untersten Schicht sollte oberhalb der Wandstärke, bei 0,8 mm oder mehr liegen.
- Eine höhere Stärke ist bei Objekten, die belastet oder geschliffen werden sollen, sinnvoll.

Druckgeschwindigkeit:

- Die Druckgeschwindigkeit hat unmittelbaren Einfluss auf die Druckqualität. Bei höherer Geschwindigkeit treten vermehrt Schwingungen auf, die das Druckbild negativ beeinflussen können.
- Eine Reduzierung der Geschwindigkeit kann bei vielen Problemen helfen.
- In Cura kann die Geschwindigkeit für verschiedene Parameter unterschiedlich eingestellt werden: Shell (Außenhülle) und TOP / Bottom (unterste und oberste Schichten) sind sichtbar. Hier kann eine Qualitätssteigerung durch Geschwindigkeitsreduktion erreicht werden. Die Inner Wall (Innenwand) kann schneller gedruckt werden, Infill (Füllung) und Helpers / Support noch schneller und Travel-Moves (Bewegungen ohne Materialextrusion) meist auf maximaler Geschwindigkeit.

Füllung:

- Die Füllung dient zum einen als Stütze für darüber liegende Schichten, zum anderen trägt sie zur Stabilität bei.
- Füllichte und Füllmuster haben Einfluss auf die Stabilität, aber auch auf Materialverbrauch und Druckdauer.

- Bei Objekten, die nicht belastet werden, reichen 10-15 % normalerweise aus, ansonsten sind mehr als 70 % selten sinnvoll.

Stützstruktur:

- Beim FDM-Druck sind Stützstrukturen notwendig, um Überhänge und Brücken zu drucken.
- Überhänge bis 45° und Brücken bis 5 mm können ohne Support gedruckt werden.
- Die Stützstrukturen müssen entfernt werden und hinterlassen meist eine unsaubere Oberfläche.
- Ein gewisser Abstand zwischen Objekt und Stützstruktur ist notwendig, damit es nicht zu einer zu festen Verbindung kommt.
- Bei Druckern mit Doppelsextrusion besteht die Möglichkeit, mit löslichem Material zu drucken, um Rückstände zu vermeiden.
- Durch andere Ausrichtung oder Teilung des Objektes kann man die Notwendigkeit von Stützstrukturen vermeiden.

Druckbehaftung:

Es gibt 3 unterschiedliche Einstellungen für die Haftung.

- **Skirt:** Linien ohne direkten Kontakt
- **Brim:** Linien mit Kontakt
- **Raft:** Einige Schichten Auflagefläche

Nachbearbeitung:

Je nach Druckqualität und gewünschtem Resultat, ist eine teils aufwändige Nachbearbeitung notwendig:

- Supportmaterialien entfernen, Entgraten, Schleifen, Polieren
- Unebenheiten ausbessern, Verkleben
- Grundieren, Lackieren, Bemalen
- Spezielle Harze für eine glasartige Oberfläche auftragen
- Bedampfen mit Aceton (bei ABS) oder Hitzebehandlung

Plattformen für 3D-Objekte:

Thingiverse - <https://www.thingiverse.com>

Printables - <https://www.printables.com>

Makerworld - <https://www.makerworld.com>

Cults3D - <https://www.cults3d.com>

Programme:

Cura - <https://ultimaker.com/software/ultimaker-cura>

PrusaSlicer - <https://www.prusa3d.com/>

Bambu Studio - <https://www.bambulab.com>

Meshmixer - <http://www.meshmixer.com0>

BayernLab

Eine Initiative des Bayerischen Staatsministeriums
der Finanzen und für Heimat



4. Veranstaltung: „Bayernatlas“ (14.03.2024, 24.07.2024) mit Franziska Berger, Vermessungsamt Dillingen

Den BayernAtlas erreichen Sie unter folgender Domain: www.bayernatlas.de.

- Luftbildbefliegung im Zweijahresrhythmus: Die Luftbilder werden im Mai/Juni alle zwei Jahre aktualisiert.
- Schnelle Aktualisierung neuer Baugebiete: Nach dem Vermessen wird ein neues Baugebiet innerhalb von etwa 2 Wochen integriert.

Der BayernAtlas bietet eine Vielzahl von Funktionen zur Erkundung Ihrer Umgebung und zur Planung Ihrer Freizeitaktivitäten:

- 3D-Darstellung: Erleben Sie Gebäude und Gelände in 3D-Grafik.
- Historische Karten: Entdecken Sie die Vergangenheit mit historischen Karten aus dem 19. und 20. Jahrhundert.
- Vielfältige Themenkarten: Wählen Sie aus einer breiten Palette von Themenkarten für unterschiedliche Interessen.
- Digitalisierung und Speicherung von Vektordaten: Speichern und laden Sie Ihre eigenen Vektordaten im gpx- oder kml-Format.
- Web Map Services (WMS): Integrieren Sie externe Kartendienste nahtlos in den BayernAtlas.
- Vielseitige Endgeräte-Unterstützung: Nutzen Sie den BayernAtlas auf verschiedenen Geräten wie Computern, Smartphones und Tablets.
- Freizeit-Routing: Planen Sie Ihre Routen auf Freizeitwegen und erleben Sie Ihre Umgebung auf ganz neue Weise.

Die Plus-Version bietet erweiterte Funktionen zu einem monatlichen Preis von 40 €. Hier sind die Hauptunterschiede zur kostenlosen Version:

- Hochauflösende Luftbilder: Die Plus-Version bietet eine Genauigkeit von 20 cm, während die kostenlose Version eine Genauigkeit von 40 cm bietet.
- Zusätzliche Kartenebenen: Höhenlinien, Höhen- und Lagefestpunkte, historische Karten ab 2003, digitale Flurkarten sowie Daten zur Bodenschätzung und tatsächlichen Nutzung sind nur in der Plus-Version verfügbar.
- Flurnummern: Diese werden ausschließlich in der kostenpflichtigen Version angezeigt.



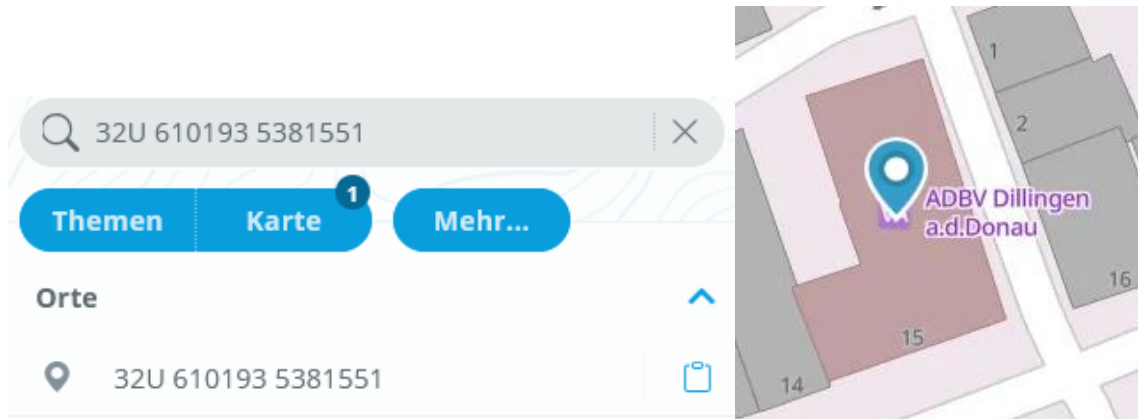
Übungen zum BayernAtlas

1. Was finden Sie unter den Koordinaten 32U 610193 5381551?

Lösung: Das Amt für Digitalisierung, Breitband und Vermessung Dillingen a.d.Donau

Vorgehen:

32U 610193 5381551 in Suchleiste eingeben und das Ergebnis unter „Orte“ auswählen.



2. Wie lange ist die Innenbahn der Laufbahn im Dillinger Stadion?

Lösung: ca. 400 Meter

Vorgehen:

Hintergrundkarte Luftbild auswählen, anschließend mit Messen die Innenlaufbahn abklicken.

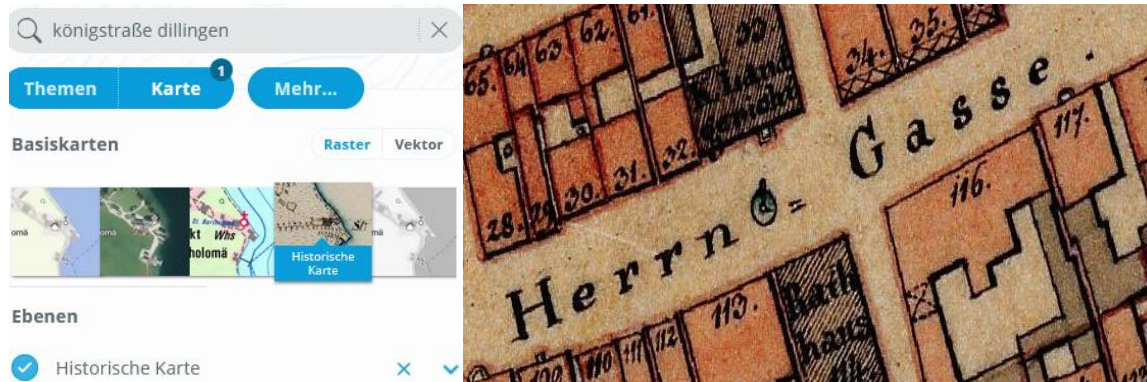


3. Wie hieß die Königstraße in Dillingen Anfang des 19. Jahrhunderts?

Lösung: Herrn-Gasse

Vorgehen:

Die Königstraße suchen und im Reiter Karten die Historische Karte auswählen.

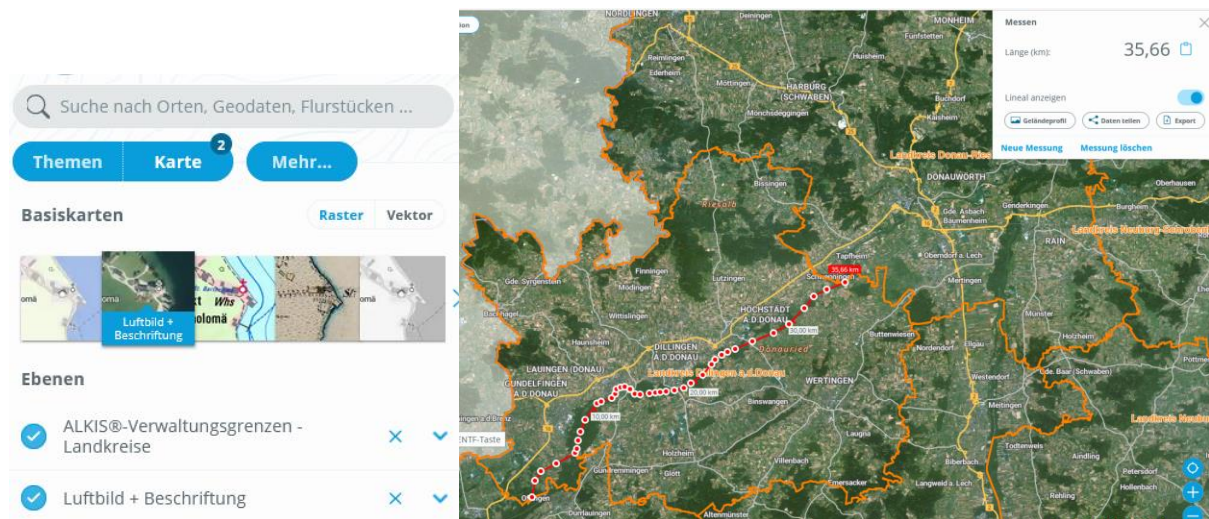


4. Auf welche Länge erstreckt sich die Donau in unserem Landkreis in Kilometern?

Lösung: ca. 35 km

Vorgehen:

Im Reiter Themen unter Verwaltung und Bildung die ALKIS-Verwaltungsgrenzen - Landkreise auswählen. Anschließend im Reiter Karte das Luftbild auswählen und mit Messen die Donau von der einen Landkreisgrenze bis zur anderen Landkreisgrenze durchklicken.



