



**information
matters**

Schulungsprogramm für Online Kurse

Modul 6

Medienkompetenz und digitale Dienste



Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Projektnummer: 2022-1-BG01-KA220-ADU-000085514



**Kofinanziert von der
Europäischen Union**

Contents

Beschreibung der Online-Lektion	3
Einführung	8
Schlüsselwörter	9
Themen	9
Definitionen	10
Einige nützliche Ressourcen	12
Aktivität 1#: Ausbildung zum digitalen Detektiv	13
Lernziele	13
Rahmenbedingungen/Material/Dauer	14
Durchführung der Aktivität:	14
Reflexionsfragen	18
Bewertung des Moduls	19
Fragebogen	19
Validierung des Moduls	19
ANHANG FÜR Modul 6	21





Beschreibung der Online-Lektion

Willkommen zu Modul 6 unseres Kurses. In dieser Lektion befassen wir uns mit den Themen Sicherheit im Internet, Schutz der Privatsphäre, sichere Online-Zahlungen und einigen wichtigen Konzepten zu diesem Thema.

Sehen wir uns einige wichtige Definitionen an.



Sicherheit bezieht sich auf den Zustand, vor potenziellem Schaden, Gefahr oder Risiko geschützt zu sein. Sie umfasst Maßnahmen und Praktiken, die zur Vermeidung von Unfällen, Verletzungen oder jeglicher Form von Schäden an Personen, Eigentum oder Informationen eingesetzt werden. Sicherheit kann physischer, emotionaler oder digitaler Natur sein und beinhaltet die Identifizierung und Abschwächung potenzieller Gefahren. Im Zusammenhang mit der Technologie kann die Sicherheit Maßnahmen zum Schutz der Benutzer vor Cyber-Bedrohungen, zur Gewährleistung der Zuverlässigkeit digitaler Systeme und zur Förderung einer sicheren Online-Umgebung umfassen.



Privatsphäre ist der Zustand, frei von unbefugten Eingriffen in das persönliche Leben, die Aktivitäten oder Informationen einer Person zu sein. Sie beinhaltet das Recht des Individuums, den Zugang und die Verwendung seiner persönlichen Daten zu kontrollieren. Der Schutz der Privatsphäre kann physisch sein, z. B. das Recht, nicht überwacht zu werden, oder digital, wenn es um den Schutz persönlicher Daten im Internet geht. Im digitalen Zeitalter dreht sich die Sorge um die Privatsphäre oft um

die Erhebung, Speicherung und Weitergabe personenbezogener Daten durch Organisationen, Websites und Online-Plattformen. Maßnahmen zum Schutz der Privatsphäre zielen darauf ab, die Autonomie der Einzelperson zu schützen und den unbefugten Zugriff auf sensible Informationen zu verhindern.



Sichere Online-Zahlungsmethoden beziehen sich auf elektronische Transaktionen über das Internet, bei denen der Schutz sensibler Finanzdaten im Vordergrund steht und die Vertraulichkeit, Integrität und Authentizität des Zahlungsvorgangs gewährleistet sind. Bei diesen Methoden werden fortschrittliche Verschlüsselungstechnologien und Sicherheitsprotokolle eingesetzt, um die

Finanzdaten der Nutzenden zu schützen und unbefugten Zugriff und betrügerische Aktivitäten zu verhindern.

Zu den wichtigsten Merkmalen der sicheren Online-Zahlungsmethoden gehören:

- **Verschlüsselung:** Die Verwendung von Verschlüsselungsalgorithmen, um Finanzdaten während der Übertragung zu verschlüsseln, so dass sie für Unbefugte nicht lesbar sind. Secure Sockets Layer (SSL) und Transport Layer Security (TLS) sind gängige Verschlüsselungsprotokolle
- **Tokenisierung:** Die Ersetzung sensibler Daten durch eine eindeutige Kennung oder ein Token. Dies trägt zum Schutz der tatsächlichen Finanzdaten bei, da das Token, selbst wenn es abgefangen wird, keine aussagekräftigen Informationen enthält.
- **Zwei-Faktoren-Authentifizierung (2FA):** Eine zusätzliche Sicherheitsebene, bei der die BenutzerInnen zwei Arten der Identifizierung angeben müssen, bevor sie eine Transaktion abschließen können. Dazu gehören häufig ein Passwort und ein temporärer Code, der an das Mobilgerät der Nutzenden gesendet wird.
- **Sichere Zahlungs-Gateways:** Zahlungsgateways fungieren als Vermittler zwischen der Website der Händler und dem Finanzinstitut und wickeln Transaktionen sicher ab. Seriöse und sichere Zahlungsgateways halten sich an Branchenstandards für den Datenschutz.

