Methodik & Handbuch für den Aufbau digitaler Resilienz

Aufbau von digitaler Resilienz durch den öffentlichen Zugang zu digitalem Wohlbefinden und Sicherheit

2022-2-SK01-KA220-ADU-000096888

Co-funded by the European Union

Erasmus+ projekt KA220 Kooperationspartnerschaften in der Erwachsenenbildung

Aufbau von digitaler Resilienz durch den öffentlichen Zugang zu digitalem Wohlbefinden und Sicherheit

2022-2-SK01-KA220-ADU-000096888

DigiWELL

Methodik & Handbuch für den Aufbau digitaler Resilienz

September, 2023

Co-funded by the European Union

Diese Publikation wurde als Ergebnis des Projekts erstellt “Aufbau digitaler Resilienz durch Ermöglichung des Zugangs zu digitalem Wohlbefinden und Sicherheit für alle” (Projekt N: 2022-2-SK01-KA220-ADU-000096888), welches im Rahmen von Erasmus+ umgesetzt wird KA220 Kooperationspartnerschaften in der Erwachsenenbildung.

DigiWELL Konsortium

Slovak University of Agriculture in Nitra, Slovakia

Muğla Sıtkı Koçman University, Turkey

Czech technical university in Prague, Czech

Innovation, Training, and Employment Association for Sustainable Development (AIFED), Spain

European Institute for Innovation – Technology (EIfI-Tech), Germany

Foundation Maker's Place Private Company (Found.ation), Greece

Syzigia Skopje Foundation (SYZYGY), Macedonia

Faculty of Economics and Management
Slovak University of Agriculture in Nitra |
Tr. Andreja Hlinku 2 | 949 76 Nitra | Slovakia | email: digiwell@uniag.sk

Website: www.digiwell.sk

Haftungsausschluss:

" Kofinanziert durch das Erasmus+ Programm der Europäischen Union. Diese Veröffentlichung gibt nur die Ansichten der Mitwirkenden wieder, und die Europäische Kommission und die Slowakische Akademische Vereinigung für Internationale Zusammenarbeit können nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden."

Arbeitspaket 2: **Aufbau Digitaler Resilienz Methodik & Handbuch**

Liste der Mitwirkenden: *Murat Sümer, Czech Technical University,*

David Vaneček, Czech Technical University,

Martina Hanová, Slovak University of Agriculture in Nitra, Slovakia

Marcela Hallová, Slovak University of Agriculture in Nitra, Slovakia

Eva Oláhová, Slovak University of Agriculture in Nitra, Slovakia

Eyüp Şen, Muğla Sıtkı Koçman University, Turkey

İlker Yorulmaz, Muğla Sıtkı Koçman University, Turkey

Maria Martinez, AIFED, Spain

Jesus de Haro Martinez, AIFED, Spain

Chris Ashe, ElfI-Tech, Germany

Mattia Ferrari, ElfI-Tech, Germany

Maria Kandilioti, Found.ation, Greece

Roula Mourmouri, Found.ation, Greece

Suzana Trajkovska, SYZYGY, Macedonia

Aleksandar Kochankovski, SYZYGY, Macedonia

INHALTSVERZEICHNIS

Zusammenfassung

Nach der COVID-19-Pandemie sind einige Bedürfnisse aufgrund der Nutzung digitaler Technologien und des Internets, die in unserem Leben eine große Rolle spielen, lebenswichtig geworden. Das Wichtigste davon ist, in der Lage zu sein, sicher in der digitalen Welt zu handeln, ohne Schaden zu nehmen. Insbesondere Erwachsene brauchen digitale Sicherheitsmaßnahmen und einige Kompetenzen, um sich vor Cyber-Bedrohungen zu schützen. Außerdem machen Internet und digitale Technologien das Leben nicht nur einfacher, sondern schaffen auch einige negative psychologische Probleme. So ist beispielsweise Cybermobbing zu einem schwer zu bewältigenden Problem geworden. Dementsprechend ist die Gewährleistung des Wohlbefindens in der digitalen Welt unter den gegenwärtigen Bedingungen zu einer Notwendigkeit geworden. Auch in diesem Zusammenhang haben die zunehmende Nutzung digitaler Technologien und der durch die digitale Transformation erreichte Punkt einige Themen wie digitale Müdigkeit auf die Tagesordnung der Menschen gebracht.

In diesem Zusammenhang zielt das DigiWELL-Projekt darauf ab, die Grundsätze des digitalen Wohlbefindens in die Erwachsenenbildung zu integrieren. Seine Initiativen zielen darauf ab, zur allgemeinen Praxis von Organisationen, Netzwerken und Initiativen der Erwachsenenbildung beizutragen. Das Projekt weiß, wie wichtig es ist, sich mit den Auswirkungen der Technologie auf die psychische Gesundheit, die Produktivität und das allgemeine Wohlbefinden von Erwachsenen im digitalen Zeitalter auseinanderzusetzen. Das Hauptziel von DigiWELL ist es, erwachsene Lernende mit den Informationen, Fähigkeiten und Ressourcen auszustatten, die sie benötigen, um sich ethisch und gewissenhaft in der digitalen Welt zurechtzufinden. Das DigiWELL-Projekt umfasst auch die Entwicklung und Durchführung zusätzlicher Initiativen zur Befähigung erwachsener Lernender. Das Ziel dieser Aktivitäten ist es, eine unterstützende Umgebung zu schaffen, in der Erwachsene ihre Erfahrungen, Schwierigkeiten und Erfolge bei der Förderung des digitalen Wohlbefindens austauschen können. In diesem Sinne bietet das DigiWELL-Projekt viele Möglichkeiten für Einzelpersonen und Organisationen für Erwachsene, sich der Bedeutung des digitalen Wohlbefindens bewusst zu werden und darüber aufzuklären, wie man das digitale Wohlbefinden von erwachsenen Einzelpersonen und Erwachsenenbildnern und -ausbildern fördern kann. Die Förderung des digitalen Wohlbefindens mit einem ganzheitlichen Ansatz ist viel besser möglich, wenn alle relevanten Parteien Maßnahmen ergreifen, um die Bedürfnisse des digitalen Wohlbefindens des Einzelnen zu unterstützen. Daher laden die in diesem Handbuch vorgestellten Informationen, Tipps und bewährten Verfahren Menschen und interessierte Organisationen dazu ein, Initiativen zu ergreifen, damit mehr von uns ein besseres digitales Wohlbefinden und auch ein stärkeres digitales Leben haben.

1 Einführung

1.1 Ziel der Methodik & Handbuch

- Einen Beitrag dazu zu leisten, dass digitales Wohlbefinden und digitale Sicherheit für alle zugänglich sind, indem Erwachsene über digitales Wohlbefinden und digitale Sicherheit und die dafür notwendigen Kompetenzen ermutigt und informiert werden.
- Einführung der digitalen Resilienz, des digitalen Wohlbefindens und der digitalen Sicherheit, des terminologischen Rahmens und der besten Verfahren des digitalen Wohlbefindens und der digitalen Sicherheit für alle Menschen.
- Gewährleistung der Multikulturalität durch Anpassung der entwickelten Ergebnisse an die relevanten Organisationen in den Partnerländern.

1.2 EU DigComp Framework

Im EU DigComp Framework umfasst die digitale Kompetenz die "selbstbewusste, kritische und verantwortungsvolle Nutzung digitaler Technologien und den Umgang mit ihnen für das Lernen, die Arbeit und die Teilnahme an der Gesellschaft. Sie ist definiert als eine Kombination aus Wissen, Fähigkeiten und Einstellungen“ (Council Recommendation on Key Competences for Life- long Learning, 2018).

Im EU DigComp Framework werden die Schlüsselkomponenten der digitalen Kompetenz in 5 Bereichen identifiziert. Die Bereiche sind im Folgenden zusammengefasst:

Informations- und Datenkompetenz: Artikulieren von Informationsbedürfnissen, Auffinden und Abrufen von digitalen Daten, Informationen und Inhalten. Beurteilung der Relevanz der Quelle und ihres Inhalts. Speichern, Verwalten und Organisieren von digitalen Daten, Informationen und Inhalten.

Kommunikation und Zusammenarbeit: Interaktion, Kommunikation und Zusammenarbeit mit Hilfe digitaler Technologien unter Berücksichtigung der kulturellen und generationsbedingten Vielfalt. Teilhabe an der Gesellschaft durch öffentliche und private digitale Dienste und Bürgerbeteiligung. Verwaltung der eigenen digitalen Präsenz, Identität und Reputation.

Erstellung digitaler Inhalte: Erstellung und Bearbeitung digitaler Inhalte. Verbesserung und Integration von Informationen und Inhalten in einen bestehenden Wissensfundus unter Berücksichtigung von Urheberrechten und Lizenzen. Wissen, wie man verständliche Anweisungen für ein Computersystem gibt.

Sicherheit: Schutz von Geräten, Inhalten, persönlichen Daten und der Privatsphäre in digitalen Umgebungen. Schutz der physischen und psychischen Gesundheit und Bewusstsein für digitale Technologien für soziales Wohlbefinden und soziale Integration. Sich der Umweltauswirkungen digitaler Technologien und ihrer Nutzung bewusst sein.

Problemlösung: Erkennen von Bedürfnissen und Problemen und Lösen von konzeptionellen Problemen und Problemsituationen in digitalen Umgebungen. Nutzung digitaler Werkzeuge zur Innovation von Prozessen und Produkten. Mit der digitalen Entwicklung Schritt halten.