5. Wie viele Schlösser, Burgen und Ruinen gibt es im Landkreis Dillingen?

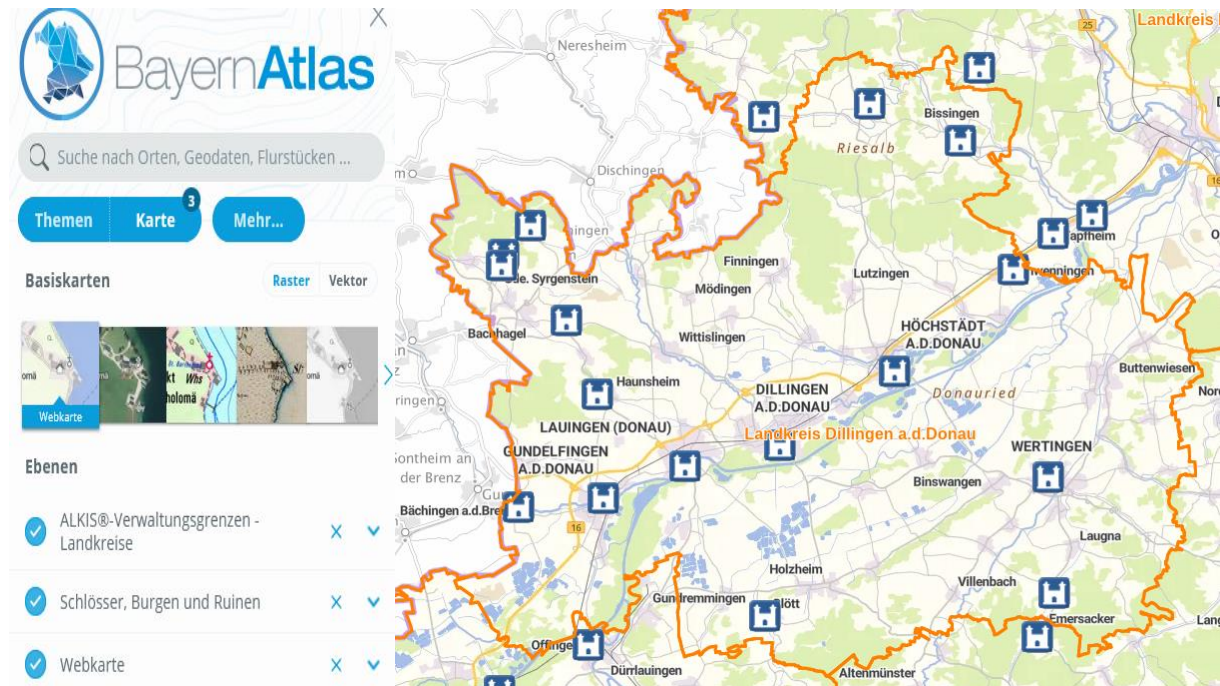
Lösung: 16 Stück

Vorgehen:

Im Reiter Themen unter Verwaltung und Bildung die ALKIS-Verwaltungsgrenzen-Landkreise auswählen. Anschließend im Reiter Themen unter Kultur und Heimat die Schlösser, Burgen und Ruinen auswählen.

Tipp:

Wenn man ein Symbol anklickt, öffnet sich links die Objektinformation zu allen eingeblendeten Diensten. In diesem Fall zu den Landkreisgrenzen und den Schlössern, Burgen und Ruinen. Bei den Schlössern ist z.B. die Homepage verlinkt.



6. Planen Sie eine Wanderung

Vorgehen:

- Suchen Sie einen Startpunkt für Ihre Strecke, z.B. Ihren Heimatort, Schule oder einen Ausgangspunkt für Wanderungen.
- Im Reiter Karte können Sie die Hintergrundkarte wechseln. Z.B. die Topographische Karte zur Darstellung des Wegenetzes oder das Luftbild zur Darstellung der Vegetation.
- Am unteren Bildschirmrand finden Sie unter Zeichnen Werkzeuge, um Strecken zu analysieren, Entfernungen und Höhenprofile darzustellen und eigene Informationen in die Karte zu integrieren.
 - Symbol: Erstellung eines beschrifteten Symbols, zu dem eine Beschreibung hinzugefügt werden kann. Diese Inhalte werden sichtbar, wenn man das Symbol in einer geteilten Karte anklickt.
 - Text: Einbinden eines Textes in die Karte
 - Linie: Erstellen von Linien/Flächen und Darstellung des Höhenprofils der Linie.
 - Messen: Messen von Strecken und Flächen, Darstellung eines Höhenprofils.
 - Teilen: Möglichkeit, den erstellten Karteninhalt über einen Link zu teilen. Die mit dem BayernAtlas digitalisierten Objekte werden ca. 1 Jahr serverseitig gespeichert.
- Zeichnen Sie mit dem Werkzeug Linie Ihren gewünschten Weg ein. Dieser kann vorhandenen Wegen folgen, oder Sie erstellen eine eigene Route. Vorhandene Wanderwege finden Sie im Reiter Themen → Sport und Freizeit → Wander- und Radwege. Hier sind allerdings nur tatsächlich vor Ort ausgeschilderte Wanderwege hinterlegt.

- Wenn Sie die Linie mit einem Doppelklick abschließen, können Sie sich das Höhenprofil anzeigen lassen.
- Besondere Punkte können mit dem Werkzeug Symbol markiert werden. In diesem Fall z.B. der Start- und Endpunkt, Hindernisse, Gefahrenstellen, Rastplätze oder andere wichtige Orte.
- Wenn Sie Ihre Linien/Symbole editieren möchten, können Sie sie im Werkzeug Zeichnen anklicken und abändern. Dabei können Sie Symbole und Knickpunkte verschieben, löschen oder hinzufügen. Weiter ist es möglich, Farben sowie Beschreibungen zu ändern oder die Objekte komplett zu löschen.
- Unter Themen können Sie weitere Daten laden, die Sie in Ihrer Karte darstellen wollen. Beispielweise finden Sie Hütten und Jugendherbergen unter Unterkünften bei Sport und Freizeit, oder Bau- und Bodendenkmäler unter Planen und Bauen.
- Wenn Sie mit Ihrer Streckenführung und Kartendarstellung zufrieden sind, können Sie die Karte entweder drucken oder als .kml-, .gpx-, GeoJSON- oder EWKT-Datei exportieren. Für einen Druck wählen Sie im unteren Bildschirm Export aus und stellen die gewünschte Position und den Maßstab ein. Für den Export wählen Sie im Menü Zeichnen Export und dann das gewünschte Dateiformat (kml, gpx, GeoJSON oder EWKT) aus und speichern Ihre Objekte auf einen Datenträger.
- Über das Werkzeug Teilen am unteren Bildschirmrand kann die aktuelle Kartendarstellung mit einem Link versehen, als E-Mail versendet und als QR-Code-Link erstellt werden (z.B. für eine weitere Nutzung auf mobilen Geräten). Falls die Karte in eine Website oder einen Blog eingebettet werden soll, ist dies über den BayernAtlas-IFrame möglich.
- Der BayernAtlas-IFrame dient dazu, erstellte und hinzugefügte Inhalte des BayernAtlas in eigene Internetseiten oder Blogs einzubinden. Der Link des IFrames kann kopiert und in eine eigene Website eingebaut werden.

5.Veranstaltung: „Künstliche Intelligenz“ (07.05.2024, 17.06.2024 und 20.06.2024) mit Kilian Modl, BayernLab Dillingen

Egal ob Empfehlungen bei Streamingdiensten, Kontrollmechanismen bei sozialen Medien, Navigationssysteme, Smart Home oder Gesichtserkennung: Künstliche Intelligenz ist in unserem Alltag nicht mehr wegzudenken. Mit Hilfe der Gesichtserkennung in Verbindung mit „Künstlicher Intelligenz“ konnte erst dieses Jahr die RAF-Terroristin Daniela Klette festgenommen werden.

In der heutigen digitalen Welt revolutionieren KI-gestützte Technologien die Art und Weise, wie Inhalte erstellt werden. Zwei herausragende Bereiche dieser Entwicklung sind die textbasierte generative KI und die generative Bild-KI, die jeweils einzigartige Möglichkeiten und Anwendungen bieten.

1. Generative Bild-KI

Generative Bild-KI sind Computerprogramme, die darauf trainiert sind, neue Bilder zu erstellen, die so aussehen, als wären sie von einem Menschen gemacht worden. Diese Technologie wird für verschiedene Zwecke genutzt, von der Erstellung digitaler Kunst über das Design von Mode und Möbeln bis hin zur Entwicklung von Computerspielen.

1.1 Grundlagen der Generativen Bild-KI

Training von Generativer Bild-KI: Ein einfacher Überblick

Der Trainingsprozess einer generativen Bild-KI ist vergleichbar mit der Ausbildung eines Künstlers. Hier sind die Schritte, die typischerweise involviert sind, vereinfacht dargestellt:

1. Datensammlung

Zuerst sammelt man viele Bilder, die als Lehrmaterial für die KI dienen. Diese Bilder können alles sein, von Landschaften bis zu Porträts, je nachdem, welche Art von Bildern die KI später erzeugen soll.

2. Lernen von Merkmalen

Während des Trainings analysiert die KI diese Bilder und lernt, wichtige Merkmale und Muster zu erkennen. Zum Beispiel könnte die KI lernen, welche Farben und Formen typisch für einen Sonnenuntergang sind oder wie das Gesicht einer Person strukturiert ist.

3. Erzeugung neuer Bilder

Nachdem die KI genug gelernt hat, beginnt sie, eigene Bilder zu erstellen. Diese Bilder basieren auf den Mustern und Merkmalen, die sie aus den Trainingsbildern gelernt hat. Ähnlich wie ein Maler, der nach viel Übung ein neues Kunstwerk schafft, generiert die KI Bilder, die den gelernten Stilen oder Motiven ähneln.

Die Technologien hinter der generativen Bild-KI, insbesondere GANs und VAEs, helfen Computern, Bilder auf ähnliche Weise zu erstellen, wie Menschen malen oder zeichnen.

Die Technologien hinter der generativen Bild-KI, insbesondere **GANs** und **VAEs**, helfen Computern, Bilder auf ähnliche Weise zu erstellen, wie Menschen malen oder zeichnen.

GANs (Generative Adversarial Networks):

Stellen Sie sich vor, zwei Künstler (ein Generator und ein Diskriminator) arbeiten zusammen, um perfekte Kunstfälschungen zu erstellen. Der Generator erstellt ein Bild, und der Diskriminator bewertet es. Wenn der Diskriminator entscheidet, dass das Bild noch nicht echt genug aussieht, versucht der Generator es erneut. Dieser Prozess wiederholt sich, bis die Bilder nicht mehr von echten unterscheidbar sind.