- **Betrugserkennung und -verhinderung:** Implementierung von Werkzeugen und Algorithmen zur Erkennung und Verhinderung betrügerischer Aktivitäten, wie z. B. ungewöhnliche Kaufmuster oder mehrfache fehlgeschlagene Anmeldeversuche.
- **Einhaltung von Standards:** Einhaltung von Industriestandards und -vorschriften wie dem Payment Card Industry Data Security Standard (PCI DSS), der Anforderungen für den Umgang mit Kreditkartendaten festlegt.
- **Kundenschulung:** Bereitstellung von Informationen und bewährten Praktiken für die Aufrechterhaltung sicherer Online-Praktiken, einschließlich der Bedeutung von sicheren Passwörtern, der Vermeidung von öffentlichem WLAN für sensible Transaktionen und der regelmäßigen Überprüfung von Finanzberichten.

Glückwunsch zum Abschluss von Lektion 6! Diese Lektion hat einen kurzen Überblick über die Sicherheit, den Datenschutz und die Finanzen im Internet gegeben. Hoffentlich fühlen Sie sich jetzt besser auf die digitale Welt vorbereitet. Wir empfehlen Ihnen, mit Lektion 7 fortzufahren. Viel Erfolg!



Einführung

Einkaufen, Arztbesuche, die Inanspruchnahme kommunaler Dienstleistungen - mit der zunehmenden Digitalisierung sind viele alltägliche Aktivitäten für Menschen mit geringen digitalen Kenntnissen komplizierter geworden. Ältere Menschen haben oft Schwierigkeiten, Online-Banking zu nutzen, Buchungen vorzunehmen, einzukaufen, Filme per Online-Streaming anzusehen, Spiele zu spielen und Online-Gesundheitsdienste in Anspruch zu nehmen.

Es ist notwendig, neue Fähigkeiten zu entwickeln, um am öffentlichen Leben (Wahlen, politische Debatten im Internet), an wirtschaftlichen Aktivitäten (wie dem Kauf/Verkauf von Waren und Dienstleistungen) und an der gesellschaftlichen Eingliederung (persönlicher Austausch, Fernbetreuung bei körperlichen Aktivitäten o. ä.) teilzunehmen.

Lernergebnisse

Nach Abschluss dieses Moduls sollten die Teilnehmenden mehr Sicherheit beim Online-Einkauf, bei der Inanspruchnahme von Arztbesuchen und bei der sicheren Nutzung von Bankdienstleistungen haben. Sie sollten auch in der Lage sein, Buchungsdienste, Unterhaltungsangebote und den Zugang zu Spielen zu nutzen. Sie werden verstehen, wie sie mit größerer Leichtigkeit an Online-Communities und am öffentlichen Leben teilnehmen können.

Schlüsselwörter

Digitale Dienste, Online-Gemeinschaften, Bankgeschäfte, Buchungen, Einkaufen, Suchen, Streaming, Spielen, Online-Arztbesuche.

Themen

Zugang zu vernetzten Geräten und digitalen Plattformen.

Zu den behandelten Themen gehören Einkaufen, Online-Unterhaltung, aktive Beteiligung an der Gemeinschaft, Erkundung von Online-Gesundheitsressourcen usw, Verständnis von Sicherheit und Datenschutz, einschließlich sicherer Zahlungsmethoden, Erkennung von Betrug und Finanzbetrug.