Schutz der Gesundheit und des Wohlbefindens bedeutet, (a) Gesundheitsrisiken und Gefahren für das physische und psychische Wohlbefinden bei der Nutzung digitaler Technologien vermeiden zu können, (b) sich selbst und andere vor möglichen Gefahren in digitalen Umgebungen (z. B. Cyber-Mobbing) schützen zu können und (c) digitale Technologien für das soziale Wohlbefinden und die soziale Integration zu nutzen.

1.3 Warum ist die Methodik & Handbuch eine gute Ressource für Erwachsene?

Wie bereits erwähnt, sind nach der COVID-19-Pandemie einige Bedürfnisse aufgrund der Nutzung digitaler Technologien und des Internets, die in unserem Leben eine große Rolle spielen, sehr wichtig geworden. Das wichtigste davon ist, in der Lage zu sein, sicher in der digitalen Welt zu handeln, ohne Schaden zu nehmen. Insbesondere Erwachsene brauchen digitale Sicherheitsmaßnahmen und einige Kompetenzen, um sich vor Cyber-Bedrohungen zu schützen. Außerdem machen Internet und digitale

Technologien das Leben nicht nur einfacher, sondern schaffen auch einige negative psychologische Probleme. So ist beispielsweise Cybermobbing zu einem schwer zu bewältigenden Problem geworden. Dementsprechend ist die Gewährleistung des Wohlbefindens in der digitalen Welt unter den gegenwärtigen Bedingungen zu einer Notwendigkeit geworden. Auch in diesem Zusammenhang haben die zunehmende Nutzung digitaler Technologien und der digitale Wandel dazu geführt, dass Themen wie digitale Müdigkeit auf die Tagesordnung der Menschen gesetzt wurden.

Dieses Handbuch verwendet so viele Beispiele aus der Praxis wie möglich und lässt die erwachsenen Lernenden einige Konzepte selbst herausfinden, um die Erwachsenenbildung auf der Grundlage von Knowles (1968) zu unterstützen.

1.4 Warum ist die Methodik & Handbuch eine gute Ressource für Trainer im Erwachsenenbereich?

Schulung und Ausbildung spielen eine entscheidende Rolle bei der Stärkung des Bewusstseins für digitale Sicherheit, indem sie den Menschen das Wissen, die Fähigkeiten und die besten Verfahren vermitteln, die sie benötigen, um sich und ihre Organisationen vor Cyber-Bedrohungen zu schützen. Darüber hinaus sind Schulung und Ausbildung im Bereich der digitalen Sicherheit wesentliche Komponenten für den Aufbau einer starken Kultur der Cybersicherheit. Durch die Entwicklung von Schulungsprogrammen, die auf die spezifischen Bedürfnisse und Rollen zugeschnitten sind, werden Erwachsene mit dem Wissen und den Fähigkeiten ausgestattet, die sie benötigen, um Cyber-Bedrohungen zu erkennen und effektiv auf sie zu reagieren.

Schulungen helfen den Teilnehmern, die verschiedenen Arten von Cyber-Bedrohungen wie Phishing, Malware, Social Engineering und Ransomware zu verstehen. Durch das Erkennen dieser Bedrohungen können Einzelpersonen bei der Nutzung digitaler Plattformen wachsamer und vorsichtiger sein. Durch Schulungen können Einzelpersonen lernen, wie sie Phishing-E-Mails, -Nachrichten oder -Websites erkennen können. Sie lernen, verdächtige Elemente zu erkennen und vermeiden es, auf bösartige Links zu klicken oder vertrauliche Informationen preiszugeben. Gleichzeitig umfasst die Schulung Richtlinien zur Sicherung von Mobilgeräten, zum Schutz mit Passcodes, zur Verwendung von Verschlüsselung und zur Vorsicht beim Herunterladen von Apps. Gleichzeitig wird sichergestellt, dass die Mitarbeiter die relevanten Cybersicherheitsvorschriften und Compliance-Anforderungen kennen, was zur Einhaltung rechtlicher und ethischer Praktiken beiträgt. Schließlich wird den Menschen durch die Aufklärung klar, dass Cybersicherheit eine gemeinsame Verantwortung ist und dass die aktive Beteiligung aller notwendig ist, um ein sicheres Umfeld aufrechtzuerhalten, während gute Cybersicherheitsgewohnheiten vermittelt werden, die die Menschen ermutigen, Sicherheitsmaßnahmen sowohl bei der Arbeit als auch im Privatleben umzusetzen.

Das DigiWELL-Projekt zielt darauf ab, die Bedürfnisse von Erwachsenen, die nicht in das Internetzeitalter hineingeboren wurden, nach digitaler Sicherheit und Wohlbefinden zu erfüllen. Dies soll durch die Schaffung und Entwicklung flexibler Lernangebote erreicht werden, die auf die spezifischen Lernbedürfnisse von Erwachsenen zugeschnitten sind. Das Projekt wird sich darauf konzentrieren, die digitale Widerstandsfähigkeit durch einen Blended-Learning-Ansatz zu verbessern. Insbesondere dieses Handbuch trägt zu dem oben genannten Ziel bei, da es eine sicherheitsbewusste Kultur schafft, die sich aktiv gegen Cyber-Bedrohungen wehrt und digitale Werte und sensible Informationen schützt.

Mit anderen Worten: Ein Handbuch, das einen Abschnitt über digitale Sicherheit enthält, kann eine wichtige Rolle dabei spielen, Erwachsene mit den notwendigen Fähigkeiten und Kenntnissen auszustatten, um sich im digitalen Zeitalter zu schützen und eine sicherere Online-Erfahrung für Einzelpersonen und Gemeinschaften gleichermaßen zu fördern. Der DigiWELL ist eine wertvolle Ressource für Erwachsene, denn er klärt sie über potenzielle Risiken auf und hilft ihnen, die Bedeutung der Cybersicherheit zu verstehen und zu wissen, wie sie sich online schützen können. Schließlich bietet er praktische Anleitungen für die Umsetzung digitaler Sicherheitsmaßnahmen und befähigt Erwachsene, sich in der digitalen Welt sicher zu bewegen. Er dient als Nachschlagewerk, das Erwachsene immer dann wieder zur Hand nehmen können, wenn sie mit neuen Herausforderungen im Bereich der digitalen Sicherheit konfrontiert werden oder eine Auffrischung bestimmter Themen benötigen.

1.5 Wörterbuch des DigiWELL-Projekts und seine Verwendung

Das Wörterbuch soll erwachsene Nutzer digitaler Technologien mit grundlegenden Begriffen und Definitionen im Zusammenhang mit digitalem Wohlbefinden, digitaler Sicherheit und digitaler Resilienz vertraut machen.

Klassifizierung der Begriffe

Inhaltlich enthält das Wörterbuch drei grundlegende Kategorien von Begriffen;

1. Begriffe und Definitionen aus dem Bereich der Informations- und Kommunikationstechnologien (digitale Technologien im Sinne des Projekts).
2. Begriffe und Definitionen aus dem Bereich der Informations-, Cyber- und digitalen Sicherheit (digitale Sicherheit im Sinne des Projekts).
3. Begriffe und Definitionen aus dem Bereich der Projektziele: digitales Wohlbefinden und digitale Resilienz. Diese Begriffe sind relativ neu und stammen aus den Recherchen der Projektteams. Es ist zu betonen, dass es keine einheitliche Definition dieser Begriffe gibt. Diese Kategorie umfasst auch Begriffe aus dem Bereich der psychischen und physischen Gesundheit, z. B. digitale Sucht, digitale Müdigkeit/Burnout, digitale Entgiftung usw.

Hinweis: In der Textdatenbank eines Wörterbuchs kann ein Begriff aus verschiedenen Gründen mehr als eine Definition haben: Die ursprüngliche Definition hat sich im Laufe der Zeit weiterentwickelt, die weit gefasste Definition ist auf einen bestimmten Bereich zugeschnitten, die Definitionen der Begriffe sind ähnlich, weisen aber feine Unterschiede auf usw.

Begriffe und Definitionen

Digitale Resilienz: 1. Digitale Resilienz bedeutet, über das Bewusstsein, die Fähigkeiten, die Agilität und das Vertrauen zu verfügen, um neue Technologien zu nutzen und sich an die sich ändernden digitalen Qualifikationsanforderungen anzupassen. Digitale Resilienz verbessert die Fähigkeit, Probleme zu lösen und sich weiterzubilden, sowie die Fähigkeit, den digitalen Wandel zu bewältigen. 2. Digitale Resilienz ist die Fähigkeit junger Menschen, beim Zugang zu digitalen Informationen eine kritische Einstellung zu entwickeln, um ihre Anfälligkeit für potenziell schädliche Informationen zu verringern. 3. Digitale Resilienz

bedeutet "der Prozess der Anpassung an digitale Stressquellen und die Entwicklung von Fähigkeiten zur Bewältigung der Auswirkungen der sich ständig verändernden digitalen Umgebungen und Anwendungen".

Digitale Sicherheit: Digitale Sicherheit ist der Schutz der digitalen Identität, da sie eine physische Identität im Netz oder in Internetdiensten darstellt. Die digitale Sicherheit besteht aus einer Reihe von bewährten Verfahren und Werkzeugen zum Schutz persönlicher Daten und der Online-Identität in der Online-Welt. Beispiele für Werkzeuge sind: Webdienste, Antivirus-Software, Smartphone-SIM-Karten, biometrische und sichere persönliche Geräte, Passwort-Manager, elterliche Kontrolle usw.