VAEs (Variational Autoencoders):

Denken Sie an einen Künstler, der lernt, durch das Studium vieler Bilder in einem bestimmten Stil zu zeichnen. Nachdem er den Stil gelernt hat, kann er neue Bilder in diesem Stil kreieren, indem er die grundlegenden Merkmale dieses Stils verwendet. VAEs arbeiten ähnlich, indem sie lernen, wie Daten aussehen, und dann neue Daten erzeugen, die diesen ähnlich sind.

Generierung:

Nach dem Training kann das KI-Modell dann neue Bilder erstellen. Diese Bilder basieren auf den Mustern und Merkmalen, die es während des Trainings gelernt hat. Es ist, als würde ein Künstler ein neues Werk schaffen, das von den vielen anderen Bildern inspiriert ist, die er gesehen hat.

1.2 Anwendungen der Generativen Bild-KI

- **Digitale Kunst:** Künstler nutzen KI, um einzigartige Werke zu schaffen, die sonst nicht möglich wären. Dies umfasst alles von abstrakter Kunst bis hin zu hyperrealistischen Bildern.
- **Produktdesign:** Designer verwenden KI um innovative Produktkonzepte zu entwickeln. Dies reicht von Möbeln, die noch nie zuvor gesehen wurden, bis hin zu futuristischen Fahrzeugdesigns.
- **Wissenschaftliche Visualisierung:** Forscher nutzen KI, um komplexe wissenschaftliche Daten in visuell ansprechender Form darzustellen, wie z.B. die Visualisierung von Klimaveränderungen oder die Struktur komplexer Moleküle.
- **Architektur und Stadtplanung:** Architekten und Stadtplaner nutzen KI, um realistische 3D-Modelle von Gebäuden und urbanen Layouts zu generieren, was den Planungsprozess beschleunigt und visuell darstellt.
- **Video- und Filmproduktion:** In der Filmindustrie wird generative Bild-KI eingesetzt, um realistische CGI-Effekte zu erzeugen, Charaktere zu animieren oder sogar ganze Szenen zu generieren, die in der realen Welt schwer umzusetzen wären.
- **Gaming:** Spieleentwickler verwenden generative Bild-KI um Texturen, Landschaften und sogar spielbare Charaktere zu erzeugen, was die Entwicklung beschleunigt und neue Arten von Spielerlebnissen ermöglicht.

2. Textbasierte Generative KI-Tools

Textbasierte generative KI umfasst Technologien, die darauf spezialisiert sind Texte zu erzeugen, die natürlich und menschenähnlich wirken. Diese Systeme finden Anwendung in einer Reihe von Bereichen, von der automatisierten Kundenbetreuung bis hin zur Erstellung von Inhalten.

2.1 ChatGPT: KI-Sprachmodell für kreative Texterstellung

KI-Tool: ChatGPT ist ein KI-Sprachmodell von OpenAI, das auf der Grundlage von GPT-3 entwickelt wurde und sich durch seine Fähigkeit zur Generierung kreativer Textformate auszeichnet.

Zielgruppe: ChatGPT richtet sich an alle, die ein KI-Tool suchen, das Ihnen bei der Erstellung von kreativen Texten helfen kann, z. B.

- Gedichte
- Code
- Drehbücher
- Musikstücke
- E-Mails
- Briefe
- Blogbeiträge
- Werbespots
- Social-Media-Beiträge
- und vieles mehr

Funktionsweise:

- Basierend auf der Transformer-Architektur und mit einem riesigen Datensatz aus Text und Code trainiert.
- Kann verschiedene kreative Textformate erstellen und dabei verschiedene Vorgaben und Anforderungen berücksichtigen.
- Kann in verschiedenen Sprachen arbeiten.
- Bietet verschiedene Funktionen zur Optimierung der Nutzererfahrung, z. B. verschiedene Einstellungsoptionen und die Möglichkeit, verschiedene kreative Textformate auszuwählen.

2.2 G Gemini: KI-Sprachmodell von Google

KI-Tool: Gemini ist ein multilinguales KI-Sprachmodell von Google AI, das sich durch seine Fähigkeit auszeichnet, verschiedene Informationsformate zu verarbeiten und zu verstehen.

Zielgruppe: Gemini richtet sich an alle, die ein KI-Sprachmodell suchen, das

- Texte generieren kann,
- Sprachen übersetzen kann,
- Fragen umfassend und informativ beantworten kann,
- verschiedene kreative Textformate erstellen kann,
- verschiedene Arten von Informationen wie Text, Audio, Bilder und Videos verarbeiten kann.

Funktionsweise:

- Basierend auf der Transformer-Architektur und mit einem riesigen Datensatz aus Text und Code trainiert.
- Kann verschiedene Aufgaben ausführen, z. B.
 - verschiedene kreative Textformate erstellen (Gedichte, Code, Drehbücher, Musikstücke, E-Mails, Briefe usw.)
 - Sprachen übersetzen
 - deine Fragen umfassend und informativ beantworten
 - verschiedene Arten von Informationen wie Text, Audio, Bilder und Videos verarbeiten
- Befindet sich noch in der Entwicklung, lernt aber ständig neue Aufgaben und Fähigkeiten.

2.3 Pi: Die KI für persönliche Gespräche

KI-Tool: Pi ist ein KI-Chatbot von Inflection AI, der sich durch seine "emotionale Intelligenz" von anderen Chatbots abhebt.

Zielgruppe: Pi richtet sich an alle, die einen intelligenten und persönlichen Gesprächspartner suchen.

Funktionsweise:

- Nutzt generative KI um menschenähnliche Texte zu erstellen.
- Kann Fragen beantworten, Informationen liefern und kreative Textformate erstellen.
- Lernt und passt sich an die Interaktionen mit dem Nutzer an.
- Bietet ein „emphatisches, freundliches und persönliches“ Gesprächserlebnis.

Eingeschränkte Funktionen:

- Kann im Gegensatz zu anderen KI-Tools wie ChatGPT keine Bilder generieren oder andere innovative Features nutzen.
- Greift im Gegensatz zu anderen KI-Tools auf keine externen Informationen wie das Internet zu und kann daher keine aktuellen Informationen liefern.

2.4 Perplexity: KI-Suchmaschine mit Fokus auf Informationsbeschaffung

KI-Tool: Perplexity ist eine KI-Suchmaschine von Dell, die sich durch die Bereitstellung von Quellenangaben von anderen Suchmaschinen unterscheidet.

Zielgruppe: Perplexity richtet sich an alle, die nach fundierten Informationen suchen und die Quellen der bereitgestellten Informationen überprüfen möchten.

Funktionsweise:

- Nutzt KI und Suchmaschinen, um Informationen zu einem breiten Themenspektrum bereitzustellen.
- Bietet präzise und umfassende Antworten auf komplexe Fragen.
- Zitiert Quellen für alle Informationen, sodass die Nutzer die Richtigkeit der Informationen überprüfen können.
- Ermöglicht die Suche nach weiteren Informationen und ähnlichen Themen.
- Bietet verschiedene Funktionen zur Optimierung der Nutzererfahrung, z. B. intelligente Suchstrategien und Datenschutz-Einstellungen.

2.5 Unterschiede zwischen kostenlosen und kostenpflichtigen Versionen

Funktionalität und Features:

- **Kostenlos:** Kostenlose Versionen bieten oft Basisfunktionen mit begrenzten Kapazitäten. Dies könnte Einschränkungen in Bezug auf die Anzahl der Anfragen, die Antwortgeschwindigkeit oder den Zugang zu fortschrittlicheren Algorithmen umfassen.
- **Kostenpflichtig:** Kostenpflichtige Versionen erweitern in der Regel die Funktionalität erheblich. Dies umfasst Zugang zu leistungsfähigeren Modellen, erweiterten Anpassungsmöglichkeiten, höheren Anfragegrenzen und Priorität bei der Verarbeitung der Anfragen.

Support und Wartung:

- **Kostenlos:** Support ist bei kostenlosen Tools oft begrenzt oder nicht vorhanden. Nutzer müssen sich häufig auf Community-Foren oder Basisdokumentationen verlassen.
- **Kostenpflichtig:** Kostenpflichtige Abonnements schließen in der Regel umfassenden technischen Support ein, der schnelle Hilfe und regelmäßige Updates bietet. Dies kann auch dedizierten Support umfassen, bei dem Kunden direkte Ansprechpartner haben.

Datenschutz und Sicherheit:

- **Kostenlos:** Bei kostenlosen Tools können Datenschutz und Datensicherheit eingeschränkter sein, da der Anbieter möglicherweise Daten sammelt, um das Produkt zu verbessern oder zu monetarisieren.
- **Kostenpflichtig:** Bei bezahlten Versionen gibt es oft strengere Datenschutzrichtlinien, die den Schutz sensibler Daten garantieren. Unternehmen, die für den Service zahlen, können in der Regel eine höhere Datenvertraulichkeit und Sicherheit erwarten.

Anpassung und Integration:

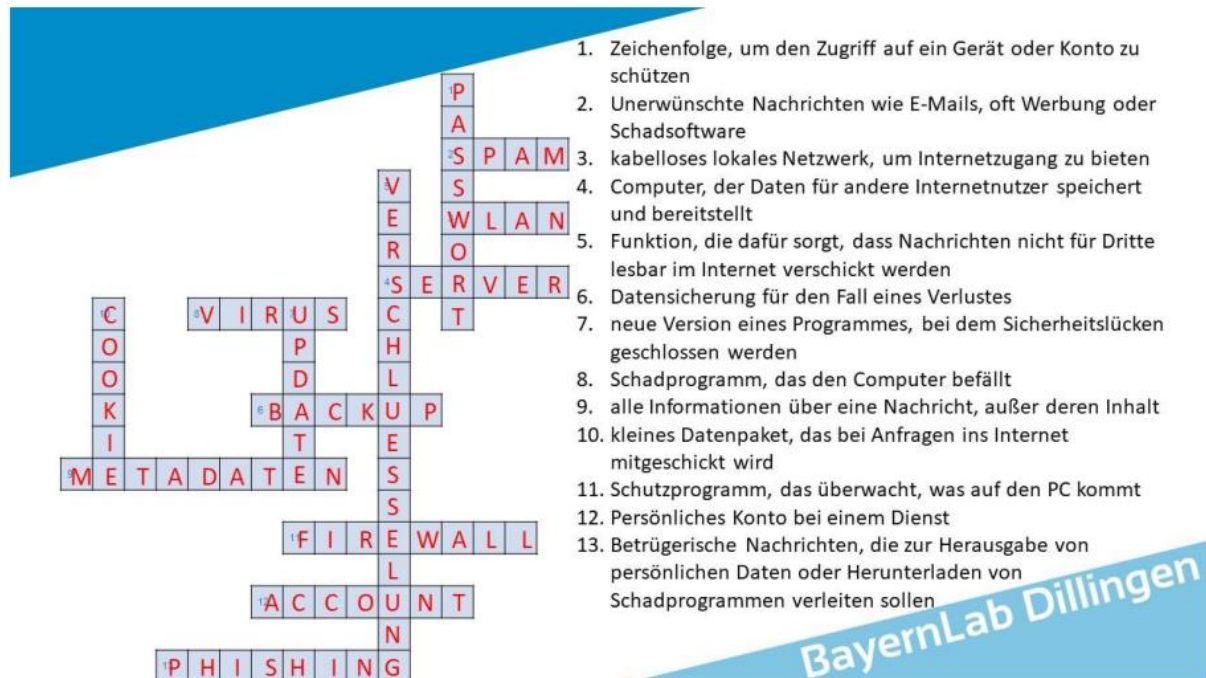
- **Kostenlos:** Kostenlose Tools bieten oft nur standardisierte Optionen mit geringen bis keinen Anpassungsmöglichkeiten.
- **Kostenpflichtig:** Bezahlte Angebote können in der Regel an spezifische Bedürfnisse angepasst werden und bieten Optionen zur Integration in bestehende Systeme und Workflows.