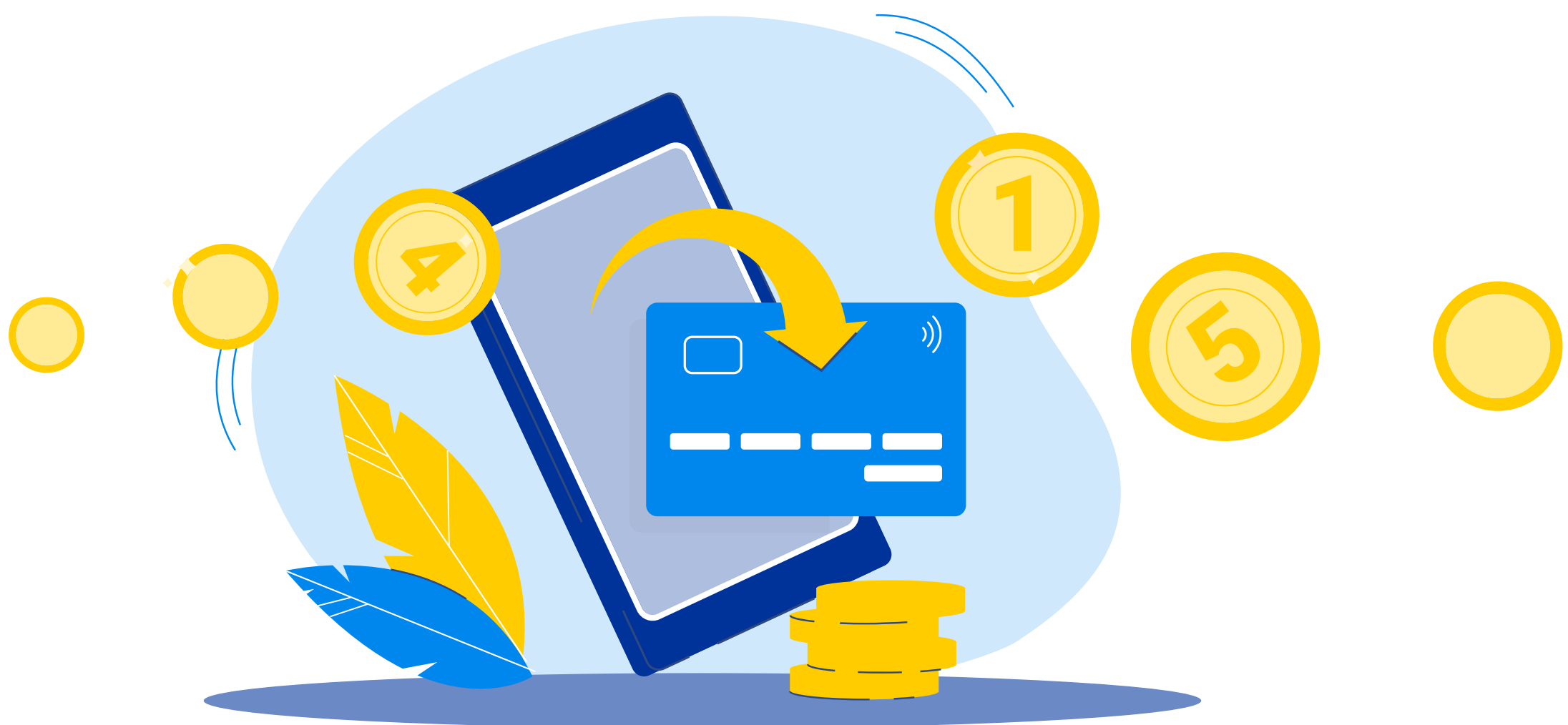


Definitionen

- 1. Sicherheit** bezieht sich auf den Zustand des Schutzes vor potenziellen Schäden, Gefahren oder Risiken. Sie umfasst Maßnahmen und Praktiken, die zur Vermeidung von Unfällen, Verletzungen oder jeglicher Form von Schäden an Personen, Eigentum oder Informationen eingesetzt werden. Sicherheit kann physischer, emotionaler oder digitaler Natur sein und beinhaltet die Identifizierung und Abschwächung potenzieller Gefahren. Im Zusammenhang mit der Technologie kann die Sicherheit Maßnahmen zum Schutz der BenutzerInnen vor Cyber-Bedrohungen, zur Gewährleistung der Zuverlässigkeit digitaler Systeme und zur Förderung einer sicheren Online-Umgebung umfassen.
- 2. Privacy Privatsphäre** ist der Zustand, frei von unbefugtem Eindringen in das persönliche Leben, die persönlichen Aktivitäten oder Informationen zu sein. Sie beinhaltet das Recht des Individuums, den Zugang und die Verwendung seiner persönlichen Daten zu kontrollieren. Der Schutz der Privatsphäre kann physisch sein, z. B. das Recht, nicht überwacht zu werden, oder digital, wenn es um den Schutz persönlicher Daten im Internet geht. Im digitalen Zeitalter dreht sich die Sorge um die Privatsphäre oft um die Erhebung, Speicherung und Weitergabe personenbezogener Daten durch Organisationen, Websites und Online-Plattformen.

