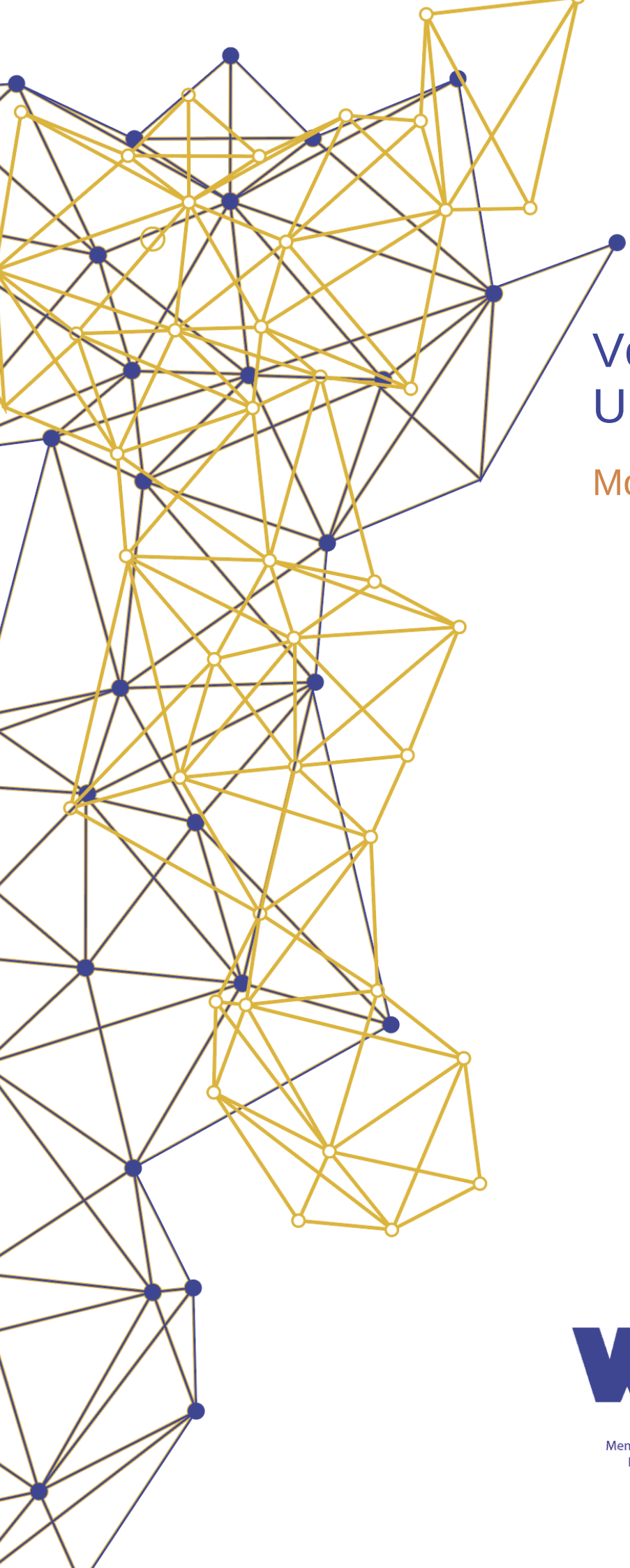
Vorlage für den Unterrichtsplan

Modul 6



WOWSA

What's on the Web Safe for All Family Members - A Family Learning Approach to Building Digital Literacy Competences