6. Veranstaltung: „**Digitaler Kompass: Internetsicherheit und Medienkompetenz für (Groß)-Eltern und Pädagogen**“ (28.01.2025) mit Kilian Modl, BayernLab Dillingen

Internetsicherheit allgemein

Wichtige Begriffe zu Internetsicherheit und Datenschutz



A crossword puzzle with the following words filled in:

- Across: 1. COOKIES, 2. VIRUS, 3. BACKUP, 4. METADATEN, 5. FIREWALL, 6. ACCOUNT, 7. PHISHING, 8. SPAM, 9. WLAN, 10. SERVER, 11. CHL, 12. PATCH, 13. PASSWORD, 14. PHISHING, 15. SPAM, 16. WLAN, 17. SERVER, 18. CHL, 19. PATCH, 20. PASSWORD, 21. PHISHING, 22. SPAM, 23. WLAN, 24. SERVER, 25. CHL, 26. PATCH, 27. PASSWORD, 28. PHISHING, 29. SPAM, 30. WLAN, 31. SERVER, 32. CHL, 33. PATCH, 34. PASSWORD, 35. PHISHING, 36. SPAM, 37. WLAN, 38. SERVER, 39. CHL, 40. PATCH, 41. PASSWORD, 42. PHISHING, 43. SPAM, 44. WLAN, 45. SERVER, 46. CHL, 47. PATCH, 48. PASSWORD, 49. PHISHING, 50. SPAM, 51. WLAN, 52. SERVER, 53. CHL, 54. PATCH, 55. PASSWORD, 56. PHISHING, 57. SPAM, 58. WLAN, 59. SERVER, 60. CHL, 61. PATCH, 62. PASSWORD, 63. PHISHING, 64. SPAM, 65. WLAN, 66. SERVER, 67. CHL, 68. PATCH, 69. PASSWORD, 70. PHISHING, 71. SPAM, 72. WLAN, 73. SERVER, 74. CHL, 75. PATCH, 76. PASSWORD, 77. PHISHING, 78. SPAM, 79. WLAN, 80. SERVER, 81. CHL, 82. PATCH, 83. PASSWORD, 84. PHISHING, 85. SPAM, 86. WLAN, 87. SERVER, 88. CHL, 89. PATCH, 90. PASSWORD, 91. PHISHING, 92. SPAM, 93. WLAN, 94. SERVER, 95. CHL, 96. PATCH, 97. PASSWORD, 98. PHISHING, 99. SPAM, 100. WLAN, 101. SERVER, 102. CHL, 103. PATCH, 104. PASSWORD, 105. PHISHING, 106. SPAM, 107. WLAN, 108. SERVER, 109. CHL, 110. PATCH, 111. PASSWORD, 112. PHISHING, 113. SPAM, 114. WLAN, 115. SERVER, 116. CHL, 117. PATCH, 118. PASSWORD, 119. PHISHING, 120. SPAM, 121. WLAN, 122. SERVER, 123. CHL, 124. PATCH, 125. PASSWORD, 126. PHISHING, 127. SPAM, 128. WLAN, 129. SERVER, 130. CHL, 131. PATCH, 132. PASSWORD, 133. PHISHING, 134. SPAM, 135. WLAN, 136. SERVER, 137. CHL, 138. PATCH, 139. PASSWORD, 140. PHISHING, 141. SPAM, 142. WLAN, 143. SERVER, 144. CHL, 145. PATCH, 146. PASSWORD, 147. PHISHING, 148. SPAM, 149. WLAN, 150. SERVER, 151. CHL, 152. PATCH, 153. PASSWORD, 154. PHISHING, 155. SPAM, 156. WLAN, 157. SERVER, 158. CHL, 159. PATCH, 160. PASSWORD, 161. PHISHING, 162. SPAM, 163. WLAN, 164. SERVER, 165. CHL, 166. PATCH, 167. PASSWORD, 168. PHISHING, 169. SPAM, 170. WLAN, 171. SERVER, 172. CHL, 173. PATCH, 174. PASSWORD, 175. PHISHING, 176. SPAM, 177. WLAN, 178. SERVER, 179. CHL, 180. PATCH, 181. PASSWORD, 182. PHISHING, 183. SPAM, 184. WLAN, 185. SERVER, 186. CHL, 187. PATCH, 188. PASSWORD, 189. PHISHING, 190. SPAM, 191. WLAN, 192. SERVER, 193. CHL, 194. PATCH, 195. PASSWORD, 196. PHISHING, 197. SPAM, 198. WLAN, 199. SERVER, 200. CHL, 201. PATCH, 202. PASSWORD, 203. PHISHING, 204. SPAM, 205. WLAN, 206. SERVER, 207. CHL, 208. PATCH, 209. PASSWORD, 210. PHISHING, 211. SPAM, 212. WLAN, 213. SERVER, 214. CHL, 215. PATCH, 216. PASSWORD, 217. PHISHING, 218. SPAM, 219. WLAN, 220. SERVER, 221. CHL, 222. PATCH, 223. PASSWORD, 224. PHISHING, 225. SPAM, 226. WLAN, 227. SERVER, 228. CHL, 229. PATCH, 230. PASSWORD, 231. PHISHING, 232. SPAM, 233. WLAN, 234. SERVER, 235. CHL, 236. PATCH, 237. PASSWORD, 238. PHISHING, 239. SPAM, 240. WLAN, 241. SERVER, 242. CHL, 243. PATCH, 244. PASSWORD, 245. PHISHING, 246. SPAM, 247. WLAN, 248. SERVER, 249. CHL, 250. PATCH, 251. PASSWORD, 252. PHISHING, 253. SPAM, 254. WLAN, 255. SERVER, 256. CHL, 257. PATCH, 258. PASSWORD, 259. PHISHING, 260. SPAM, 261. WLAN, 262. SERVER, 263. CHL, 264. PATCH, 265. PASSWORD, 266. PHISHING, 267. SPAM, 268. WLAN, 269. SERVER, 270. CHL, 271. PATCH, 272. PASSWORD, 273. PHISHING, 274. SPAM, 275. WLAN, 276. SERVER, 277. CHL, 278. PATCH, 279. PASSWORD, 280. PHISHING, 281. SPAM, 282. WLAN, 283. SERVER, 284. CHL, 285. PATCH, 286. PASSWORD, 287. PHISHING, 288. SPAM, 289. WLAN, 290. SERVER, 291. CHL, 292. PATCH, 293. PASSWORD, 294. PHISHING, 295. SPAM, 296. WLAN, 297. SERVER, 298. CHL, 299. PATCH, 300. PASSWORD, 301. PHISHING, 302. SPAM, 303. WLAN, 304. SERVER, 305. CHL, 306. PATCH, 307. PASSWORD, 308. PHISHING, 309. SPAM, 310. WLAN, 311. SERVER, 312. CHL, 313. PATCH, 314. PASSWORD, 315. PHISHING, 316. SPAM, 317. WLAN, 318. SERVER, 319. CHL, 320. PATCH, 321. PASSWORD, 322. PHISHING, 323. SPAM, 324. WLAN, 325. SERVER, 326. CHL, 327. PATCH, 328. PASSWORD, 329. PHISHING, 330. SPAM, 331. WLAN, 332. SERVER, 333. CHL, 334. PATCH, 335. PASSWORD, 336. PHISHING, 337. SPAM, 338. WLAN, 339. SERVER, 340. CHL, 341. PATCH, 342. PASSWORD, 343. PHISHING, 344. SPAM, 345. WLAN, 346. SERVER, 347. CHL, 348. PATCH, 349. PASSWORD, 350. PHISHING, 351. SPAM, 352. WLAN, 353. SERVER, 354. CHL, 355. PATCH, 356. PASSWORD, 357. PHISHING, 358. SPAM, 359. WLAN, 360. SERVER, 361. CHL, 362. PATCH, 363. PASSWORD, 364. PHISHING, 365. SPAM, 366. WLAN, 367. SERVER, 368. CHL, 369. PATCH, 370. PASSWORD, 371. PHISHING, 372. SPAM, 373. WLAN, 374. SERVER, 375. CHL, 376. PATCH, 377. PASSWORD, 378. PHISHING, 379. SPAM, 380. WLAN, 381. SERVER, 382. CHL, 383. PATCH, 384. PASSWORD, 385. PHISHING, 386. SPAM, 387. WLAN, 388. SERVER, 389. CHL, 390. PATCH, 391. PASSWORD, 392. PHISHING, 393. SPAM, 394. WLAN, 395. SERVER, 396. CHL, 397. PATCH, 398. PASSWORD, 399. PHISHING, 400. SPAM, 401. WLAN, 402. SERVER, 403. CHL, 404. PATCH, 405. PASSWORD, 406. PHISHING, 407. SPAM, 408. WLAN, 409. SERVER, 410. CHL, 411. PATCH, 412. PASSWORD, 413. PHISHING, 414. SPAM, 415. WLAN, 416. SERVER, 417. CHL, 418. PATCH, 419. PASSWORD, 420. PHISHING, 421. SPAM, 422. WLAN, 423. SERVER, 424. CHL, 425. PATCH, 426. PASSWORD, 427. PHISHING, 428. SPAM, 429. WLAN, 430. SERVER, 431. CHL, 432. PATCH, 433. PASSWORD, 434. PHISHING, 435. SPAM, 436. WLAN, 437. SERVER, 438. CHL, 439. PATCH, 440. PASSWORD, 441. PHISHING, 442. SPAM, 443. WLAN, 444. SERVER, 445. CHL, 446. PATCH, 447. PASSWORD, 448. PHISHING, 449. SPAM, 450. WLAN, 451. SERVER, 452. CHL, 453. PATCH, 454. PASSWORD, 455. PHISHING, 456. SPAM, 457. WLAN, 458. SERVER, 459. CHL, 460. PATCH, 461. PASSWORD, 462. PHISHING, 463. SPAM, 464. WLAN, 465. SERVER, 466. CHL, 467. PATCH, 468. PASSWORD, 469. PHISHING, 470. SPAM, 471. WLAN, 472. SERVER, 473. CHL, 474. PATCH, 475. PASSWORD, 476. PHISHING, 477. SPAM, 478. WLAN, 479. SERVER, 480. CHL, 481. PATCH, 482. PASSWORD, 483. PHISHING, 484. SPAM, 485. WLAN, 486. SERVER, 487. CHL, 488. PATCH, 489. PASSWORD, 490. PHISHING, 491. SPAM, 492. WLAN, 493. SERVER, 494. CHL, 495. PATCH, 496. PASSWORD, 497. PHISHING, 498. SPAM, 499. WLAN, 500. SERVER, 501. CHL, 502. PATCH, 503. PASSWORD, 504. PHISHING, 505. SPAM, 506. WLAN, 507. SERVER, 508. CHL, 509. PATCH, 510. PASSWORD, 511. PHISHING, 512. SPAM, 513. WLAN, 514. SERVER, 515. CHL, 516. PATCH, 