Maßnahmen zum Schutz der Privatsphäre zielen darauf ab, die Autonomie des Individuums zu schützen und den unbefugten Zugriff auf sensible Informationen zu verhindern.

- 3. Sichere Online-Zahlungsmethoden** beziehen sich auf elektronische Transaktionen über das Internet, bei denen der Schutz sensibler Finanzdaten im Vordergrund steht und die die Vertraulichkeit, Integrität und Authentizität des Zahlungsvorgangs gewährleisten. Bei diesen Methoden werden fortschrittliche Verschlüsselungstechnologien und Sicherheitsprotokolle eingesetzt, um die Finanzdaten der NutzerInnen zu schützen und unbefugten Zugriff und betrügerische Aktivitäten zu verhindern.



Einige nützliche Ressourcen

Digitalisierung von Dienstleistungen: Sicherstellung eines gleichberechtigten Zugangs für alle, auch für ältere Menschen von heute und morgen:

 <https://www.age-platform.eu/special-briefing/digitalisation-services-ensuring-equal-access-all-including-older-people-today-and>

HWie können wir die digitale Integration älterer Menschen sicherstellen?

 <https://www.weforum.org/agenda/2021/10/how-can-we-ensure-digital-inclusion-for-older-adults>

Senior Planet und AARP bieten kostenlose Online-App-Kurse an:

 <https://www.digitallearn.org>

 www.aarp.org/home-family/personal-technology/info-2021/senior-planet-and-aarp-online-classes.html

Making It Click: Unterstützung für Menschen mit geringer Internetnutzung

 <http://www.goodthingsfoundation.org/insights/making-it-click-supporting-people-with-low-internet-use>



Aktivität 1#: Ausbildung zum digitalen Detektiv

Erstellen Sie eine Liste mit allen Funktionen, die ein modernes Smartphone vereint. Wie viele Geräte sind heutzutage darin enthalten?

Lernziele

- Verbesserung der Fähigkeiten der Teilnehmenden, Fehlinformationen im Internet zu erkennen und zu bekämpfen, durch eine praktische, interaktive Aktivität.

Rahmenbedingungen/Material/Dauer

- Geräte mit Internetanschluss (Laptops, Tablets oder Desktop-Computer)
- Zugang zu einem Webbrowser
- Liste ausgewählter Websites (einige verlässlich, andere enthalten Fehlinformationen)

Durchführung der Aktivität:

Schritt 1 - Einführung:

(15 Minuten)

- Beginnen Sie mit einer kurzen Präsentation über die Verbreitung von Fehlinformationen im Internet und deren Auswirkungen.
- Betonen Sie die Bedeutung von Faktenüberprüfung und kritischer Bewertung im digitalen Zeitalter.

Schritt 2 - Verlässliche Quellen verstehen

(20 Minuten)

- Stellen Sie eine Liste zuverlässiger Websites zusammen, die für genaue und vertrauenswürdige Informationen bekannt sind (z. B. Websites zur Überprüfung von Fakten, seriöse Nachrichtenagenturen).
- Diskutieren Sie die Kriterien, die diese Quellen zuverlässig machen (Glaubwürdigkeit, Transparenz, Standards zur Überprüfung der Fakten).

Schritt 3 - Erkennen von Fehlinformationen

(30 Minuten)

- Stellen Sie eine Liste von Websites vor, die Fehlinformationen enthalten oder dafür bekannt sind, falsche Informationen zu verbreiten.
- Ermutigen Sie die Teilnehmenden, diese Websites auf Anzeichen von Fehlinformationen hin zu untersuchen (Sensationslust, Fehlen glaubwürdiger Quellen, verzerrte Sprache).
- Diskutieren Sie die häufigsten Anzeichen für Fehlinformationen.