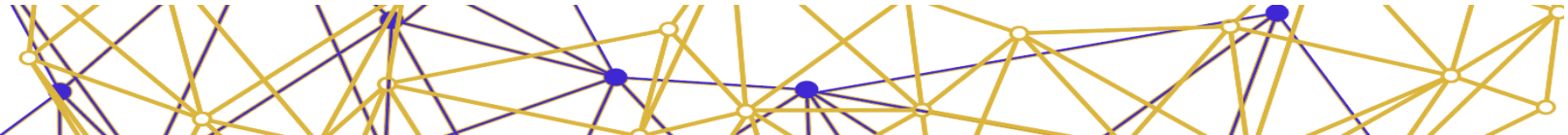
Stundenplan – Modul 6

Lernergebnisse

	WISSEN	FÄHIGKEITEN	HALTUNG
Modul 6: EXTERNE BEDROHUNGEN & PRIVATSPHÄRE-Einstellungen und elterliche Kontrolle in den Sozialen Medien	Definition des Konzepts der Informationsstörung (siehe Modul 3, Workshop 1).	Fähigkeit, die verschiedenen Arten von Informationen und die Formen, die sie annehmen können, zu erkennen (siehe Modul 3, Workshop 1).	Bewusstsein für die Bedeutung von Medienkompetenz, um eine aktive Haltung gegenüber dem Konsum und der Gestaltung von Medien einzunehmen.
	Verstehen, was ein „fake“ Konto ist. Den Unterschied zwischen „fake“ Konten, die von Menschen erstellt werden, und ihren Zielen und gefälschten Konten, die von Software erstellt werden, und ihren Zielen verstehen. Definition des Begriffs „scam“ (=Betrug) und seine Ziele. Definition der Hauptmerkmale eines „Scams“.	Fähigkeit zu erklären, was ein Fake-Account ist und was er bezweckt (Trolling, Satire, Betrug, Verbreitung von Fehlinformationen; einige Fake-Accounts werden von Bots betrieben und sind rund um die Uhr aktiv). Fähigkeit, zwischen einem von einem Bot betriebenen Fake-Account (und seinen Zielen), einem von einem Menschen betriebenen Fake-Account (und seinen Zielen) und einem Bot, der nicht mit einem Fake-Account verwechselt werden soll, zu unterscheiden. Die Fähigkeit zu erklären, was ein Scam ist, und einen Scam-Versuch zu erkennen, während man sich in digitalen Umgebungen bewegt.	Bewusstsein, dass Fake-Konten die Navigation in digitalen Umgebungen erschweren und gefährlich machen können. Erkennen, dass verschiedene Arten von Fake-Konten unterschiedliche Ziele verfolgen und dass es wichtig ist, sie voneinander unterscheiden zu können. Erkennen, dass Scam per Definition ein Versuch ist, jemanden mit einem (böswilligen) Endziel zu täuschen, z. B. Geld zu stehlen. Kritisches Denken und erworbenes Wissen einsetzen, um sich und seine

		Fähigkeit, einen Scam-Versuch anhand verschiedener Merkmale von Betrügereien zu erkennen (E-Mail-Adresse, unaufgeforderter oder unerwarteter Kontakt, zu schön, um wahr zu sein, Aufforderung zur Angabe persönlicher Daten, Aufforderung zu einer schnellen Entscheidung, Gewinnspiel).	Familie vor Betrügereien/Scams zu schützen.
	Definition des Begriffs „Identitätsdiebstahl“ und Auflistung der Möglichkeiten, wie Identitätsdiebe in den Besitz der persönlichen Daten einer Person gelangen können. Wissen, wie man persönliche Daten vor Identitätsdiebstahl schützen kann.	Fähigkeit, den Begriff des Identitätsdiebstahls zu erklären und die verschiedenen Möglichkeiten (Datenschutzverletzungen, unsicheres Surfen, Dark Web usw.), wie man Opfer eines Identitätsdiebstahls werden kann, zu beschreiben. Anwendung verschiedener Methoden zum Schutz persönlicher Daten im Internet (Überwachung von Kredit Berichten, nicht autorisierte Banktransaktionen, Stoppen des Empfangs von Rechnungen usw., Kontaktaufnahme mit Behörden, Einrichtung eines Betrugswarnsystems).	Anerkennen, dass es unmöglich ist, die eigenen Daten online vollständig zu schützen, aber Wissen und häufige Kontrolle der Konten können einen großen Beitrag zum Schutz persönlicher Daten in digitalen Umgebungen leisten. Erkennen, dass das inhärente Risiko von Online-Geschäften und Methoden zum Schutz persönlicher Daten anwenden.
	Definition des Begriffs „Material über sexuellen Kindesmissbrauch“ (CSAM) (auch bekannt als Kinderpornografie; dieser Begriff sollte jedoch vermieden werden, da	Fähigkeit, den Begriff CSAM und die Folgen der Beschäftigung mit solchem Material im Internet zu erklären (illegal, verwischt das Urteil darüber, was als	Erkennen, dass CSAM eine moderne Version von Kindesmissbrauch und -ausbeutung im Internet ist, die ebenfalls zunimmt. Persönliche Verantwortung übernehmen und