Digitales Wohlbefinden: 1. Digitales Wohlbefinden beschreibt die Fähigkeit einer Person, die negativen Auswirkungen der Technologie auf ihr berufliches und privates Leben effektiv zu bewältigen. Das Ziel des digitalen Wohlbefindens ist die Förderung einer gesunden Nutzung von technischen Geräten und digitalen Diensten. 2. Ein Zustand des persönlichen Wohlbefindens, der durch die gesunde Nutzung digitaler Technologie erfahren wird. 3. Digitales Wohlbefinden umfasst die Art und Weise, wie Informationstechnologie - einschließlich Kommunikation und Sensoren - den Menschen helfen kann, ein langes und gesundes Leben zu führen.

Digitale Kompetenz: Selbstbewusste, kritische und verantwortungsvolle Nutzung digitaler Technologien und der Umgang mit ihnen für das Lernen, die Arbeit und die Teilnahme an der Gesellschaft. Sie ist definiert als eine Kombination aus Wissen, Fähigkeiten und Einstellungen.

Digitale Fertigkeiten: Digitale Kompetenzen sind eine Reihe von Fähigkeiten zur Nutzung digitaler Geräte, Kommunikationsanwendungen und Netzwerke für den Zugang zu und die Verwaltung von Informationen. Sie ermöglichen es den Menschen, digitale Inhalte zu erstellen und zu teilen, zu kommunizieren und zusammenzuarbeiten und Probleme zu lösen, um sich im Leben, beim Lernen, bei der Arbeit und bei sozialen Aktivitäten effektiv und kreativ zu verwirklichen.

Digitale Abhängigkeit: Digitalsucht ist eine schädliche Abhängigkeit von digitalen Medien, Geräten und dem Internet, die durch eine übermäßige Nutzung gekennzeichnet ist, die sich negativ auf das Leben des Nutzers auswirkt.

Cyber-Bedrohung*:* Jeder Umstand oder jedes Ereignis, der/das das Potenzial hat, Organisationen/Personen durch unbefugten Zugriff, Zerstörung, Offenlegung, Änderung von Informationen und/oder Denial-of-Service nachteilig zu beeinflussen. Das Ziel ist es, Daten zu stehlen/beschädigen oder das digitale Wohlbefinden zu stören.

Cybermobbing*:* Ein Begriff für verschiedene Formen von Mobbing im Online-Raum, bei denen eine oder mehrere Personen die digitale Technologie nutzen, um eine andere Person absichtlich und wiederholt zu schädigen (z. B. durch das Versenden von E-Mails oder Sofortnachrichten, das Posten von Kommentaren in sozialen Netzwerken oder öffentlichen Foren).

Cybersecurity: Cybersicherheit ist ein Teilbereich der Informationssicherheit, dessen Ziel es ist, den Cyberspace (d. h. Netze, Intranets, Server, Informations- und Computersysteme und -infrastruktur) vor unbefugtem Zugriff, Cyberangriffen oder Schäden zu schützen. Die Cybersicherheit konzentriert sich auf den Schutz von Informationen in elektronischer/digitaler Form, die sich in Computern, Speichern und Netzen (im Cyberspace) befinden.

Digitaler Datenschutz: Unter digitaler Privatsphäre versteht man die Möglichkeit des Einzelnen, den Zugang und die Nutzung seiner persönlichen Daten beim Zugang zum Internet zu kontrollieren und zu schützen. Die digitale Privatsphäre hilft Einzelpersonen, online anonym zu bleiben, indem sie persönlich identifizierbare Informationen wie Namen, Adressen, Sozialversicherungsnummern, Kreditkartendaten usw. schützt.

Digitale Sicherheit vs. Cybersicherheit vs. Informationssicherheit*:* Informationssicherheit: Schutz von Informationen (in jedem Format und jeder Form) und Informationssystemen vor unbefugtem Zugriff und unbefugter Nutzung, um die Privatsphäre wichtiger Daten zu schützen und zu bewahren. Cybersicherheit: schützt ganze Netzwerke und Kommunikationssysteme, Computersysteme und andere digitale Komponenten sowie die darin gespeicherten digitalen Daten. Digitale Sicherheit: Schutz der Online-Präsenz (Identität und damit verbundene sensible Informationen, Vermögenswerte.

Bewährtes Verfahren*:* Eine bewährte Methode oder ein bewährtes Verfahren, das in einem bestimmten Bereich die effektivste Lösung bietet, die nachweislich zu optimalen Ergebnissen führt und als geeigneter Standard für eine breite Anwendung festgelegt (vorgeschlagen) wird. Im Bereich der digitalen Sicherheit sind dies definierte Verfahren, die den Schutz einer Person/Organisation im digitalen Raum gewährleisten (z. B. empfohlene Techniken, Programme, Anweisungen, Handbücher).

2 Digitales Wohlbefinden

2.1 Was ist Wohlbefinden?

Der Begriff "**Wohlbefinden**" beschreibt den Zustand, zufrieden, fröhlich und gesund zu sein. Er umfasst das körperliche, geistige und emotionale Wohlbefinden einer Person und andere Bereiche ihrer Existenz. Über das bloße Freisein von Krankheiten oder Beschwerden hinaus konzentriert sich das Wohlbefinden auf das allgemeine Glück und die Lebensqualität.

Körperliches Wohlbefinden ist der Zustand des eigenen Körpers, wobei Dinge wie körperliche Fitness, Ernährung und das Fehlen von Krankheiten berücksichtigt werden. Dazu gehört ein gesunder Lebensstil mit konsequenter Bewegung, nährstoffreicher Ernährung, ausreichend Schlaf und Stressbewältigung.

Die kognitive und emotionale Gesundheit einer Person steht im Zusammenhang mit ihrem **geistigen Wohlbefinden.** Dazu gehört, dass man eine gute Perspektive hat, Erfüllung erfährt und in der Lage ist, mit Stress und den Schwierigkeiten des Lebens umzugehen. Aktivitäten wie das Üben von Achtsamkeit, die Beschäftigung mit einem Hobby, das Bitten um Unterstützung durch nahestehende

Personen und die Inanspruchnahme professioneller Hilfe, wenn dies erforderlich ist, können dazu beitragen, das psychische Wohlbefinden eines Menschen zu fördern.

Ein gutes Verständnis für die eigenen Emotionen und die Fähigkeit, sie zu kontrollieren, wird als **emotionales Wohlbefinden** bezeichnet. Dazu gehört, dass man seine Widerstandsfähigkeit kultiviert, gute Beziehungen pflegt und ein positives Selbstwertgefühl hat. Selbsterkenntnis, emotionale Kontrolle, wirksame Kommunikation und die Entwicklung von unterstützenden Beziehungen tragen alle zum emotionalen Wohlbefinden bei.

Die Qualität der Beziehungen einer Person und das Gefühl der Zugehörigkeit zu einer Gemeinschaft sind allesamt Bestandteile des **sozialen Wohlbefindens**. Dazu gehört die Pflege dauerhafter Bindungen zu nahen Angehörigen, engen Freunden und einem größeren sozialen Netzwerk. Die Teilnahme an sozialen Aktivitäten, das Engagement für die Gemeinschaft und die Aufrechterhaltung eines Gefühls der Verbundenheit und Zugehörigkeit können das soziale Wohlbefinden verbessern.

Insgesamt ist das Wohlbefinden ein umfassendes Konzept, das die Wechselbeziehungen zwischen den verschiedenen Aspekten des Lebens einer Person berücksichtigt. Es beinhaltet das aktive Streben nach einer ausgewogenen und befriedigenden Existenz, die Pflege der körperlichen und geistigen Gesundheit, die Pflege gesunder Beziehungen und die Suche nach dem Sinn des eigenen Lebens.

2.2 Wohlbefinden und Digitalisierung

Technologie und Digitalisierung haben das Potenzial, das Wohlbefinden zu verbessern, indem sie Kommunikation ermöglichen, die Effizienz steigern und den Zugang zu Informationen verbessern. Um die digitale Nutzung zu steuern, die Privatsphäre und die Sicherheit zu schützen und ein gutes Gleichgewicht zwischen Technologie und anderen Lebensbereichen zu finden, ist es entscheidend, sich der möglichen Nachteile bewusst zu sein und die notwendigen Vorsichtsmaßnahmen zu treffen.

Technologie und Digitalisierung haben den Zugang zu Informationen und Dienstleistungen erheblich verbessert, was sich positiv auf das Wohlbefinden auswirkt. Die Menschen haben jetzt leichten Zugang zu digitalen Hilfsmitteln für die persönliche Entwicklung, zu Informationen über die Gesundheitsfürsorge, zu Online-Selbsthilfegruppen und zu Bildungsressourcen. Durch die nahtlose Kommunikation und die Verbindung über Entfernungen hinweg fördert die Technologie soziale Verbindungen und verringert das Gefühl der Einsamkeit. Dank digitaler Plattformen, sozialer Medien und Messaging-Anwendungen können die Menschen mit Freunden, Familie und Gemeinschaften in Kontakt bleiben, was das soziale Wohlbefinden verbessert. Viele Bereiche des Lebens sind dank der Digitalisierung effizienter und bequemer geworden. Durch den Einsatz digitaler Tools und Dienste können Aufgaben, die früher viel Zeit und Mühe erforderten, jetzt schnell und mühelos erledigt werden. Dies kann zum allgemeinen Wohlbefinden beitragen, indem es Zeit spart und Stress reduziert. Außerdem werden digitale Fähigkeiten mit der technologischen Entwicklung auf dem Arbeitsmarkt immer wichtiger. Die Beschäftigungsfähigkeit und das sozioökonomische Wohlergehen einer Person können durch den Erwerb und die Nutzung dieser Fähigkeiten verbessert werden. Die digitale Kluft, die entsteht, wenn einigen Menschen oder Gruppen der Zugang zur Technologie oder die digitale Kompetenz fehlt, kann jedoch bereits bestehende Ungleichheiten noch verschärfen.