517. PASSWORD, 518. PHISHING, 519. SPAM, 520. WLAN, 521. SERVER, 522. CHL, 523. PATCH, 524. PASSWORD, 525. PHISHING, 526. SPAM, 527. WLAN, 528. SERVER, 529. CHL, 530. PATCH, 531. PASSWORD, 532. PHISHING, 533. SPAM, 534. WLAN, 535. SERVER, 536. CHL, 537. PATCH, 538. PASSWORD, 539. PHISHING, 540. SPAM, 541. WLAN, 542. SERVER, 543. CHL, 544. PATCH, 545. PASSWORD, 546. PHISHING, 547. SPAM, 548. WLAN, 549. SERVER, 550. CHL, 551. PATCH, 552. PASSWORD, 553. PHISHING, 554. SPAM, 555. WLAN, 556. SERVER, 557. CHL, 558. PATCH, 559. PASSWORD, 560. PHISHING, 561. SPAM, 562. WLAN, 563. SERVER, 564. CHL, 565. PATCH, 566. PASSWORD, 567. PHISHING, 568. SPAM, 569. WLAN, 570. SERVER, 571. CHL, 572. PATCH, 573. PASSWORD, 574. PHISHING, 575. SPAM, 576. WLAN, 577. SERVER, 578. CHL, 579. PATCH, 580. PASSWORD, 581. PHISHING, 582. SPAM, 583. WLAN, 584. SERVER, 585. CHL, 586. PATCH, 587. PASSWORD, 588. PHISHING, 589. SPAM, 590. WLAN, 591. SERVER, 592. CHL, 593. PATCH, 594. PASSWORD, 595. PHISHING, 596. SPAM, 597. WLAN, 598. SERVER, 599. CHL, 600. PATCH, 601. PASSWORD, 602. PHISHING, 603. SPAM, 604. WLAN, 605. SERVER, 606. CHL, 607. PATCH, 608. PASSWORD, 609. PHISHING, 610. SPAM, 611. WLAN, 612. SERVER, 613. CHL, 614. PATCH, 615. PASSWORD, 616. PHISHING, 617. SPAM, 618. WLAN, 619. SERVER, 620. CHL, 621. PATCH, 622. PASSWORD, 623. PHISHING, 624. SPAM, 625. WLAN, 626. SERVER, 627. CHL, 628. PATCH, 629. PASSWORD, 630. PHISHING, 631. SPAM, 632. WLAN, 633. SERVER, 634. CHL, 635. PATCH, 636. PASSWORD, 637. PHISHING, 638. SPAM, 639. WLAN, 640. SERVER, 641. CHL, 642. PATCH, 643. PASSWORD, 644. PHISHING, 645. SPAM, 646. WLAN, 647. SERVER, 648. CHL, 649. PATCH, 650. PASSWORD, 651. PHISHING, 652. SPAM, 653. WLAN, 654. SERVER, 655. CHL, 656. PATCH, 657. PASSWORD, 658. PHISHING, 659. SPAM, 660. WLAN, 661. SERVER, 662. CHL, 663. PATCH, 664. PASSWORD, 665. PHISHING, 666. SPAM, 667. WLAN, 668. SERVER, 669. CHL, 670. PATCH, 671. PASSWORD, 672. PHISHING, 673. SPAM, 674. WLAN, 675. SERVER, 676. CHL, 677. PATCH, 678. PASSWORD, 679. PHISHING, 680. SPAM, 681. WLAN, 682. SERVER, 683. CHL, 684. PATCH, 685. PASSWORD, 686. PHISHING, 687. SPAM, 688. WLAN, 689. SERVER, 690. CHL, 691. PATCH, 692. PASSWORD, 693. PHISHING, 694. SPAM, 695. WLAN, 696. SERVER, 697. CHL, 698. PATCH, 699. PASSWORD, 700. PHISHING, 701. SPAM, 702. WLAN, 703. SERVER, 704. CHL, 705. PATCH, 706. PASSWORD, 707. PHISHING, 708. SPAM, 709. WLAN, 710. SERVER, 711. CHL, 712. PATCH, 713. PASSWORD, 714. PHISHING, 715. SPAM, 716. WLAN, 717. SERVER, 718. CHL, 719. PATCH, 720. PASSWORD, 721. PHISHING, 722. SPAM, 723. WLAN, 724. SERVER, 725. CHL, 726. PATCH, 727. PASSWORD, 728. PHISHING, 729. SPAM, 730. WLAN, 731. SERVER, 732. CHL, 733. PATCH, 734. PASSWORD, 735. PHISHING, 736. SPAM, 737. WLAN, 738. SERVER, 739. CHL, 740. PATCH, 741. PASSWORD, 742. PHISHING, 743. SPAM, 744. WLAN, 745. SERVER, 746. CHL, 747. PATCH, 748. PASSWORD, 749. PHISHING, 750. SPAM, 751. WLAN, 752. SERVER, 753. CHL, 754. PATCH, 755. PASSWORD, 756. PHISHING, 757. SPAM, 758. WLAN, 759. SERVER, 760. CHL, 761. PATCH, 762. PASSWORD, 763. PHISHING, 764. SPAM, 765. WLAN, 766. SERVER, 767. CHL, 768. PATCH, 769. PASSWORD, 770. PHISHING, 771. SPAM, 772. WLAN, 773. SERVER, 774. CHL, 775. PATCH, 776. PASSWORD, 777. PHISHING, 778. SPAM, 779. WLAN, 780. SERVER, 781. CHL, 782. PATCH, 783. PASSWORD, 784. PHISHING, 785. SPAM, 786. WLAN, 787. SERVER, 788. CHL, 789. PATCH, 790. PASSWORD, 791. PHISHING, 792. SPAM, 793. WLAN, 794. SERVER, 795. CHL, 796. PATCH, 797. PASSWORD, 798. PHISHING, 799. SPAM, 800. WLAN, 801. SERVER, 802. CHL, 803. PATCH, 804. PASSWORD, 805. PHISHING, 806. SPAM, 807. WLAN, 808. SERVER, 809. CHL, 810. PATCH, 811. PASSWORD, 812. PHISHING, 813. SPAM, 814. WLAN, 815. SERVER, 816. CHL, 817. PATCH, 818. PASSWORD, 819. PHISHING, 820. SPAM, 821. WLAN, 822. SERVER, 823. CHL, 824. PATCH, 825. PASSWORD, 826. PHISHING, 827. SPAM, 828. WLAN, 829. SERVER, 830. CHL, 831. PATCH, 832. PASSWORD, 833. PHISHING, 834. SPAM, 835. WLAN, 836. SERVER, 837. CHL, 838. PATCH, 839. PASSWORD, 840. PHISHING, 841. SPAM, 842. WLAN, 843. SERVER, 844. CHL, 845. PATCH, 846. PASSWORD, 847. PHISHING, 848. SPAM, 849. WLAN, 850. SERVER, 851. CHL, 852. PATCH, 853. PASSWORD, 854. PHISHING, 855. SPAM, 856. WLAN, 857. SERVER, 858. CHL, 859. PATCH, 860. PASSWORD, 861. PHISHING, 862. SPAM, 863. WLAN, 864. SERVER, 865. CHL, 866. PATCH, 867. PASSWORD, 868. PHISHING, 869. SPAM, 870. WLAN, 871. SERVER, 872. CHL, 873. PATCH, 874. PASSWORD, 875. PHISHING, 876. SPAM, 877. WLAN, 878. SERVER, 879. CHL, 880. PATCH, 881. PASSWORD, 882. PHISHING, 883. SPAM, 884. WLAN, 885. SERVER, 886. CHL, 887. PATCH, 888. PASSWORD, 889. PHISHING, 890. SPAM, 891. WLAN, 892. SERVER, 893. CHL, 894. PATCH, 895. PASSWORD, 896. PHISHING, 897. SPAM, 898. WLAN, 899. SERVER, 900. CHL, 901. PATCH, 902. PASSWORD, 903. PHISHING, 904. SPAM, 905. WLAN, 906. SERVER, 907. CHL, 908. PATCH, 909. PASSWORD, 910. PHISHING, 911. SPAM, 912. WLAN, 913. SERVER, 914. CHL, 915. PATCH, 916. PASSWORD, 917. PHISHING, 918. SPAM, 919. WLAN, 920. SERVER, 921. CHL, 922. PATCH, 923. PASSWORD, 924. PHISHING, 925. SPAM, 926. WLAN, 927. SERVER, 928. CHL, 929. PATCH, 930. PASSWORD, 931. PHISHING, 932. SPAM, 933. WLAN, 934. SERVER, 935. CHL, 936. PATCH, 937. PASSWORD, 938. PHISHING, 939. SPAM, 940. WLAN, 941. SERVER, 942. CHL, 943. PATCH, 944. PASSWORD, 945. PHISHING, 946. SPAM, 947. WLAN, 948. SERVER, 949. CHL, 950. PATCH, 951. PASSWORD, 952. PHISHING, 953. SPAM, 954. WLAN, 955. SERVER, 956. CHL, 957. PATCH, 958. PASSWORD, 959. PHISHING, 960. SPAM, 961. WLAN, 962. SERVER, 963. CHL, 964. PATCH, 965. PASSWORD, 966. PHISHING, 967. SPAM, 968. WLAN, 969. SERVER, 970. CHL, 971. PATCH, 972. PASSWORD, 973. PHISHING, 974. SPAM, 975. WLAN, 976. SERVER, 977. CHL, 978. PATCH, 979. PASSWORD, 980. PHISHING, 981. SPAM, 982. WLAN, 983. SERVER, 984. CHL, 985. PATCH, 986. PASSWORD, 987. PHISHING, 988. SPAM, 989. WLAN, 990. SERVER, 991. CHL, 992. PATCH, 993. PASSWORD, 994. PHISHING, 995. SPAM, 996. WLAN, 997. SERVER, 998. CHL, 999. PATCH, 1000. PASSWORD, 1001. PHISHING, 1002. SPAM, 1003. WLAN, 1004. SERVER, 1005. CHL, 1006. PATCH, 1007. PASSWORD, 1008. PHISHING, 1009. SPAM, 1010. WLAN, 1011. SERVER, 1012. CHL, 1013. PATCH, 1014. PASSWORD, 1015. PHISHING, 1016. SPAM, 1017. WLAN, 1018. SERVER, 1019. CHL, 1020. PATCH, 1021. PASSWORD, 1022. PHISHING, 1023. SPAM, 1024. WLAN, 1025. SERVER, 1026. CHL, 1027. PATCH, 1028. PASSWORD, 1029. PHISHING, 1030. SPAM, 1031. WLAN, 1032. SERVER, 1033. CHL, 1034. PATCH, 1035. PASSWORD, 1036. PHISHING, 1037. SPAM, 1038. WLAN, 1039. SERVER, 1040. CHL, 1041. PATCH, 1042. PASSWORD, 1043. PHISHING, 1044. SPAM, 1045. WLAN, 1046. SERVER, 