	er ungenau ist und darauf abzielt, die Ausbeutung von Kindern zu legitimieren).	angemessenes Verhalten gegenüber Kindern oder Jugendlichen gilt usw.).	CSAM-Material melden und wissen, wie man einem/einer Freund*in helfen kann, der/die unangemessene Gedanken oder Verhaltensweisen hat.
	Definition des Begriffs „Online-Missbrauch“. Definition des Begriffs „Cybermobbing“. Definition des Konzepts anderer Formen des Online-Missbrauchs und Möglichkeiten, diese zu bekämpfen.	Fähigkeit, die verschiedenen Arten von Online-Missbrauch (Cybermobbing, emotionaler Missbrauch, Grooming, Sexting, sexueller Missbrauch und Ausbeutung) zu erklären und zu erkennen. Fähigkeit, Cybermobbing zu erklären und zu erkennen, wenn es in Online-Umfeld auftritt. Fähigkeit, verschiedene Arten von Online-Missbrauch zu erkennen und Maßnahmen zu ergreifen, um diese zu bekämpfen (z. B. Sexting).	Erkennen, dass Missbrauch auch online stattfinden kann, und zuversichtlich sein, ihn erkennen zu können. Erkennen, dass Cybermobbing eine Form der Belästigung ist, die speziell online stattfindet (auch bekannt als Online-Mobbing oder Online-Belästigung). In der Lage fühlen, ein Familienmitglied über die Formen des Missbrauchs zu informieren, denen es online begegnen oder die es miterleben kann, sowie über Möglichkeiten, dagegen vorzugehen.
	Definition des Konzepts der Datenschutzeinstellungen.	Fähigkeit, den Begriff „Datenschutzeinstellungen“ zu erklären und zu erläutern, wie man diese Einstellungen anpassen kann, um seine Privatsphäre online zu schützen (privates Profil, keine Anfragen von zufälligen Personen annehmen, kein Passwort freigeben, Beiträge nur für Freund*innen sichtbar machen, Tags bewerten usw.).	Erkennen, dass die meisten Social Media-Plattformen die Möglichkeit bieten, die eigene Online-Präsenz individuell zu gestalten.