Schritt 4 - Interaktive Überprüfung der Fakten

(40 Minuten)

- Bieten Sie den Teilnehmenden spezifische Behauptungen oder Nachrichtenartikel aus zuverlässigen und unzuverlässigen Quellen an.
- Geben Sie den Teilnehmenden die Aufgabe, die Behauptungen mit Hilfe seriöser Websites auf ihre Richtigkeit zu überprüfen.
- Diskutieren Sie die Ergebnisse in der Gruppe und betonen Sie, wie wichtig es ist, Informationen mit Querverweisen zu versehen.

Schritt 5 - Gruppendiskussion

(15 Minuten):

- Leiten Sie eine Gruppendiskussion über die Herausforderungen und Strategien, die während des Faktencheck-Prozesses aufgetreten sind.
- Ermutigen Sie die Teilnehmenden, Erkenntnisse und Tipps zur Unterscheidung zwischen zuverlässigen und unzuverlässigen Quellen auszutauschen.



Schritt 6 - Austausch von Ressourcen

(20 Minuten):

- Lassen Sie die Teilnehmenden eine Liste mit nützlichen Websites und Tools zur Überprüfung von Fakten und zur Erkennung von Fehlinformationen zusammenstellen.
- Teilen Sie die zusammengestellte Liste mit der Gruppe und diskutieren Sie, wie diese Ressourcen in ihre täglichen Online-Aktivitäten integriert werden können.

Schritt 7 - Reflexion und Fragen und Antworten

(15 Minuten):

- Schließen Sie die Sitzung mit einer Reflexion über die wichtigsten Erkenntnisse und Erfahrungen ab.
- Bieten Sie die Möglichkeit, Fragen zu stellen, und stellen Sie zusätzliche Ressourcen für weiteres Lernen zur Verfügung.

Nachbereitung:

Ermutigen Sie die Teilnehmenden, ihre Fähigkeiten zur Überprüfung von Fakten weiter zu üben, indem sie sich regelmäßig mit seriösen Websites zur Überprüfung von Fakten beschäftigen. Verteilen Sie außerdem eine Liste mit zuverlässigen Nachrichtenquellen und Tools zur Überprüfung von Fakten, die sie in ihre Online-Routine integrieren können.

Diese Aktivität verbessert nicht nur die Fähigkeit der Teilnehmenden, Fehlinformationen zu erkennen, sondern vermittelt ihnen auch praktische Fähigkeiten, um sich verantwortungsvoll in der digitalen Landschaft zu bewegen.

Reflexionsfragen

- Sind alle Websites sicher?
- Wie können wir erkennen, dass eine Website nicht sicher ist?
- Was ist zu tun, wenn wir sehen, dass eine Website nicht sicher ist?

Bewertung des Moduls

Fragebogen

Wird von den Lernenden am Ende des Moduls ausgefüllt, um die Gesamtwirkung des Schulungsprogramms zu beurteilen.

- Sind alle Websites sicher und wie können wir eine Website als nicht sicher erkennen?
- Welches sind die sicheren Websites?
- Was macht eine Website sicher?
- Woran erkennt man, dass eine Website sicher ist?

Validierung des Moduls

Am Ende des Moduls haben die Lernenden gelernt, wie man die Sicherheit einer Website überprüft und wie man erkennt, welche Websites nicht sicher sind.

Wissen:

Die Lernenden sind in der Lage

- die Sicherheit einer Website zu überprüfen
- zu verstehen, welche Websites sicher und welche nicht sicher sind
- eine Auswahl an sicheren Websites für ihre Nutzung zu haben

Fertigkeiten:

Die Lernenden sind in der Lage

- die wichtigsten Punkte der Webseiten-Sicherheit zu identifizieren
- die Sicherheit der von ihnen besuchten Websites zu überprüfen
- den Unterschied zwischen sicheren und unsicheren Websites zu erkennen

Kompetenzen:

Die Lernenden verfügen über

- Verständnis für die Online-Sicherheit
- Kenntnisse zur Identifizierung der wichtigsten Punkte der Online-Sicherheit im Zusammenhang mit einer Website

ANHANG FÜR Modul 6

Medienkompetenz und digitale Dienste

Einstiegstest - Medienkompetenz und digitale Dienste

Frage 1: Online-Shopping kann für ältere Menschen bequem sein und ihnen Zugang zu einer breiten Produktpalette verschaffen.