1047. CHL, 1048. PATCH, 1049. PASSWORD, 1050. PHISHING, 1051. SPAM, 1052. WLAN, 1053. SERVER, 1054. CHL, 1055. PATCH, 1056. PASSWORD, 1057. PHISHING, 1058. SPAM, 1059. WLAN, 1060. SERVER, 1061. CHL, 1062. PATCH, 1063. PASSWORD, 1064. PHISHING, 1065. SPAM, 1066. WLAN, 1067. SERVER, 1068. CHL, 1069. PATCH, 1070. PASSWORD, 1071. PHISHING, 1072. SPAM, 1073. WLAN, 1074. SERVER, 1075. CHL, 1076. PATCH, 1077. PASSWORD, 1078. PHISHING, 1079. SPAM, 1080. WLAN, 1081. SERVER, 1082. CHL, 1083. PATCH, 1084. PASSWORD, 1085. PHISHING, 1086. SPAM, 1087. WLAN, 1088. SERVER, 1089. CHL, 1090. PATCH, 1091. PASSWORD, 1092. PHISHING, 1093. SPAM, 1094. WLAN, 1095. SERVER, 1096. CHL, 1097. PATCH, 1098. PASSWORD, 1099. PHISHING, 1100. SPAM, 1101. WLAN, 1102. SERVER, 1103. CHL, 1104. PATCH, 1105. PASSWORD, 1106. PHISHING, 1107. SPAM, 1108. WLAN, 1109. SERVER, 1110. CHL, 1111. PATCH, 1112. PASSWORD, 1113. PHISHING, 1114. SPAM, 1115. WLAN, 1116. SERVER, 1117. CHL, 1118. PATCH, 1119. PASSWORD, 1120. PHISHING, 1121. SPAM, 1122. WLAN, 1123. SERVER, 1124. CHL, 1125. PATCH, 1126. PASSWORD, 1127. PHISHING, 1128. SPAM, 1129. WLAN, 1130. SERVER, 1131. CHL, 1132. PATCH, 1133. PASSWORD, 1134. PHISHING, 1135. SPAM, 1136. WLAN, 1137. SERVER, 1138. CHL, 1139. PATCH, 1140. PASSWORD, 1141. PHISHING, 1142. SPAM, 1143. WLAN, 1144. SERVER, 1145. CHL, 1146. PATCH, 1147. PASSWORD, 1148. PHISHING, 1149. SPAM, 1150. WLAN, 1151. SERVER, 1152. CHL, 1153. PATCH, 1154. PASSWORD, 1155. PHISHING, 1156. SPAM, 1157. WLAN, 1158. SERVER, 1159. CHL, 1160. PATCH, 1161. PASSWORD, 1162. PHISHING, 1163. SPAM, 1164. WLAN, 1165. SERVER, 1166. CHL, 1167. PATCH, 1168. PASSWORD, 1169. PHISHING, 1170. SPAM, 1171. WLAN, 1172. SERVER, 1173. CHL, 1174. PATCH, 1175. PASSWORD, 1176. PHISHING, 1177. SPAM, 1178. WLAN, 1179. SERVER, 1180. CHL, 1181. PATCH, 1182. PASSWORD, 1183. PHISHING, 1184. SPAM, 1185. WLAN, 1186. SERVER, 1187. CHL, 1188. PATCH, 1189. PASSWORD, 1190. PHISHING, 1191. SPAM, 1192. WLAN, 1193. SERVER, 1194. CHL, 1195. PATCH, 1196. PASSWORD, 1197. PHISHING, 1198. SPAM, 1199. WLAN, 1200. SERVER, 1201. CHL, 1202. PATCH, 1203. PASSWORD, 1204. PHISHING, 1205. SPAM, 1206. WLAN, 1207. SERVER, 1208. CHL, 1209. PATCH, 1210. PASSWORD, 1211. PHISHING, 1212. SPAM, 1213. WLAN, 1214. SERVER, 1215. CHL, 1216. PATCH, 1217. PASSWORD, 1218. PHISHING, 1219. SPAM, 1220. WLAN, 1221. SERVER, 1222. CHL, 1223. PATCH, 1224. PASSWORD, 1225. PHISHING, 1226. SPAM, 1227. WLAN, 1228. SERVER, 1229. CHL, 1230. PATCH, 1231. PASSWORD, 1232. PHISHING, 1233. SPAM, 1234. WLAN, 1235. SERVER, 1236. CHL, 1237. PATCH, 1238. PASSWORD, 1239. PHISHING, 1240. SPAM, 1241. WLAN, 1242. SERVER, 1243. CHL, 1244. PATCH, 1245. PASSWORD, 1246. PHISHING, 1247. SPAM, 1248. WLAN, 1249. SERVER, 1250. CHL, 1251. PATCH, 1252. PASSWORD, 1253. PHISHING, 1254. SPAM, 1255. WLAN, 1256. SERVER, 1257. CHL, 1258. PATCH, 1259. PASSWORD, 1260. PHISHING, 1261. SPAM, 1262. WLAN, 1263. SERVER, 1264. CHL, 1265. PATCH, 1266. PASSWORD, 1267. PHISHING, 1268. SPAM, 1269. WLAN, 1270. SERVER, 1271. CHL, 1272. PATCH, 1273. PASSWORD, 1274. PHISHING, 1275. SPAM, 1276. WLAN, 1277. SERVER, 1278. CHL, 1279. PATCH, 1280. PASSWORD, 1281. PHISHING, 1282. SPAM, 1283. WLAN, 1284. SERVER, 1285. CHL, 1286. PATCH, 1287. PASSWORD, 1288. PHISHING, 1289. SPAM, 1290. WLAN, 1291. SERVER, 1292. CHL, 1293. PATCH, 1294. PASSWORD, 1295. PHISHING, 1296. SPAM, 1297. WLAN, 1298. SERVER, 1299. CHL, 1300. PATCH, 1301. PASSWORD, 1302. PHISHING, 1303. SPAM, 1304. WLAN, 1305. SERVER, 1306. CHL, 1307. PATCH, 1308. PASSWORD, 1309. PHISHING, 1310. SPAM, 1311. WLAN, 1312. SERVER, 1313. CHL, 1314. PATCH, 1315. PASSWORD, 1316. PHISHING, 1317. SPAM, 1318. WLAN, 1319. SERVER, 1320. CHL, 1321. PATCH, 1322. PASSWORD, 1323. PHISHING, 1324. SPAM, 1325. WLAN, 1326. SERVER, 1327. CHL, 1328. PATCH, 1329. PASSWORD, 1330. PHISHING, 1331. SPAM, 1332. WLAN, 1333. SERVER, 1334. CHL, 1335. PATCH, 1336. PASSWORD, 1337. PHISHING, 1338. SPAM, 1339. WLAN, 1340. SERVER, 1341. CHL, 1342. PATCH, 1343. PASSWORD, 1344. PHISHING, 1345. SPAM, 1346. WLAN, 1347. SERVER, 1348. CHL, 1349. PATCH, 1350. PASSWORD, 1351. PHISHING, 1352. SPAM, 1353. WLAN, 1354. SERVER, 1355. CHL, 1356. PATCH, 1357. PASSWORD, 1358. PHISHING, 1359. SPAM, 1360. WLAN, 1361. SERVER, 1362. CHL, 1363. PATCH, 1364. PASSWORD, 1365. PHISHING, 1366. SPAM, 1367. WLAN, 1368. SERVER, 1369. CHL, 1370. PATCH, 1371. PASSWORD, 1372. PHISHING, 1373. SPAM, 1374. WLAN, 1375. SERVER, 1376. CHL, 1377. PATCH, 1378. PASSWORD, 1379. PHISHING, 1380. SPAM, 1381. WLAN, 1382. SERVER, 1383. CHL, 1384. PATCH, 1385. PASSWORD, 1386. PHISHING, 1387. SPAM, 1388. WLAN, 1389. SERVER, 1390. CHL, 1391. PATCH, 1392. PASSWORD, 1393. PHISHING, 1394. SPAM, 1395. WLAN, 1396. SERVER, 1397. CHL, 1398. PATCH, 1399. PASSWORD, 1400. PHISHING, 1401. SPAM, 1402. WLAN, 1403. SERVER, 1404. CHL, 1405. PATCH, 1406. PASSWORD, 1407. PHISHING, 1408. SPAM, 1409. WLAN, 1410. SERVER, 1411. CHL, 1412. PATCH, 1413. PASSWORD, 1414. PHISHING, 1415. SPAM, 1416. WLAN, 1417. SERVER, 1418. CHL, 1419. PATCH, 1420. PASSWORD, 1421. PHISHING, 1422. SPAM, 1423. WLAN, 1424. SERVER, 1425. CHL, 1426. PATCH, 1427. PASSWORD, 1428. PHISHING, 1429. SPAM, 1430. WLAN, 1431. SERVER, 1432. CHL, 1433. PATCH, 1434. PASSWORD, 1435. PHISHING, 1436. SPAM, 1437. WLAN, 1438. SERVER, 1439. CHL, 1440. PATCH, 1441. PASSWORD, 1442. PHISHING, 1443. SPAM, 1444. WLAN, 1445. SERVER, 1446. CHL, 1447. PATCH, 1448. PASSWORD, 1449. PHISHING, 1450. SPAM, 1451. WLAN, 1452. SERVER, 1453. CHL, 1454. PATCH, 1455. PASSWORD, 1456. PHISHING, 1457. SPAM, 1458. WLAN, 1459. SERVER, 1460. CHL, 1461. PATCH, 1462. PASSWORD, 1463. PHISHING, 1464. SPAM, 1465. WLAN, 1466. SERVER, 1467. CHL, 1468. PATCH, 1469. PASSWORD, 1470. PHISHING, 1471. SPAM, 1472. WLAN, 1473. SERVER, 1474. CHL, 1475. PATCH, 1476. PASSWORD, 1477. PHISHING, 1478. SPAM, 1479. WLAN, 1480. SERVER, 1481. CHL, 1482. PATCH, 1483. PASSWORD, 1484. PHISHING, 1485. SPAM, 1486. WLAN, 1487. SERVER, 1488. CHL, 1489. PATCH, 1490. PASSWORD, 1491. PHISHING, 1492. SPAM, 1493. WLAN, 1494. SERVER, 1495. CHL, 1496. PATCH, 1497. PASSWORD, 1498. PHISHING, 1499. SPAM, 1500. WLAN, 1501. SERVER, 1502. CHL, 1503. PATCH, 1504. PASSWORD, 1505. PHISHING, 1506. SPAM, 1507. WLAN, 1508. SERVER, 1509. CHL, 1510. PATCH, 1511. PASSWORD, 1512. PHISHING, 1513. SPAM, 1514. WLAN, 1515. SERVER, 1516. CHL, 1517. PATCH, 1518. PASSWORD, 1519. PHISHING, 1520. SPAM, 1521. WLAN, 1522. SERVER, 1523. CHL, 1524. PATCH, 1525. PASSWORD, 1526. PHISHING, 1527. SPAM, 1528. WLAN, 1529. SERVER, 1530. CHL, 1531. PATCH, 1532. PASSWORD, 1533. PHISHING, 1534. SPAM, 1535. WLAN, 1536. SERVER, 1537. CHL, 1538. PATCH, 1539. PASSWORD, 1540. PHISHING, 154