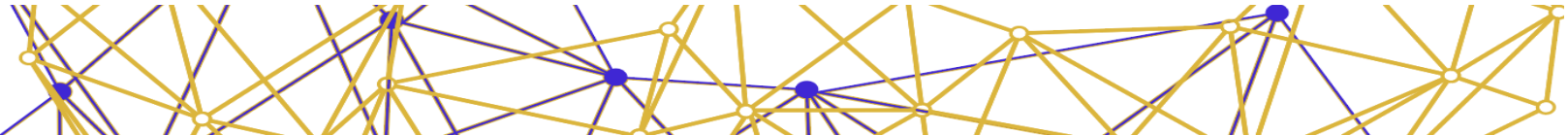


	Kenntnis des europäischen Rechtsrahmens zum Schutz personenbezogener Daten (Allgemeine Datenschutzverordnung 2016/679).	Möglichkeit, die Hauptverantwortlichkeiten von Social Media-Plattformen und Online-Unternehmen gemäß der Datenschutz-Grundverordnung (DSGVO) bei der Erhebung und Weitergabe personenbezogener Daten und der allgemeinen Kommunikation mit dem Kunden darzulegen. Datenschutzerklärungen bieten detaillierte Informationen zum Umgang mit personenbezogenen Daten.	Vertrauen in die Anwendung von Sicherheits- (z. B. Zwei-Faktor-Authentifizierung Passwort) und Datenschutzmaßnahmen in verschiedenen digitalen Umgebungen haben.
	Definition des Konzepts der elterlichen Kontrolle in der digitalen Welt. Definition der Arten der elterlichen Kontrolle, die man in den soziale Medien anwenden kann. Kenntnis verschiedener Möglichkeiten zur Anwendung der elterlichen Kontrolle auf verschiedenen Social Media-Plattformen.	Fähigkeit, die elterliche Kontrolle in verschiedenen Umgebungen (z. B. Fernsehen, Computer, Videospiele usw.) zu erklären und anzuwenden. Fähigkeit, die verschiedenen Arten der elterlichen Kontrolle zu erklären (Inhaltsfilter, Nutzungskontrolle, Tools zur Verwaltung der Computernutzung und Überwachung). Fähigkeit, die elterliche Kontrolle auf verschiedenen Social Media-Plattformen anzuwenden und zu wissen, welche Plattformen einschränkende Optionen für die elterliche Kontrolle bieten.	Anerkennen, dass die elterliche Kontrolle notwendig ist, um eine kinderfreundliche Erfahrung in der Online-Welt zu gewährleisten. Anerkennen, dass Eltern die Möglichkeit haben, den Kontakt ihrer Kinder mit unerwünschten Inhalten zu begrenzen. Wissen, wie man die elterliche Kontrolle in den sozialen Medien anwendet, um eine sichere und kinderfreundliche Erfahrung in den sozialen Medien zu fördern.

Das Modul 6 ist in zwei Workshops von je 2 Stunden Dauer unterteilt. Der Lernprozess des Moduls 6 umfasst auch 4 Stunden selbstständiges Lernen.

Stundenplan

Inhalt - Beschreibung	Unterweisungsmethode	Zeit Dauer	Erforderliche Materialien/ Ausrüstung	Ratschläge/Tipps für Pädagogen, die sie den Teilnehmer*innen geben können	Beurteilung/ Bewertung	Weiterführende Lektüre/ Links zu Materialien
Einführung	Begrüße die Teilnehmer*innen. Zu diesem Zeitpunkt sollten sich alle kennen, aber du kannst eine Vorstellungsrunde einleiten, indem du mit dir selbst beginnst und deinen Vornamen und deinen Beruf bzw. alle relevanten Informationen über dich bekannt gibst. Führe dann das Thema dieses Moduls ein: die externe Bedrohung durch die sozialen Medien. Du kannst die Teilnehmer*innen fragen, woran sie denken, wenn sie über dieses Thema sprechen und die Schlüsselwörter auf den Pappkarton schreiben.	15 min	Pappmarker	Die Begrüßung sollte so freundlich wie möglich sein. Alle Teilnehmer*innen sollten das Gefühl haben, dass sie eine tolle Zeit verbringen werden, also... viel lächeln!	k.A.	k.A.



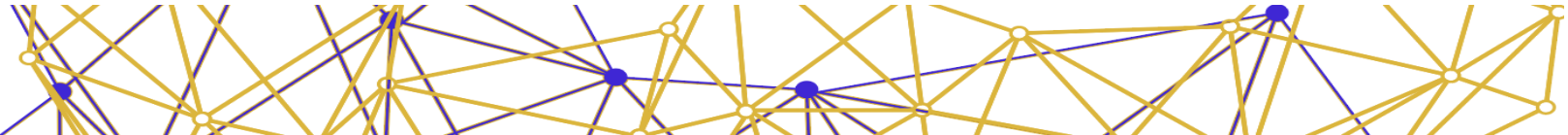
Modul 6 - Workshop 1: Externe Bedrohungen	Erkläre den Teilnehmer*innen dann, dass wir uns auf 3 Hauptthemen konzentrieren werden: ● Fake-Konten ● Identitätsdiebstahl ● Online-Missbrauch Erinnere sie daran, dass das Thema „Informationsstörung“ bereits in früheren Modulen behandelt wurde, dass es aber auch eine Gefahr darstellt, wenn man online ist. Dieses Thema wird auch in den Materialien zum selbstständigen Lernen behandelt **1) Catfishing (30 min)** Beginne mit der Frage an die Teilnehmer*innen, ob sie wissen, was Catfishing ist. Zeige dann dieses kurze Video, um das Konzept vorzustellen: Catfishing - Was ist das? - YouTube Nachdem die Teilnehmer*innen nun wissen, was Catfishing ist, zeige ihnen ein weiteres Video mit Tipps, wie sie gefälschte Online-Profile erkennen können	30 min	PC/Laptop Beamer PPT workshop 1 PC/Laptop Beamer		k.A.	k.A.