Die unsachgemäße oder übermäßige Nutzung von Technologie kann sich zwar negativ auf die psychische Gesundheit auswirken, aber auch positive Effekte haben. Angstzustände, Verzweiflung und ein geringes Selbstwertgefühl können durch zu viel Bildschirmzeit, Vergleiche in sozialen Medien und Online-Missbrauch beeinflusst werden. Um die psychische Gesundheit zu schützen, ist es wichtig, ein gesundes

Gleichgewicht zu wahren und die Technologie achtsam zu nutzen. Die digitale Umgebung birgt auch einige Probleme in Bezug auf Datenschutz und Sicherheit. Cyber-Bedrohungen, Datenschutzverletzungen und Online-Betrug können die finanzielle Sicherheit und die persönlichen Daten der Menschen in Gefahr bringen. Um das allgemeine Wohlbefinden im digitalen Zeitalter aufrechtzuerhalten, müssen die digitale Sicherheit und die Privatsphäre geschützt werden.

2.3 Was ist digitales Wohlbefinden?

Die Entwicklung der digitalen Resilienz und die Annahme von Sicherheitsverfahren führen zu einem Zustand optimaler Gesundheit und allgemeinen Wohlbefindens in der digitalen Sphäre, der als digitales Wohlbefinden bezeichnet wird. Das digitale Wohlbefinden stammt aus dem Konzept des Wohlbefindens und hat mit dem digitalen Leben des Einzelnen zu tun. Die Fähigkeit der Menschen, sich in der digitalen Welt anzupassen, zurechtzukommen und zu gedeihen und dabei sowohl ihr Wohlbefinden als auch ihre Sicherheit erfolgreich zu managen, wird als digitale Resilienz bezeichnet, die eine Mischung aus digitalem Wohlbefinden und Sicherheit darstellt. Der Eckpfeiler der digitalen Resilienz ist das digitale Wohlbefinden, bei dem es darum geht, eine positive und sinnvolle Verbindung zur Technologie zu bewahren. Dazu gehört es, die Bildschirmzeit zu begrenzen, der geistigen und emotionalen Gesundheit einen hohen Stellenwert einzuräumen, unterstützende Online-Communities zu schaffen und digitale Kompetenz zu erlernen. Im Kontext des Wohlbefindens hilft die digitale Resilienz den Menschen, mit Online-Schwierigkeiten wie Cybermobbing, Online-Belästigung oder dem Kontakt mit gefährlichen Inhalten umzugehen und gleichzeitig ihr allgemeines Wohlbefinden zu bewahren. Durch die Integration von digitalem Wohlbefinden und digitaler Sicherheit können Einzelpersonen eine starke digitale Resilienz aufbauen, die es ihnen ermöglicht, sich sicher und verantwortungsbewusst in der digitalen Welt zu bewegen. Sie sind besser in der Lage, mit den Herausforderungen der digitalen Welt umzugehen, sich an wechselnde Gefahren anzupassen, kluge Entscheidungen zu treffen, ihre persönlichen Daten zu schützen und ihre geistige, emotionale und körperliche Gesundheit bei der Nutzung des Internets zu erhalten. Digitale Resilienz fördert letztendlich eine sicherere, gesündere und erfüllendere Online-Erfahrung für die Menschen.

2.3.1 Psychische Gesundheit, Wohlbefinden und digitales Wohlbefinden

Unsere gesamte Lebensqualität wird durch die enge Verbindung zwischen unserer psychischen Gesundheit und unserem allgemeinen Wohlbefinden beeinflusst. Unser psychologisches und emotionales Wohlbefinden, das Aspekte wie unsere Gedanken, Gefühle und Verhaltensweisen umfasst, wird als psychische Gesundheit bezeichnet. Sie ist für unsere gesamte Gesundheit von grundlegender Bedeutung, ebenso wichtig wie das körperliche Wohlbefinden. Im Gegensatz dazu ist Wohlbefinden ein umfassender Zustand des Gleichgewichts, der Erfüllung und der Zufriedenheit im Leben. Die Beziehung zwischen diesen beiden Begriffen beruht darauf, dass die geistige Gesundheit eines Menschen einen erheblichen Einfluss auf seine körperliche Gesundheit hat und umgekehrt. Unser gesamtes Wohlbefinden steigt, wenn wir eine positive geistige Gesundheit kultivieren, indem wir Stress kontrollieren, Hindernisse überwinden und gesunde Beziehungen aufbauen, was zu einem erfüllteren und sinnvolleren Leben führt. Auf der anderen Seite kann ein Gefühl des Wohlbefindens die psychische Gesundheit erheblich verbessern, indem es die Widerstandsfähigkeit, die emotionale Stabilität und die Fähigkeit, mit den Herausforderungen des Lebens umzugehen, stärkt. Wir können ein glückliches und erfolgreiches Leben führen, indem wir uns auf die Beziehung zwischen unserer geistigen Gesundheit und unserem Wohlbefinden konzentrieren.

Aufgrund der rasanten Verbesserungen in der Technologie und ihrer allgegenwärtigen Integration in unser tägliches Leben nimmt die psychische Gesundheit im digitalen Zeitalter einen komplexen und dynamischen Charakter an. Im Zusammenhang mit dem digitalen Zeitalter wird das geistige und emotionale Wohlbefinden einer Person als "digitale psychische Gesundheit" bezeichnet. Dazu gehören soziale Medien, Online-Interaktionen, die psychologischen Auswirkungen digitaler Technologien und die ständige Vernetzung, die das moderne Leben bestimmt. Obwohl die Technologie viele Vorteile und Möglichkeiten geschaffen hat, hat sie auch erhebliche Schwierigkeiten für die psychische Gesundheit mit sich gebracht. Trotz des ständigen virtuellen Kontakts kann das digitale Zeitalter zu Problemen wie Internetsucht, Cybermobbing, Informationsüberlastung, sozialem Vergleich und Gefühlen der Isolation führen. Es bietet jedoch auch innovative Ansätze für den Umgang mit der psychischen Gesundheit, wie z. B. Anwendungen für die psychische Gesundheit, Online-Therapie und virtuelle Selbsthilfegruppen. Ein gesundes Gleichgewicht zwischen unserem Online- und Offline-Leben aufrechtzuerhalten, sich bewusst zu machen, wie viel digitale Medien wir konsumieren, und aktiv nach digitalen Werkzeugen zu suchen, die unser psychisches Wohlbefinden verbessern können, während wir uns gleichzeitig vor potenziellen Fallen hüten, ist unerlässlich, wenn wir die Feinheiten des digitalen Zeitalters durchqueren.

In der heutigen Zeit besteht eine komplexe Beziehung zwischen psychischer Gesundheit und digitalem Wohlbefinden. Das psychologische und emotionale Wohlbefinden des Einzelnen, das Faktoren wie Stimmung, Gedanken, Gefühle und Verhalten umfasst, wird als psychische Gesundheit bezeichnet. Das digitale Wohlbefinden hingegen beschreibt das Gleichgewicht und die Harmonie, die man bei der Nutzung von Technologie und der Pflege digitaler Beziehungen empfindet. Das digitale Zeitalter hat viele Vorteile: Es ermöglicht Konnektivität, Zugang zu Informationen und Chancen für die persönliche Entwicklung. Die übermäßige Nutzung der Technologie, ständige Benachrichtigungen, der Druck der sozialen Medien und die Informationsflut können sich jedoch negativ auf die psychische Gesundheit auswirken, indem sie Spannungen, Sorgen und ein Gefühl der Trennung von der Realität verursachen. Andererseits kann es sich positiv auf die psychische Gesundheit auswirken, wenn dem digitalen Wohlbefinden Vorrang eingeräumt wird, indem man Grenzen setzt, regelmäßige Pausen von Bildschirmen einlegt und auf den digitalen Konsum achtet. Um sowohl die psychische Gesundheit als auch das digitale Wohlbefinden zu fördern und ein harmonisches Nebeneinander von virtuellem und realem Leben zu gewährleisten, ist es wichtig, ein gesundes Gleichgewicht zwischen digitalem Engagement und Offline-Aktivitäten herzustellen. Ein sinnvolleres und ausgewogeneres Leben im digitalen Zeitalter kann erreicht werden, indem man sich bewusst mit der Technologie auseinandersetzt und digitale Werkzeuge zur Verbesserung der psychischen Gesundheit einsetzt.