- a. Richtig
- b. Falsch

Frage 2: Welches der folgenden Beispiele ist KEIN Beispiel für Online-Unterhaltung für ältere Menschen?

- a. Filme oder Serien online ansehen
- b. Spiele auf Social-Media-Plattformen spielen
- c. Teilnahme an virtuellen Rundgängen durch Museen und Sehenswürdigkeiten
- d. Teilnahme an Online-Kursen oder Webinaren

Frage 3: Die aktive Teilnahme an der Gemeinschaft über Online-Plattformen kann älteren Menschen helfen, mit anderen in Kontakt zu bleiben und Einsamkeit zu bekämpfen.

- a. Richtig
- b. Falsch

Frage 4: Welche der folgenden Maßnahmen wird NICHT empfohlen, um Betrügereien und Finanzbetrug bei der Nutzung digitaler Dienste zu erkennen?

- a. Weitergabe von persönlichen oder finanziellen Informationen an unbekannte Personen oder Websites
- b. Prüfen Sie bei Online-Zahlungen auf sichere Website-Verbindungen (https://)
- c. Seien Sie vorsichtig bei unaufgeforderten E-Mails oder Anrufen, in denen Sie nach persönlichen oder finanziellen Informationen gefragt werden
- d. Lesen Sie Online-Bewertungen und Feedback, bevor Sie etwas kaufen.

Richtige Antworten:

Frage 1: a) Richtig

Frage 2: d) Teilnahme an Online-Kursen oder Webinaren

Frage 3: a) Richtig

Frage 4: a) Weitergabe von persönlichen oder finanziellen Informationen an unbekannte Personen oder Websites

Abschlusstest - Medienkompetenz und digitale Dienste

Frage 1: Online-Einkäufe sind sicherer als Einkäufe in physischen Geschäften.

- a. Richtig
- b. Falsch

Frage 2: Welches der folgenden Beispiele ist KEIN Beispiel für Online-Unterhaltung?

- a. Streaming von Filmen und Fernsehsendungen
- b. Spielen von Online-Spielen
- c. Beitritt zu Plattformen sozialer Medien
- d. Lesen von digitalen Nachrichtenartikeln

Frage 3: Die aktive Teilnahme an der Gemeinschaft kann durch Online-Plattformen erleichtert werden.

- a. Richtig
- b. Falsch

Frage 4: Was ist ein wichtiger Aspekt bei der Erkundung von Online-Gesundheitsressourcen?

- a. Überprüfung der Glaubwürdigkeit der Quellen
- b. Weitergabe persönlicher medizinischer Informationen im Internet
- c. Ignorieren von Nutzerbewertungen und Feedback
- d. Meiden seriöser Gesundheits-Websites

Richtige Antworten:

Frage 1: b) Falsch. Online-Shopping kann zwar bequem sein, aber es ist wichtig, vorsichtig zu sein und sich von der Rechtmäßigkeit und Sicherheit der verwendeten Websites und Plattformen zu überzeugen.

Frage 2: d) Lesen von digitalen Nachrichtenartikeln.

Online-Unterhaltung bezieht sich in der Regel auf Aktivitäten wie Streaming, Spiele und die Nutzung sozialer Medien.

Frage 3: a) Richtig. Online-Plattformen bieten Einzelpersonen die Möglichkeit, sich in ihren Gemeinschaften zu engagieren, an Diskussionen teilzunehmen, Interessengruppen beizutreten und zu verschiedenen Anliegen beizutragen.

Frage 4: a) Überprüfung der Glaubwürdigkeit der Quellen

Es ist wichtig, die Zuverlässigkeit und den Ruf von Online-Gesundheitsressourcen zu überprüfen, bevor man sich auf sie verlässt, um genaue Informationen zu erhalten.





information matters

contact@informationmatters.eu

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Projektnummer: 2022-1-BG01-KA220-ADU-000085514



**Kofinanziert von der
Europäischen Union**