	(beginnen das Video bei 0:21 und stoppe es bei 3:06): Fake Profile erkennen [3 Möglichkeiten] - YouTube Hier ist eine Liste der Tools, die zum Erkennen von Catfishing verwendet werden können: ● Google umgekehrte Bildersuche ● Bitte um weitere Informationen und ein Selfie Starte dann eine Diskussion mit den Teilnehmer*innen: ● Was sind die Ziele von Catfishen/Internet-betrüger*innen (Identitätsdiebstahl, Geld, Einsamkeit usw.)? ● Wie kannst du verhindern, dass deine Verwandten Opfer von Catfishing werden? ● Was können wir als Elternteil tun, um solche Situationen zu verhindern? Zeige den Abschnitt des PPT „Vermeiden von Catfishen“.		Papier und Stift für die Teilnehmer*innen zum Mitschreiben PPT-Abschnitt „Vermeiden von Catfish“ PC/Laptop Beamer			

	2) Identitätsdiebstahl (30 min) Identitätsdiebstahl kann der Zweck von Catfishing sein. Dies ist ein häufiger Missbrauch im Internet. Beginne damit, den Teilnehmer*innen dieses kurze Video zu zeigen: Identitätsdiebstahl | Cyber-Gefahren - YouTube Um Identitätsdiebstahl zu vermeiden und ein sicheres Online-Verhalten zu haben, müssen wir einfache Regeln beachten. Zeige den Abschnitt „Sicheres Online-Verhalten“ auf dem PPT. Beginne dann eine Diskussion mit der Gruppe über Identitätsdiebstahl. Erkläre der Gruppe, dass diese Betrügereien auch auf ältere Nutzer*innen abzielen und dass dies jede/n in der Familie betrifft.		PPT-Abschnitt „Sicheres Online-Verhalten“			

	Frag die Gruppe, ob sie schon einmal von Betrüger*innen angesprochen worden sind. Diskutiere die Techniken, die zum Datendiebstahl verwendet werden: ● Phising: betrügerische Praxis des Versendens von E-Mails, die vorgeben, von seriösen Unternehmen zu stammen, um Personen dazu zu bringen, persönliche Informationen preiszugeben ● Pharming: kriminelle Handlung, bei der eine gefälschte Website erstellt wird, auf der die Nutzer*innen dann umgeleitet werden ● Vishing: Anrufe oder Sprachnachrichten, die vorgeben, von seriösen Unternehmen zu stammen, um Personen zur Preisgabe persönlicher Daten zu bewegen ● Smishing: Versenden von Textnachrichten,		PC/Beamer Laptop			

	die vorgeben, von seriösen Unternehmen zu stammen, um Personen dazu zu bringen, persönliche Daten preiszugeben Bitte die Gruppe, sich über ihre Erfahrungen mit diesen Praktiken auszutauschen und darüber, wie sie diese überwunden haben. **3) Online-Missbrauch (30min)** Du wirst nun den Albtraum aller Eltern besprechen: Online-Missbrauch. Beginne mit dem PPT-Abschnitt „Online-Missbrauch“. Dank der Präsentation haben die Teilnehmer*innen verstanden, dass aktives Zuhören eine der wichtigsten Eigenschaften von Eltern ist, um nichts zu verpassen und um Probleme zu erkennen. Die folgende Aktivität dauert 10 Minuten und ist ein Brainstorming über aktives Zuhören.	15 min	PPT-Abschnitt „Online-Missbrauch“			