2.3.2 Warum brauchen wir digitales Wohlbefinden?

Die wichtigsten Faktoren des digitalen Wohlbefindens sind Lebensqualität, Kommunikation, Produktivität und Erfolg sowie geistige und körperliche Gesundheit. Das digitale Wohlbefinden ist wichtig, weil es den gesamten Zustand der Gesundheit, des Glücks und der Zufriedenheit eines Menschen umfasst. Es bezieht sich auf die allgemeine Gesundheit von Menschen und Gemeinschaften unter Berücksichtigung ihrer sozialen, psychologischen und physischen Aspekte. Die übermäßige oder ungesunde Nutzung von Mobiltelefonen, sozialen Medien und Videospielen kann sich negativ auf die psychische Gesundheit auswirken. Ängste, Verzweiflung, Einsamkeit und ein geringes Selbstwertgefühl können durch übermäßige Bildschirmzeit, häufige Vergleiche mit anderen in den sozialen Medien oder Cybermobbing noch verstärkt werden. In dieser Hinsicht ist digitales Wohlbefinden der Weg, um die Kontrolle über unser eigenes Leben zu behalten. Ein gesunder Umgang mit der Technologie ist für die psychische Gesundheit und das digitale Wohlbefinden von entscheidender Bedeutung. Dazu kann es gehören, die Nutzung von Geräten

einzuschränken, digitale Entgiftungsprogramme durchzuführen, an Offline-Aktivitäten teilzunehmen und der Selbstfürsorge und persönlichen Kontakten höchste Priorität einzuräumen. Wir müssen uns der Auswirkungen der digitalen Technologie auf unsere psychische Gesundheit bewusst sein und proaktive Maßnahmen ergreifen, um ihre sinnvolle Nutzung sicherzustellen.

Digitales Wohlbefinden ist im digitalen Zeitalter zu einem grundlegenden Bedürfnis der Menschen geworden, insbesondere im Zuge der Covid-19-Pandemie. Unsere Abhängigkeit von digitalen Plattformen hat zugenommen, da die Technologie weiterhin in jeden Bereich unseres täglichen Lebens eindringt, von der Kommunikation und Bildung bis hin zu Beschäftigung und Unterhaltung. Die Epidemie hat dazu geführt, dass die Digitalisierung in einem noch nie dagewesenen Tempo voranschreitet, was Fernarbeit, Online-Schulbildung und mehr virtuelle Beziehungen erfordert. Daher ist die Aufrechterhaltung unseres digitalen Wohlbefindens entscheidend für ein erfülltes und gesundes Leben. Wir können die Technologie gewissenhaft und verantwortungsbewusst nutzen, um sicherzustellen, dass sie unser Leben verbessert und nicht eine Bedrohung für unser allgemeines Wohlbefinden in diesem sich schnell verändernden digitalen Umfeld darstellt, indem wir das digitale Wohlbefinden als ein grundlegendes menschliches Bedürfnis anerkennen.

2.3.3 Gutes und schlechtes digitales Wohlbefinden

Digitales Wohlbefinden ist ein umfassender Begriff, der eine Vielzahl von Aspekten der digitalen Welt abdeckt. Er bezieht sich sowohl auf die physische, psychische und soziale Gesundheit des Einzelnen als auch auf sein digitales Bewusstsein, sein Gleichgewicht, seine Sicherheit, seine Zufriedenheit und seine Gesundheit auf der anderen Seite. Wie man sieht, ist die Bedeutung, die dem Begriff "digitales Wohlbefinden" zugeschrieben wird, meist auf die positive Seite der Digitalisierung gerichtet, die sich auf ein gutes digitales Wohlbefinden bezieht. Umgekehrt bedeutet ein Mangel an digitalem Wohlbefinden für die Betroffenen ein schlechtes digitales Wohlbefinden. In Anbetracht dessen könnten die folgenden Aspekte als Hauptindikatoren für ein gutes digitales Wohlbefinden gelten:

- Digitale Sicherheit: Die Gewährleistung der digitalen Sicherheit leistet einen bemerkenswerten Beitrag zum digitalen Wohlbefinden. Sie umfasst den Schutz Ihrer Online-Präsenz einschließlich Ihrer Identität, Ihrer Daten und Ihres Vermögens.
- Digitale Sicherheit: Dazu gehört, dass man sich potenzieller Risiken in der digitalen Welt bewusst ist und dass man in der Lage ist, verschiedene Bedrohungen im digitalen Umfeld kritisch zu erkennen und zu bewältigen.
- Digitales Gleichgewicht: Sie bezieht sich auf die gezielte Nutzung von Technologie und der digitalen Welt. Digitales Gleichgewicht hat damit zu tun, dass man die digitale Welt, die digitalen Werkzeuge und Geräte für bestimmte Lebensbereiche und nicht für alles nutzt. Ein regelmäßiges und konsistentes Online-/Offline-Gleichgewicht und die Vermeidung einer starken Abhängigkeit von der Technologie sind Zeichen für ein gutes digitales Gleichgewicht.
- Digitale Unabhängigkeit: Das ist die Fähigkeit, die Zeit, die man online verbringt, zu kontrollieren und zu vermeiden, dass man die digitale Welt in den Mittelpunkt seines täglichen Lebens stellt. Zu viel Zeit online zu verbringen und weniger soziale Aktivitäten zu planen, weil man das Internet übermäßig nutzt, sind einige Anzeichen für digitale Abhängigkeit.
- Digitale Zufriedenheit: Sie bezieht sich auf das Erreichen von Zufriedenheit und das Empfinden von Vergnügen bei der Nutzung digitaler Werkzeuge und Geräte und der Verflechtung mit der Technologie.

- Digitale Möglichkeiten: Es geht darum, von der Technologie und der Digitalisierung zu profitieren, um neue Möglichkeiten im Zusammenhang mit der Verbreitung digitaler Technologien zu erschließen und neue Kompetenzen zu erwerben, um neue Chancen aufzubauen.
- Kritischer und verantwortungsvoller Umgang mit der Technologie: Neben den Möglichkeiten, die die Technologie bietet, müssen die Nutzer verantwortungsbewusst handeln, indem sie ihre eigenen Rechte schützen und die Rechte anderer respektieren, verantwortungsbewusst und vorsichtig handeln und kritisch gegenüber allen Inhalten in der digitalen Welt denken.

Diese Aspekte könnten auch zu den Dimensionen des digitalen Wohlbefindens gezählt werden. Wenn jemand bei der Nutzung digitaler Werkzeuge und Geräte ein relativ hohes Maß an digitaler Sicherheit, Ausgewogenheit, Unabhängigkeit, Zufriedenheit, Chancen und/oder kritischem und verantwortungsvollem Umgang mit der Technologie hat oder gewährleistet, könnte man von einem guten digitalen Wohlbefinden sprechen. Fehlen hingegen einige der oben genannten Komponenten, bedeutet dies, dass das digitale Wohlbefinden schlecht ist. Es sei daran erinnert, dass die physische, psychische und soziale Gesundheit einer Person auch auf ein gutes digitales Wohlbefinden hinweist und dass weitere Aspekte einen potenziellen Beitrag zum digitalen Wohlbefinden und zum allgemeinen Wohlbefinden des Einzelnen leisten.

2.3.4 Förderung des digitalen Wohlbefindens von Einzelpersonen: Potenzieller Nutzen für alle und für die Erwachsenenbildung

Die Förderung des digitalen Wohlbefindens in der Erwachsenenbildung oder die Stärkung des Wohlbefindens von Erwachsenen und des digitalen Wohlbefindens bietet viele Möglichkeiten. In erster Linie ist das Wohlbefinden ein menschliches Grundbedürfnis. Vor allem nach COVID-19 verbringen die meisten Menschen viel mehr Zeit online und sind der Technologie und ihren Risiken und Bedrohungen stärker ausgesetzt. Ob die Menschen es wollen oder nicht, sie bringen sich voll und ganz in die Arbeit ein, d. h. es besteht ein eindeutiger Zusammenhang zwischen dem eigenen Wohlbefinden und der Atmosphäre im Arbeitsumfeld. Die potenziellen Maßnahmen zur Förderung des Wohlbefindens und des digitalen Wohlbefindens des Einzelnen tragen also sowohl zu ihm als Mensch als auch zu dem Unternehmen bei, für das er arbeitet. Aus organisatorischer Sicht trägt die Förderung des digitalen Wohlbefindens der Arbeitnehmer zu Teamleistung, Engagement, Innovation und Zufriedenheit bei, ist aber nicht darauf beschränkt. Digitales Wohlbefinden ermöglicht es dem Einzelnen, konzentrierter, engagierter und produktiver zu sein, was zu einem gesünderen Leben sowohl innerhalb als auch außerhalb des Arbeitsumfelds beiträgt. Wenn die Mitarbeiter digitale Wellness-Praktiken anwenden, sind sie weniger erschöpft und abgelenkt. Die Förderung von Maßnahmen zur Unterstützung des digitalen Wohlbefindens stärkt die Work-Life-Balance des Einzelnen. Darüber hinaus werden die negativen Auswirkungen einer übermäßigen Belastung durch die Digitalisierung beseitigt, so dass weniger Ängste, Verzweiflung, Stress usw. auftreten können.