Weitere Maßnahmen zur Internetsicherheit

- Laden Sie Programme nur aus sicherer Quelle auf Ihre Geräte. Für Smartphones sind sichere Quellen der App- oder Play-Store, je nach Betriebssystem. Am PC laden Sie ein Programm am sichersten direkt von der Herstellerseite.
- Passwörter knacken wird durch Ausprobieren realisiert. Vermeiden Sie Passwörter, die in Wörterbüchern stehen, sowie Namen, Jahresdaten und Zeichenfolgen.
- Sicher sind Passwörter, die aus mehreren Wörtern ohne Zusammenhang zueinander oder Account bestehen oder Passwörter, die sich aus einem Passwortsatz bilden.
- Beispiel: Pferd_Tastatur_3_Tannenbaum
- Beispiel: Meine Oma radelt jeden Samstag um 19 Uhr zum BayernLab und zurück -> Morj\$u19UzB&z
- Passwörter aufschreiben und sicher verwahren ist unter anderem für den Erbfall empfehlenswert. Passwortmanager können Ihre Passwörter verwalten und Sie brauchen sich nur das Masterpasswort merken. Wechseln Sie Passwörter nur nach unsicheren Situationen wie Log-In in einem öffentlichen WLAN. Denken Sie über 2-Faktor-Authentifizierung für besondere Sicherheit nach.
- Phishing richtet sich nicht gezielt gegen Sie, aber Sie sind immer ein lukratives Ziel. Betrüger werden versuchen, Sie durch zeitlichen Druck und Angst vor Konsequenzen zu unüberlegtem Handeln zu drängen. Banken, Ärzte, Anwälte und alle, die hochsensiblen Daten von Ihnen verwalten, werden nicht per E-Mail mit Ihnen kommunizieren.
- Überprüfen Sie die Absenderadresse (Achtung, kann auch gefälscht sein), Betreff, Links und Anhänge, bevor Sie eine Mail oder Links und Anhänge öffnen. Ein Link sollte das Format (...)Name der Seite.Länderkennung/(...) haben. Die Platzhalter können dabei beliebig sein. Öffnen Sie keine .exe-Dateien in Anhängen.
- Unter www.bsi.bund.de – der Internetseite des Bundesinstituts für Sicherheit in der Informationstechnik – können Sie sich über Maßnahmen zur Internetsicherheit informieren.

Kinder und das Internet

- Ab dem Alter von 12 Jahren sind praktisch alle Kinder im Internet unterwegs. Regelmäßige Statistiken zum Medienumgang mit Kindern und Jugendliche werden durch den Medienpädagogischen Forschungsverband Südwest – www.mpfs.de – erhoben. Es wird dabei zwischen den Altersstufen 2-5 Jahre, 6-13 Jahre und 12-19 Jahre unterschieden.
- Pauschale Empfehlungen, wann ein Kind wie viel Umgang mit digitalen Medien haben sollte, gibt es nicht. Besondere Vorsicht ist geboten, wenn Kinder noch nicht zwischen Realität und Medien unterscheiden können (bis ca. 3 Jahre) oder noch keine ausreichende Distanz zu dem Gesehenen aufbauen können (bis ca. 6 Jahre). Danach geht es je nach Entwicklungsstand darum, wie ein Kind Umgang und Gefahren der Mediennutzung einschätzen kann. Dabei braucht es weiterhin Beratung und Unterstützung. Erwachsene dienen als Vorbilder.
 - Anhaltspunkte finden Sie unter frühe Kindheit und Medien bei www.mpfs.de, Medienerziehung bei www.klicksafe.de oder Bildschirmzeiten bei www.schau-hin.info
 - Eine Seite, auf der Kinder Mediennutzung lernen können ist beispielsweise www.internet-abc.de.
- Als besondere Privatsphäre-Einstellungen sollten Berechtigungen von Apps überprüft werden, ggfs. weitere Einstellungen in den Apps vorgenommen werden und nicht gebrauchte Apps deinstalliert werden. Käufe und Zahlungen sollten mit Passwort geschützt werden und (Bildschirm-)Sperrungen so gewählt werden, dass sie schwer nachzumachen sind.
 - Anleitungen zu Privatsphäre Einstellungen für Geräte und Apps unter www.meiden-kindersicher.de
- Spezielle Kindersuchmaschinen schulen den Umgang mit dem Internet. Meist werden nur geprüfte Seiten zugelassen. Die Nützlichkeit der Suchergebnisse hängt von der redaktionellen Arbeit ab, wie viele kinderfreundliche Seiten freigeschaltet werden.
 - Beispiele sind www.fragfinn.de und www.helles-koepfchen.de

Typische Rechtsfragen

- Wenden Sie sich im Zweifel an Polizei, (Fach-)Anwälte oder Verbraucherschutzorganisationen
- Informationen über aktuelle Gefahren an Jugendliche gerichtet gibt es unter www.handysektor.de, an Erwachsene und Jugendliche unter www.klicksafe.de, www.saferinternet.de oder www.schau-hin.info
- Die Datenschutzgrundverordnung (DSGVO) ist seit 2016 geltendes EU-Recht zum Schutz des Grundrechts auf informationelle Selbstbestimmung. Sie schreibt unter anderem fest, dass Sie von einem Unternehmen oder einer Behörde Herausgabe oder Löschung Ihrer Daten verlangen können. Jeder nicht notwendigen Verarbeitung Ihrer Daten müssen Sie zustimmen.
 - Aktuelle Entwicklungen unter www.stiftungdatenschutz.org
- Es gibt verschiedene Sorten von Cookies, die für die Funktion der Seite zuständig sind, darf der Betreiber immer nutzen. Cookies zur Analyse der Beliebtheit der Seite oder Profilbildung für personalisierte Werbung sind nicht notwendig. Nach DSGVO muss man sie ablehnen können. Unternehmen und Verbraucherschützer streiten, ob das genauso einfach und kostenfrei sein muss wie die Zustimmung.
- Im Kunsturheberrecht ist geregelt, dass Bilder nur mit Einverständnis der darin erkennbaren Personen veröffentlicht werden dürfen. Erkennbar ist eine Person auch dann, wenn zwar nicht ihr Gesicht zu sehen ist, aber sonstige markante körperliche Merkmale. Bei Kindern unter 16 Jahren erfolgt die Zustimmung durch die Eltern. Ausnahme ist öffentliches Interesse oder wenn die Person Beiwerk auf einem Landschaftsbild ist. Achtung, auch Personen des öffentlichen Lebens haben ein Privatleben, dass sie gegeben falls rechtlich schützen.
- Das Urheberrecht schützt persönliche geistige Schöpfung, Bilder, Musik, Texte, auch Gebrauchsgegenstände mit gewissem schöpferischem Wert. Dabei hat der Urheber oder seine Erben immer das Recht der Namensnennung, Erstveröffentlichung und Schutz vor Entstellung des Werks. Rechte zur Nutzung wie der Bearbeitung, Verbreitung, Vervielfältigung, öffentlichen Wiedergabe, etc. kann er veräußern. Eine Nutzung ohne Einwilligung der Rechteinhaber kann rechtlich verfolgt werden.
- Jugendgefährdende Inhalte im Netz können sowohl Straftaten an Kindern sein, als auch Anstiftung zu Straftaten durch Kinder, die online oder im echten Leben ausgeführt werden. Die häufigsten Kategorien sind körperliche oder psychische Gewalt, sexualisierte Gewalt und Extremismus, vor allem Rechtsextremismus und Islamismus. Unter körperliche Gewalt fallen auch so genannte Challenges, Mutproben, die sich online verbreiten und teilweise gefährliche Tätigkeiten verlangen, oder Mobbing. Die Anbahnung gefährdender Kontakte erfolgt durch harmlos erscheinende Interaktionen, die ein Gefühl von Zugehörigkeit oder Wertschätzung hervorgerufen. Eine Eskalation erfolgt stufenweise.
 - Weitere Informationen und eine Beschwerdestelle gibt es unter www.jugendschutz.net

Soziale Medien

- In Abgrenzung zu linearen Medien ist für soziale Medien wichtig, dass sie kommunikativ sind und dass alle Teilnehmer Inhalte konsumieren, aber auch veröffentlichen können. Anbieter stellen dabei die Plattform, Nutzer die Inhalte. Die Plattformen unterscheiden sich zwischen Instant Messengern, Sozialen Netzwerken, Videoplattformen, Blogs, Wikis, etc. Funktionelle Grenzen verschwimmen zunehmend, da viele Anbieter aktuellen Kommunikationstrends folgen wollen.
- Bei Instant Messengern liegt der Fokus auf direkter Kommunikation. Diese erfolgt in 1-zu-1-Chats oder Gruppenchats. Auch Mediendateien können darüber versandt werden. Viele Messenger sind mit Zusatzfunktionen ausgestattet wie (Video-)Anrufen, Statusmeldungen oder Kanälen

Messenger

Messenger	Ende-zu-Ende-Verschlüsselung	Metadaten	Offener Quellcode	Anmerkungen
	Der Nachrichteninhalt ist von Absender bis Empfänger verschlüsselt, auch bei Lagerung beim Anbieter.	Daten über die Nachricht wie Größe, Uhrzeit, Ort etc. fallen an und werden gespeichert.	Dritte können überprüfen, ob der Code sicher vor Angriffen ist und was gespeichert wird.	
Whatsapp	immer	viele	nein	gehört zu Meta
Telegram	nicht standardmäßig, nie in Gruppen	viele	nein	
Signal	immer	wenige	ja	Sitz in USA
Facebook Messenger	nicht standardmäßig	viele	nein	
Threema	immer	kaum bis keine	nein	kostenpflichtig, Sitz in der Schweiz

BayernLab Dillingen

- Die Möglichkeit selbstlöschender Nachrichten bietet ein trügerisches Gefühl von Sicherheit. Empfänger können immer durch Abfilmen des Bildschirms oder Bildschirmaufnahmen das Gesehene speichern. Kommt dies wie beim Anbieter Snapchat mit fehlender Ende-zu-Ende-Verschlüsselung zusammen, kann es schnell zur Verbreitung persönlicher Inhalte kommen. Unverschlüsselte Plattformen sollten daher grundsätzlich wie öffentliche Plätze behandelt werden.
- Auf Medienplattformen geht es in erster Linie um das Veröffentlichen, Teilen und Konsumieren von Inhalten (Content). Beispiele sind Instagram für Bilder und Videos, Tik Tok für Kurzvideos, Youtube für Lang- und Kurzvideos, auch live, Twitch für Video-Liveübertragungen, X (ehemals Twitter) oder Bluesky für Kurznachrichten.
 - Kurzgefasste Allgemeine Geschäftsbedingungen vieler Seiten gibt es auf www.handysektor.de
- Plattformbetreiber nutzen Formeln (Algorithmen) zur Berechnung, welche Inhalte Nutzer als nächstes zu sehen bekommen. Sie werten dabei aus, wie Nutzer mit Inhalten der Plattform interagieren. Die Algorithmen folgen wirtschaftlichen und politischen Interessen der Plattformbetreiber. Sie streben danach, Nutzer an die Plattform zu binden, wobei die Ablehnung zu höherer Interaktion führt als Zustimmung. Nutzer können durch gezielte Steuerung, welchen Inhalten sie Aufmerksamkeit schenken, bestimmen, wie gut oder schlecht der Umgang ihrer psychischen Gesundheit tut.