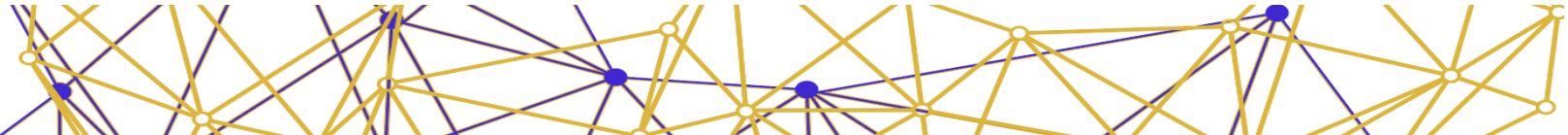


	Frag die Teilnehmer*innen, was die Fähigkeiten aktiver Zuhörer*innen sind, mach dir Notizen auf dem Pappkarton; achte darauf, dass die folgenden Begriffe aus dem Gespräch hervorgehen: - Neutral - Nicht wertend - Geduldig - Verbale und nonverbale Kommunikation - Fragen stellen - Zurückspiegeln des Gesagten - Nachfragen zur Klärung - Zusammenfassen **Zusammenfassung** Frag die Eltern abschließend, was sie heute gelernt haben und ob sie dieses Wissen zu Hause anwenden werden.		Pappmarker			
Module 6 – Workshop 2	**Begrüßung** Begrüße die Teilnehmer*innen, erklären die wichtigsten Lernergebnisse des vorangegangenen Workshops	10 min	k.A.	k.A.	k.A.	k.A.

	und teilen ihnen mit, dass es in dieser Sitzung um Datenschutzeinstellungen und elterliche Kontrolle in sozialen Medien geht. Beginne den Workshop, indem du dieses kurze Video zeigst: So schützt du deine Daten auf Social Media - YouTube Dieses Video veranschaulicht die Anzahl der Daten, die aus einfachen Beiträgen in sozialen Medien abgerufen werden können. Zeige dann dieses Video, in dem personenbezogene Daten vorgestellt werden: Was sind eigentlich personenbezogene Daten im Datenschutz? - YouTube Mit den Datenschutzeinstellungen kannst du kontrollieren, wer Informationen über dich sehen kann. Zeige dann den PPT-Abschnitt „Datenschutzeinstellungen“.	5 min 10mn 35 min	PC/Laptop Beamer PPT-Workshop 2 Papier und Stift für die Teilnehmer*innen zum Mitschreiben PC/Laptop Projektor Papier und Stift für die Teilnehmer*innen zum Mitschreiben PC/Laptop Beamer			

	Stelle sicher, dass die Teilnehmer*innen ihre Fragen stellen können. Zeige den PPT-Abschnitt „Elterliche Kontrolle“ an. Stelle sicher, dass die Teilnehmer*innen ihre Fragen stellen können. Zeige den Teilnehmer*innen abschließend das folgende Video, in dem Software zur elterlichen Kontrolle vorgestellt wird: https://www.youtube.com/watch?v=9DSAi4q6SmQ&ab_channel=10BestOnes Handy für Kinder beschränken - so geht's! | App-Tipps: TimeLimit & Bildschirmzeit | mobil & safe - YouTube	30 min 15 min	PPT-Abschnitt „Datenschutz-Einstellungen“ Papier und Stift für die Teilnehmer*innen zum Mitschreiben PC/Laptop Beamer PPT-Abschnitt „Kindersicherung“ Papier und Stift für die Teilnehmer*innen zum Mitschreiben PC/Laptop Beamer			

	Frag die Teilnehmer*innen nach ihrem Feedback. Denken sie, dass eine solche Software eine gute Idee ist? Wie sieht es mit der Privatsphäre des Kindes aus? Wie kann man gegenseitiges Vertrauen sicherstellen?					
Schlussfolgerung	**Abschluss und Auswertung des Moduls 6** Frag die Eltern abschließend, was sie heute gelernt haben und ob sie dieses Wissen zu Hause anwenden werden. Frag sie, ob das Modul 6 ihre Bedürfnisse erfüllt hat und ob sie weitere Fragen haben.	15 min	Pappmarker			



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

Project Number: 2020-1-AT01-KA204-077958