Das Konzept des Wohlbefindens im Kontext der Erwachsenenbildung geht über die herkömmlichen Vorstellungen von akademischen Leistungen hinaus und umfasst auch die allgemeine Gesundheit und Zufriedenheit der Studierenden. Das Konzept des "digitalen Wohlbefindens" hat mit dem Aufkommen des digitalen Zeitalters an Bedeutung gewonnen, insbesondere für digitale Nomaden, die in ihrem mobilen Lebensstil weitgehend auf Technologie angewiesen sind. In der Erwachsenenbildung bezieht sich der Begriff "digitales Wohlbefinden" darauf, den Schülern die Fähigkeiten und Informationen zu vermitteln, die sie für eine sinnvolle und ethisch vertretbare Nutzung des Internets benötigen. Die

Förderung des digitalen Wohlbefindens ist für die Schaffung eines erfolgreichen Lernumfelds von entscheidender Bedeutung, da digitale Nomaden häufig mit besonderen Schwierigkeiten konfrontiert sind, wie z. B. der Vereinbarkeit von Privat- und Berufsleben und der Überwindung von Gefühlen der Einsamkeit. Die Integration des digitalen Wohlbefindens in die Erwachsenenbildung bedeutet, dass den Schülern beigebracht wird, wie sie ihre Bildschirmzeit richtig kontrollieren, positive Online-Gemeinschaften aufbauen und sich ihrer digitalen Nutzung bewusst bleiben können. Außerdem geht es um Themen wie Cybersicherheit, digitale Müdigkeit und Datenschutz. In der heutigen digital geprägten Welt können Pädagogen eine positive und bereichernde Lernerfahrung gewährleisten, indem sie den offensichtlichen Bedarf an digitalem Wohlbefinden in der Erwachsenenbildung aufgreifen und digitalen Nomaden und anderen Lernenden die Werkzeuge an die Hand geben, um ein gesundes Gleichgewicht zwischen ihren digitalen Interaktionen und ihrem allgemeinen Wohlbefinden zu wahren.

Es bedarf einer sorgfältigen und gründlichen Strategie, um das digitale Wohlbefinden erfolgreich in die Erwachsenenbildung zu integrieren, da es sich um einen komplizierten und kontinuierlichen Prozess handelt. Der erste und wichtigste Schritt besteht darin, erwachsene Lernende zu schulen, damit sie sich des Wertes des digitalen Wohlbefindens bewusst sind und wissen, wie es sich auf ihre allgemeine Gesundheit und Produktivität auswirkt. Dank dieser Schulung erwerben sie die notwendigen praktischen Fähigkeiten, um sich in der digitalen Welt vernünftig und sicher zu bewegen. Der zweite Schritt besteht darin, das Kursmaterial so anzupassen, dass der Lehrplan die Konzepte des digitalen Wohlbefindens widerspiegelt. Dies bedeutet, dass Ideen wie die Kontrolle digitaler Ablenkungen, der Schutz der Online-Privatsphäre, die digitale Etikette und die digitale Kompetenz einbezogen werden. Durch die Einbeziehung dieser Aspekte in die Kurse können erwachsene Lernende ein besseres Verständnis für die Vor- und Nachteile der Technologie entwickeln und lernen, sie effektiv zu nutzen. Es wird ein unterstützendes Umfeld geschaffen, in dem die Lernenden ihre Erfahrungen austauschen, sich über Techniken informieren und ihr Engagement für digitales Wohlbefinden bekräftigen können, indem zusätzliche Veranstaltungen zur Stärkung der Handlungskompetenz, wie Seminare und Gespräche, konzipiert werden. Um das Wohlbefinden im digitalen Zeitalter relevant und effektiv zu fördern, muss sich die Erwachsenenbildung kontinuierlich weiterentwickeln, um mit der sich schnell verändernden digitalen Landschaft Schritt halten zu können.

3 Digitale Sicherheit

3.1 Digitale Sicherheit und Cybersecurity

Nach Ansicht der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist die **digitale Sicherheit** eine wesentliche Voraussetzung für das Vertrauen im digitalen Zeitalter. Seit den frühen 1990er Jahren fördert die OECD die internationale Zusammenarbeit und entwickelt politische Analysen und Empfehlungen zur digitalen Sicherheit. Die Arbeit in diesem Bereich zielt darauf ab, Strategien zu entwickeln und zu fördern, die das Vertrauen stärken, ohne das Potenzial der Informations- und Kommunikationstechnologien (IKT) zur Förderung von Innovation, Wettbewerbsfähigkeit und Wachstum zu beeinträchtigen. Die digitale Sicherheit bezieht sich auf die wirtschaftlichen und sozialen Aspekte der Cybersicherheit, im Gegensatz zu den rein technischen Aspekten und den Aspekten, die mit der Strafverfolgung oder der nationalen und internationalen Sicherheit zusammenhängen. Der Begriff "digital" steht im Einklang mit Begriffen wie digitale Wirtschaft, digitale Transformation und digitale Technologien.

Er bildet die Grundlage für einen konstruktiven internationalen Dialog zwischen den Akteuren, die das Vertrauen fördern und die Chancen der IKT maximieren wollen.[1]

Digitale Sicherheit und **Cybersicherheit** sind zwar miteinander verwandt, aber nicht dasselbe. Bei beiden geht es um den Schutz digitaler Werte und Informationen vor unbefugtem Zugriff, Verwendung oder Beschädigung, aber sie unterscheiden sich in Umfang und Schwerpunkt.

Digitale Sicherheit bezieht sich auf die Praxis des Schutzes digitaler Daten, Informationen und Vermögenswerte vor unbefugtem Zugriff, Diebstahl oder Beschädigung. Sie umfasst ein breiteres Spektrum an Sicherheitsmaßnahmen zum Schutz von Daten und Informationen auf verschiedenen digitalen Plattformen und Geräten, darunter Computer, Smartphones, Tablets und andere digitale Technologien.

Zu den digitalen Sicherheitsmaßnahmen können gehören:

- Passwortschutz: Erstellung sicherer und eindeutiger Passwörter für Online-Konten und Geräte.
- Datenverschlüsselung: Verschlüsselung von Daten, um unbefugten Zugriff oder Datenverletzungen zu verhindern.
- Sichere Kommunikation: Verwendung von Verschlüsselungsprotokollen für eine sichere Datenübertragung.
- Zugriffskontrollen: Implementierung von Berechtigungen und Einschränkungen, um den Zugriff auf sensible Daten zu begrenzen.
- Gerätesicherheit: Verwendung von Funktionen wie Bildschirmsperren und Fernlöschung bei verlorenen oder gestohlenen Geräten.

Cybersicherheit ist ein Teilbereich der digitalen Sicherheit und konzentriert sich speziell auf den Schutz digitaler Werte vor Cyber-Bedrohungen und -Angriffen. Sie umfasst die Verteidigung gegen unbefugten Zugriff, Beschädigung oder Störung digitaler Systeme, Netzwerke und Infrastrukturen.

Zu den Maßnahmen der Cybersicherheit können gehören:

- Firewall-Schutz: Einrichtung von Barrieren, die den unbefugten Zugang zu einem Netz verhindern.
- Systeme zur Erkennung von Eindringlingen: Überwachung von Netzwerken auf verdächtige Aktivitäten und potenzielle Bedrohungen.
- Schutz vor Malware: Einsatz von Antiviren-Software zur Erkennung und Entfernung von Schadsoftware.
- Planung der Reaktion auf Vorfälle: Entwicklung von Protokollen zur wirksamen Reaktion auf Cybersicherheitsvorfälle.
- Aufklärung über Cyber-Bedrohungen: Sammeln und Analysieren von Informationen, um Cyber-Bedrohungen vorherzusehen und zu verhindern.

Digitale Sicherheit umfasst ein breiteres Spektrum von Verfahren zum Schutz von Daten und Informationen im digitalen Bereich, während Cybersicherheit ein Spezialgebiet ist, das sich auf die Abwehr von Cyber-Bedrohungen und -Angriffen in digitalen Systemen und Netzen konzentriert. Beide Bereiche sind

[1] HTTPS://WWW.OECD.ORG/DIGITAL/DIGITAL-SECURITY/

von entscheidender Bedeutung für die Gewährleistung der allgemeinen Sicherheit und des Schutzes digitaler Werte und Informationen.

3.2 Cybersecurity-Bedrohungen für Erwachsene

Erwachsene sind in der heutigen digitalen Welt einer Vielzahl von Cybersicherheitsbedrohungen ausgesetzt. Hier sind einige häufige Cybersicherheitsbedrohungen, denen Erwachsene häufig ausgesetzt sind:

- **Phishing-Angriffe:** Phishing ist eine Technik, die von Cyberkriminellen eingesetzt wird, um Personen dazu zu bringen, vertrauliche Informationen wie Anmeldeinformationen, Kreditkartennummern oder persönliche Daten preiszugeben. Phishing-E-Mails, Nachrichten oder Websites können den Anschein erwecken, von vertrauenswürdigen Quellen zu stammen, zielen aber darauf ab, die Benutzer zur Preisgabe ihrer Daten zu verleiten.
- **Malware:** Malware ist bösartige Software, die darauf abzielt, Computersysteme zu infiltrieren, zu beschädigen oder sich unbefugten Zugang zu ihnen zu verschaffen. Zu den Arten von Malware gehören Viren, Ransomware, Spyware und Trojaner. Malware kann durch bösartige E-Mail-Anhänge, infizierte Websites oder kompromittierte Software verbreitet werden.
- **Identitätsdiebstahl:** Cyberkriminelle können persönliche Informationen wie Sozialversicherungsnummern, Geburtsdaten oder Finanzdaten stehlen, um Identitätsdiebstahl zu begehen. Diese Informationen werden häufig durch Datenschutzverletzungen oder Phishing-Versuche erlangt.
- **Online-Betrügereien:** Es gibt zahlreiche Online-Betrügereien, die auf Erwachsene abzielen, wie z. B. Lotterie-Betrügereien, Romantik-Betrügereien, gefälschte technische Support-Betrügereien und betrügerische Investitionspläne. Die Betrüger verwenden verschiedene Taktiken, um Personen dazu zu bringen, Geld zu überweisen oder persönliche Daten preiszugeben.
- **Datenschutzverletzungen:** Datenschutzverletzungen treten auf, wenn sensible Informationen von Unternehmen oder Organisationen offengelegt oder gestohlen werden. Als Erwachsener können Sie von Datenschutzverletzungen betroffen sein, wenn Ihre persönlichen Daten bei den betroffenen Unternehmen gespeichert sind.
- **Social Engineering:** Beim Social Engineering werden Personen dazu gebracht, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen. Cyberkriminelle können Social-Engineering-Techniken einsetzen, um sich unbefugten Zugang zu Systemen oder Konten zu verschaffen.
- **Passwort-Angriffe:** Schwache Passwörter oder die Wiederverwendung von Passwörtern können zu Passwortangriffen wie Brute-Force- oder Wörterbuchangriffen führen, bei denen Cyberkriminelle versuchen, Passwörter zu erraten oder zu knacken, um unbefugten Zugang zu erhalten.
- **Öffentliche Wi-Fi-Risiken:** Die Nutzung öffentlicher Wi-Fi-Netzwerke kann Erwachsene Sicherheitsrisiken aussetzen, da diese Netzwerke möglicherweise nicht richtig verschlüsselt sind und von Angreifern abgehört werden können.
- **Insider-Bedrohungen:** Bei Insider-Bedrohungen handelt es sich um Mitarbeiter oder Personen mit autorisiertem Zugang zu Systemen oder Daten, die absichtlich oder unabsichtlich Schaden anrichten oder sensible Informationen weitergeben.

- **IoT-Schwachstellen:** Die zunehmende Verbreitung von Geräten aus dem Internet der Dinge (IoT) kann Risiken für die Cybersicherheit mit sich bringen, da viele dieser Geräte unzureichende Sicherheitsmaßnahmen aufweisen und von Cyberkriminellen ausgenutzt werden können.

Um sich vor diesen Bedrohungen zu schützen, sollten Erwachsene eine gute Cybersicherheitshygiene praktizieren, z. B. sichere und eindeutige Passwörter verwenden, eine Multi-Faktor-Authentifizierung aktivieren, Software und Geräte auf dem neuesten Stand halten, bei verdächtigen E-Mails und Links Vorsicht walten lassen und darauf achten, welche Informationen sie online weitergeben. Regelmäßige Schulungen zum Thema Cybersicherheit können auch dazu beitragen, dass Einzelpersonen über neue Bedrohungen und bewährte Verfahren für einen sicheren Online-Auftritt informiert bleiben. Im nächsten Abschnitt werden einige der wichtigsten digitalen Sicherheitspraktiken für Erwachsene im Detail vorgestellt, um das Risiko zu verringern, Opfer von Cybersicherheitsbedrohungen zu werden und ihre digitalen Identitäten und Vermögenswerte zu schützen.

3.3 Digitale Sicherheitsmaßnahmen für Erwachsene

Digitale Sicherheitspraktiken sind für Erwachsene unerlässlich, um ihre persönlichen Informationen, Daten und Online-Konten vor Bedrohungen der Cybersicherheit zu schützen. Hier sind einige wichtige digitale Sicherheitspraktiken, die Erwachsene befolgen sollten:

- **Verwenden Sie sichere und eindeutige Passwörter**: Erwachsene sollten sichere und eindeutige Passwörter für ihre Online-Konten erstellen. Vermeiden Sie leicht zu erratende Passwörter wie "123456" oder "password". Erwägen Sie die Verwendung eines Passwortmanagers, um komplexe Passwörter zu erstellen und sicher zu speichern.
- **Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA):** Aktivieren Sie, wann immer möglich, die Multi-Faktor-Authentifizierung für Ihre Online-Konten. MFA bietet eine zusätzliche Sicherheitsebene, indem es zusätzlich zu Ihrem Passwort eine zweite Form der Verifizierung verlangt, z. B. einen einmaligen Code, der an Ihr Mobilgerät gesendet wird.
- **Halten Sie Software und Geräte auf dem neuesten Stand**: Aktualisieren Sie regelmäßig Ihr Betriebssystem, Ihre Webbrowser und Softwareanwendungen. Die Updates enthalten oft Sicherheits-Patches, die bekannte Schwachstellen beheben.
- **Seien Sie vorsichtig mit E-Mails und Links:** Seien Sie vorsichtig, wenn Sie E-Mails von unbekannten Absendern öffnen oder auf verdächtige Links klicken. Seien Sie besonders vorsichtig bei E-Mails, die nach vertraulichen Informationen fragen oder Sie auffordern, sich auf einer gefälschten Website anzumelden.
- **Sichern Sie Ihr Heimnetzwerk:** Ändern Sie das Standardpasswort Ihres Wi-Fi-Routers zu Hause und aktivieren Sie die WPA2- oder WPA3-Verschlüsselung, um Ihr drahtloses Netzwerk zu schützen. Vermeiden Sie die Nutzung öffentlicher Wi-Fi-Netzwerke für sensible Aktivitäten, es sei denn, Sie verwenden ein virtuelles privates Netzwerk (VPN).
- **Sichern Sie regelmäßig Ihre Daten:** Erstellen Sie regelmäßig Sicherungskopien Ihrer wichtigen Dateien und Daten auf einer externen Festplatte, in einem Cloud-Speicher oder bei einem sicheren Backup-Dienst. Im Falle eines Datenverlusts oder eines Ransomware-Angriffs können Sie mit Hilfe von Sicherungskopien Ihre Dateien wiederherstellen.

- **Verwenden Sie sicheres WLAN und HTTPS:** Wenn Sie auf sensible Websites zugreifen, achten Sie darauf, dass sie HTTPS-Verschlüsselung verwenden. Achten Sie auf das Vorhängeschloss-Symbol in der Adressleiste des Browsers, um die Sicherheit der Website zu überprüfen.
- **Seien Sie achtsam in sozialen Medien:** Seien Sie vorsichtig mit den Informationen, die Sie auf Social-Media-Plattformen teilen. Vermeiden Sie es, persönliche Daten wie Ihre Adresse, Telefonnummer oder Reisepläne zu veröffentlichen, da diese Informationen für Social-Engineering-Angriffe verwendet werden können.
- **Installieren Sie Antiviren- und Sicherheitssoftware:** Verwenden Sie auf Ihren Geräten seriöse Antiviren- und Sicherheitssoftware, um sich vor Malware und anderen Bedrohungen zu schützen. Halten Sie die Software auf dem neuesten Stand, um optimalen Schutz zu gewährleisten.
- **Informieren Sie sich über Cybersecurity:** Informieren Sie sich über die neuesten Bedrohungen der Cybersicherheit und bewährte Verfahren, indem Sie seriöse Quellen lesen, Webinare besuchen oder an Programmen zur Sensibilisierung für Cybersicherheit teilnehmen (siehe die für Erwachsene verfügbaren Ressourcen zur digitalen Sicherheit).

Indem sie diese digitalen Sicherheitspraktiken in ihre tägliche Routine integrieren, können Erwachsene das Risiko, Opfer von Cybersecurity-Bedrohungen zu werden, erheblich verringern und ihre digitalen Identitäten und Vermögenswerte schützen.

3.4 Digitale Sicherheits-Ressourcen für Erwachsene

Das Cybersecurity Education Hub[2] (CEH) an der California State University San Marcos bietet Ressourcen und Orientierungshilfen für die Bemühungen des Campus und der Gemeinschaft, die Aufklärung und das Bewusstsein für digitale Sicherheit zu verbessern. Das CEH ist eine gemeinsame Anstrengung des Informationssicherheitsbüros der Universität, des Colleges of Science and Math und des Colleges of Business Administration.

Das CEH setzt sich dafür ein, dass die Bildungsprogramme zur digitalen Sicherheit auf dem Campus breit gefächerte Themen im Zusammenhang mit aktuellen Ereignissen auf dem Gebiet der digitalen Sicherheit ansprechen, und es bietet die Möglichkeit, Themen der digitalen Sicherheit in Lehrveranstaltungen an der gesamten Universität zu integrieren. Das CEH bietet auch Ressourcen für Studenten, Studentenorganisationen und die Öffentlichkeit an. Es fördert und erleichtert die Kommunikation und Zusammenarbeit im Bereich der digitalen Sicherheit in der gesamten Gemeinschaft. Das CEH hat Lernmaterialien zu Themen wie Datenschutz und soziale Medien, Cybersicherheit für Studenten, Cybersicherheit heute und Cybersicherheitskonzepte bereitgestellt.

Außerdem wurde 2008 das ENISA[3] Schulungsmaterial für Cybersicherheit eingeführt. Es wurde seitdem um neue Abschnitte erweitert, die wichtige Informationen für den Erfolg im Bereich der Cybersicherheit enthalten. ENISA enthält Schulungsmaterialien wie Lehrerhandbücher, Schüler-Toolkits und virtuelle Bilder zur Ergänzung praktischer Schulungen.