7. Veranstaltung: „Mikrotransaktionen – In-App-Käufe & andere Verkaufsstrategien der Spieleindustrie“ (04.02.2025) mit Kilian Modl, BayernLab Dillingen

In-App-Käufe:

Hierbei handelt es sich um zusätzliche Inhalte oder Abonnements, die in einer App gekauft werden. Es gibt drei Arten von In-App-Käufen:

Abonnement (Zahlung für Zugriff auf Inhalte in einer App während eines bestimmten Zeitraums, verlängert sich automatisch)

Nicht aufbrauchbarer In-App-Kauf (Entfernen von Werbung, Upgrade auf Pro-Version, Einmaliger Kauf häufig auf andere Geräte übertragbar)

Aufbrauchbarer In-App-Kauf (Spielwährung, nach Aufbrauchen der Inhalte, erneuter Kauf notwendig), häufig nicht übertragbar)

In-Game-Käufe:

Hierbei handelt es sich um eine Unterkategorie von In-App-Käufen. Diese werden während eines Spiels getätigt und sind meistens Spiel-Erweiterungen mit echtem Geld und werden über In-Game-Shops gekauft. Prominente Beispiele für In-Game-Käufe sind Mikrotransaktionen und Lootboxen.

Mikrotransaktionen sind kleine Online-Käufe, die in Videospielen, Social-Media und Apps angeboten werden. Hier werden virtuelle Gegenstände, Dienstleistungen oder Upgrades gekauft. Die Transaktionen finden meist innerhalb der Anwendung statt und werden über digitale Zahlungsmethoden abgewickelt (Kreditkarten, PayPal und virtuelle Geldbörsen).

Es gibt verschiedene Arten von Mikrotransaktionen:

Virtuelle Währungen (Kauf von virtuellen Währungen in einem Spiel um Gegenstände, Upgrades oder neue Level zu erwerben)

Gegenstände & Upgrades (Direkter Kauf von Gegenständen & Upgrades für eine Verbesserung der Spielerfahrung)

Zeitersparnis (Verkürzen der Wartezeit oder Freischaltung bestimmter Funktionen beschleunigen)

Abonnements (Abschließen von Abonnements für zusätzliche Vorteile wie z.B. exklusive Inhalte, Rabatte & Werbefreiheit)

Werbefreiheit (Kauf von Mikrotransaktionen um Anzeigen zu entfernen - für ein werbefreies Nutzererlebnis)

Lootboxen:

Hierbei handelt es sich um virtuelle Behälter oder (Beute-) Kisten in Videospielen. Diese enthalten zufällige Güter wie z.B. Waffe, Rüstung, kosmetische Items oder eine Klassifizierung nach Farben. Sie können freigeschaltet oder gekauft werden mit virtueller Währung oder echtem Geld und werden kontrovers diskutiert aufgrund von Suchtpotential und Glücksspielelementen. Ein generelles Verbot von Lootboxen auf EU-Ebene besteht nicht. Das Glücksspielrecht fällt in die Zuständigkeit der Mitgliedstaaten.

Auswirkungen auf Kinder & Jugendliche:

Finanzielle Auswirkungen:

Kauf von virtuellen Währungen führt schnell zu dem Gefühl, kein echtes Geld auszugeben. Das Verständnis für den Wert des Geldes & die langfristigen Kosten gehen verloren.

Suchtpotenzial:

Nervenkitzel des Zufalls bei Mikrotransaktionen & Lootboxen kann für erhöhtes Suchtpotential sorgen.

Großes Verlangen nach dem nächsten glücklichen Kauf

Ungleichgewicht im Spiel:

Spiele mit starkem Fokus auf In-Game-Käufe -> Ungleichgewicht innerhalb des Spiels

Einige Spieler sind bereit mehr Geld auszugeben mit dem Ziel einen Vorteil gegenüber anderen Spielern zu haben.

Unrealistische Erwartungen:

Entwicklung falscher Erwartungen mit Hinblick auf den Erwerb von In-Game-Käufen.

Ausgeben von Geld im Spiel führt zum Erhalt von Erfolgen & Belohnungen; Der Wert von Arbeit und Geduld im realen Leben wird unterschätzt.

Datenschutz & Online-Sicherheit:

In-Game-Käufe erfordern häufig Eingabe von Zahlungsinformationen. Dies kann zu potentiellen Datenschutz- und Sicherheitsrisiken führen.

Kinder und Jugendliche können sich in unsicheren Umgebungen wiederfinden -> Gefährdung persönlicher Daten.

Verantwortungsvoller Umgang mit In-Game-Käufen:**Offene Kommunikation:**

Mit Kindern & Jugendlichen über die Konzepte von virtuellen Käufen, Mikrotransaktionen & Lootboxen sprechen.

Funktionsweise dieser Systeme und mögliche Auswirkungen diskutieren.

Es sollten Regeln gemeinsam aufgestellt werden z.B. Wie viel Geld darf ausgegeben werden, wie oft dürfen Käufe getätigt werden, kein Kauf über Paypal oder Kreditkarten usw.

Kritische Betrachtung:

Kritisches Hinterfragen von Spielen und Apps, da nicht alles was dort beworben und angeboten wird ist notwendig. Es sollten Fähigkeiten angelernt werden um zwischen sinnvollen Inhalten und reinen Kaufanreizen zu unterscheiden.

Begrenzung der Bildschirmzeit:

Angemessene Begrenzung der Bildschirmzeit. Ausgewogenes Verhältnis zwischen Online- & Real-Life-Aktivitäten.

Aufklärung über Online-Sicherheit:

Themen wie Datenschutz, Online-Sicherheit, Risiken von Betrug & Missbrauch im Zusammenhang mit In-Game-Käufen ansprechen sowie aufklären.

Für eine bewusste und keine leichtfertige Weitergabe von persönlichen Informationen sensibilisieren.

Vorbildfunktion:

Dienen Sie selbst als Vorbild.

Zeigen Sie einen verantwortungsvollen Umgang mit In-Game/App-Käufen auf und treffen Sie selbst bewusste Kaufentscheidungen.



8.Veranstaltung: „Kryptowährung“ (09.04.2025, 14.05.2025 und 26.05.2025) mit Kilian Modl, BayernLab Dillingen

Was ist eine Kryptowährung?

Kryptowährungen sind digitale Zahlungsmittel, die auf kryptographischen Verfahren und einer dezentralen Infrastruktur – der sogenannten Blockchain – basieren. Im Gegensatz zu klassischen Währungen werden sie nicht von einer Zentralbank ausgegeben oder kontrolliert, sondern durch ein weltweites Netzwerk von Computern (Nodes) verwaltet. Diese Nodes speichern die Blockchain, validieren Transaktionen, nehmen neue Blöcke entgegen und sichern somit das gesamte System ab.

Chancen und Nutzen von Kryptowährungen

Kryptowährungen bieten zahlreiche Vorteile. Einer der größten Pluspunkte ist die Möglichkeit, weltweit innerhalb von Sekunden Geld zu transferieren – ohne klassische Bankinstitute. Nutzer sind dabei ihre eigene Bank: Sie verwalten ihre digitalen Vermögenswerte unabhängig von Dritten. Die Blockchain-Technologie sorgt zudem für hohe Transparenz: Jede Transaktion ist nachvollziehbar dokumentiert.

Ein weiterer wichtiger Aspekt sind die innovativen Anwendungen, die durch Plattformen wie Ethereum entstehen – z. B. sogenannte Smart Contracts. Diese intelligenten Verträge automatisieren Abläufe und könnten zahlreiche Branchen revolutionieren. Nicht zuletzt lockt viele das hohe Gewinnpotential, das sich aus der Volatilität der Kurse ergeben kann.

Risiken und Gefahren

Doch wo Chancen sind, gibt es auch Risiken. Der Kursverlauf vieler Kryptowährungen ist extrem schwankungsanfällig – das birgt ein hohes Verlustrisiko. Zusätzlich können Fehlbedienungen, technische Fehler oder Diebstahl zum Verlust des gesamten Guthabens führen. Anders als bei klassischen Bankkonten gibt es keine Einlagensicherung.

Ein weiteres Problem ist die fehlende staatliche Kontrolle. Dadurch können Kryptowährungen auch für illegale Zwecke – wie Geldwäsche oder Transaktionen im Darknet – missbraucht werden. Schließlich wirkt die technische Komplexität abschreckend auf viele Nutzer, besonders im Vergleich zum gewohnten Online-Banking.

Einblick in die Praxis: Kaufen und Verkaufen von Kryptowährungen

Um Kryptowährungen zu kaufen oder zu handeln, nutzen die meisten Menschen sogenannte Kryptobörsen. Diese Plattformen erlauben es, Fiatgeld (z. B. Euro) gegen Kryptowährungen zu tauschen. Dabei ist es entscheidend auf seriöse Anbieter zu setzen und grundlegende Sicherheitsregeln einzuhalten. Zu Anfang erst mit Demo-Guthaben handeln!

Vergleich von verschiedenen Kryptobörsen: <https://www.finanzfluss.de/vergleich/kryptoboersen/>

Sicherheit und Betrugsprävention

Obwohl Transaktionen in der Blockchain grundsätzlich sicher sind, liegt die Verantwortung für die Zugangsdaten allein beim Nutzer. Der wichtigste Punkt: Die private Zugangsinformation – der sogenannte „Private Key“ oder die „Seed Phrase“ – darf niemals in fremde Hände geraten.

Sicherheits-Tipps:

Starke Passwörter für Börsen-Accounts verwenden

Zwei-Faktor-Authentifizierung aktivieren - Backups der Wallet-Zugangsdaten offline an einem sicheren Ort speichern

Größere Beträge möglichst offline („Cold Wallet“) lagern

Besondere Vorsicht ist bei Betrugsmaschinen geboten. Häufige Szenarien:

Phishing-E-Mails, die täuschend echt aussehen und Passwörter abfragen

Gefälschte Investment-Angebote mit unrealistischen Gewinnversprechen

Schadsoftware, die Daten auf dem PC ausliest

Hier gilt: Misstrauen ist der beste Schutz. Niemals Zugangsdaten an Dritte weitergeben und bei Unsicherheit unabhängigen Rat einholen.

Rechtliche und steuerliche Aspekte in Deutschland

In Deutschland ist der Besitz und die Nutzung von Kryptowährungen legal. Sie gelten als sogenannte „Rechnungseinheiten“, jedoch nicht als gesetzliches Zahlungsmittel. Niemand ist verpflichtet, sie als Bezahlung zu akzeptieren.

Der Handel unterliegt in bestimmten Fällen der Aufsicht durch die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) insbesondere, wenn Anbieter als Finanzdienstleister auftreten. Zudem greifen EU-Regularien, etwa zur Bekämpfung von Geldwäsche und zur Kundenidentifikation.

Steuerliche Behandlung

Gewinne aus privaten Kryptowährungen unterliegen der Einkommensteuer, wenn sie innerhalb eines Jahres nach Erwerb veräußert werden. Dabei gilt:

- Haltefrist von 1 Jahr: Danach sind Gewinne steuerfrei
- Freigrenze von 600 €: Gewinne darunter bleiben steuerfrei
- Verluste können mit Gewinnen verrechnet werden

Die steuerliche Behandlung erfordert eine genaue Dokumentation der Käufe und Verkäufe – idealerweise mit Unterstützung spezialisierter Software oder Beratung.