[2] https://www.csusm.edu/cybersec-hub/index.html

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

4. Bewährte Verfahren beim Aufbau digitaler Sicherheit für Erwachsene

Die digitale Sicherheit wird in unserer vernetzten Gesellschaft immer wichtiger, und ältere Menschen gehören zu den am meisten gefährdeten Gruppen im Internet. Mit dem technologischen Fortschritt nehmen auch die Cyber-Bedrohungen zu. Daher ist es wichtig, Maßnahmen und Leitlinien zum Schutz älterer Erwachsener im digitalen Umfeld festzulegen. Im Folgenden werden einige bewährte Verfahren und erfolgreiche Maßnahmen vorgestellt, die in mehreren Ländern umgesetzt wurden und als Referenz für andere dienen können.

Die Berichte zur Cybersicherheitsstrategie der Europäischen Union sind alle auf der offiziellen Website der Europäischen Kommission abrufbar und bieten wertvolle Einblicke in bewährte Verfahren zur Verbesserung der digitalen Sicherheit in Europa.

4.1. Schlüsselaspekte für die digitale Sicherheit

Dieser Abschnitt mag wie eine Wiederholung von Abschnitt 3.3. Digitale Sicherheitspraktiken für Erwachsene, aber er enthält mehr praxisnahe Szenarien und Beispiele.

Sichere Passwörter: Helfen Sie ihnen, sichere und eindeutige Passwörter für jedes Konto zu erstellen. Passwörter müssen lang sein und Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Passwörter müssen lang sein (mindestens 8 Zeichen), Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Vermeiden Sie die Verwendung von vorhersehbaren persönlichen Informationen wie Namen oder Geburtsdaten. Erinnern Sie sie daran, ihre Passwörter nicht weiterzugeben und sie regelmäßig zu ändern.

Ein sicheres Passwort könnte zum Beispiel "P@ssw0rd2023!" sein, das Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen kombiniert. Vermeiden Sie die Verwendung vorhersehbarer persönlicher Daten wie Namen oder Geburtsdaten, z. B. "John1980" oder "MarySmith123".

Aufklärung und Bewusstseinsbildung: Informieren Sie sie über Online-Risiken und -Bedrohungen wie Phishing, Malware und Identitätsdiebstahl. Helfen Sie ihnen zu verstehen, wie sie diese Situationen erkennen und vermeiden können. Es ist wichtig, sie über Online-Risiken wie Phishing (Versuche, auf betrügerische Weise an vertrauliche Informationen zu gelangen), Malware (Schadprogramme) und Identitätsdiebstahl aufzuklären. Lernen Sie, diese Warnzeichen zu erkennen und zu vermeiden, in diese Fallen zu tappen. Erklären Sie mögliche negative Auswirkungen und wie Sie sich schützen können.

Erklären Sie z. B., dass Phishing-E-Mails den Anschein erwecken können, von seriösen Quellen zu stammen, und sie auffordern, auf Links zu klicken und vertrauliche Informationen einzugeben. Zeigen Sie ihnen Beispiele für verdächtige E-Mails und wie sie diese erkennen können. Informieren Sie sie über gängige Arten von Malware, wie z. B. gefälschte Antiviren-Software oder Pop-ups, und wie man sie vermeiden kann.

Zwei-Faktoren-Authentifizierung (2FA): Helfen Sie ihnen, wann immer möglich, die Zwei-Faktor-Authentifizierung zu implementieren. Dadurch wird eine zusätzliche Sicherheitsebene für Ihre Konten

geschaffen. Die Zwei-Faktor-Authentifizierung bietet eine zusätzliche Sicherheitsebene. Helfen Sie ihnen, diese Funktion in ihren Konten zu aktivieren, wenn möglich. Die 2FA erfordert zusätzlich zum Standardpasswort eine weitere Authentifizierungsmethode, z. B. einen SMS-Code, einen Authentifikator oder einen Fingerabdruck.

Nach der Eingabe des Kennworts erhalten sie beispielsweise eine SMS mit einem Verifizierungscode, den sie eingeben müssen, um auf ihr Konto zuzugreifen. Dies bietet eine zusätzliche Sicherheitsebene und erschwert unbefugten Nutzern den Zugang zu ihren Konten.

Sichere Nutzung von Mobilgeräten: Helfen Sie ihnen, Bildschirmsperren, Gesichtserkennung oder Fingerabdrücke einzurichten, um ihre mobilen Geräte zu schützen. Erinnern Sie sie daran, ihre Geräte nicht mit Personen zu teilen, die sie nicht kennen, und beim Herunterladen von Apps aus unzuverlässigen Quellen vorsichtig zu sein.

Zeigen Sie ihnen beispielsweise, wie sie eine PIN aktivieren oder ihren Fingerabdruck zum Entsperren ihres Smartphones verwenden können. Erinnern Sie sie daran, ihre Geräte nicht mit Personen zu teilen, die sie nicht kennen, und beim Herunterladen von Apps aus unzuverlässigen Quellen vorsichtig zu sein.

Software-Updates: Stellen Sie sicher, dass auf Ihren Geräten (Computer, Tablets, Smartphones) die neuesten Sicherheitspatches und Updates installiert sind. Aktualisierungen enthalten häufig Korrekturen für bekannte Sicherheitslücken, so dass Sie Ihre Geräte auf dem neuesten Stand halten können.

Online-Einkauf: Erinnern Sie sie daran, nur auf zuverlässigen und sicheren Websites einzukaufen und sichere Zahlungsmethoden zu verwenden. Bringen Sie ihnen bei, auf ein Schloss in der Adressleiste zu achten und sichere Zahlungsmethoden zu verwenden, z. B. Kreditkarten mit zusätzlichen Sicherheitsmaßnahmen.

Sichere Nutzung von E-Mails: Warnen Sie sie vor Phishing und raten Sie ihnen, nicht auf Links zu klicken oder Anhänge von unbekannten Absendern herunterzuladen. Warnen Sie sie vor E-Mail-Phishing, bei dem Betrüger versuchen, sensible Informationen zu erhalten, indem sie sich als legitime Absender ausgeben. Dies unterstreicht, wie wichtig es ist, nicht auf Links zu klicken oder Anhänge von verdächtigen E-Mails oder unbekannten Absendern herunterzuladen. Es wird dringend empfohlen, die Legitimität von E-Mails beim Absender zu überprüfen, bevor vertrauliche Informationen gesendet werden.

Soziale Medien: Helfen Sie ihnen, die Datenschutzeinstellungen in ihren sozialen Medien anzupassen, um zu kontrollieren, wer ihre Beiträge sieht, und vermeiden Sie die Weitergabe sensibler persönlicher Informationen. Bringen Sie ihnen bei, dass sie keine sensiblen Informationen wie Telefonnummern, Adressen oder finanzielle Informationen in sozialen Medien veröffentlichen sollten.

Führen Sie sie zum Beispiel durch die Privatsphäre-Einstellungen auf Facebook, damit nur Freunde ihre Beiträge sehen können. Betonen Sie, wie wichtig es ist, bei der Weitergabe von Informationen wie Telefonnummern, Adressen oder finanziellen Details auf Social Media-Plattformen vorsichtig zu sein.

Sicheres Surfen: Lernen Sie, diese sicheren Websites zu erkennen ("https" und "lock") und vermeiden Sie es, auf verdächtige Links zu klicken oder unbekannte Dateien herunterzuladen. Bringen Sie Ihren Kindern bei, sichere Websites zu unterscheiden, indem Sie in der Adressleiste auf ein Schloss achten und prüfen, ob sie gestartet werden. "http" statt "https". Erklären Sie, wie wichtig es ist, nicht auf verdächtige Links zu klicken oder Dateien von unbekannten Quellen herunterzuladen, da sie Malware enthalten oder zu betrügerischen Websites weiterleiten können.

Wi-Fi-Sicherheit: Vergewissern Sie sich, dass sie sichere Passwörter für ihr heimisches Wi-Fi-Netzwerk verwenden und vermeiden Sie es, sich mit öffentlichen oder unbekannten Wi-Fi-Netzwerken zu verbinden. Erklären Sie, wie wichtig es ist, sichere Passwörter für das heimische Wi-Fi-Netzwerk zu verwenden und die Verbindung mit öffentlichen oder unbekannten Wi-Fi-Netzwerken zu vermeiden. Ungesicherte Wi-Fi-Netzwerke können potenziell angegriffen oder für Datenspionage abgefangen werden.

Inaktive Konten: Helfen Sie ihnen, nicht mehr genutzte Online-Konten zu schließen oder zu löschen, um das Sicherheitsrisiko zu verringern. Inaktive Konten können anfällig für Angriffe sein, insbesondere wenn sie persönliche Daten enthalten.

Achten Sie auf verdächtige Anrufe und Nachrichten: Bringen Sie ihnen bei, bei unerwarteten Anrufen oder Nachrichten keine persönlichen oder finanziellen Informationen preiszugeben. Bringen Sie ihnen bei, vorsichtig zu sein, wenn sie bei unerwarteten Anrufen oder Textnachrichten persönliche oder finanzielle Informationen preisgeben. Ermutigen Sie den Absender, seine Identität zu überprüfen, bevor er sensible Informationen preisgibt. Geben Sie Beispiele für gängige Betrugsversuche, wie z. B. gefälschte Anrufe beim technischen Support oder Benachrichtigungen über Lottogewinne**.**

Beaufsichtigung und Unterstützung: Bieten Sie Ihre Hilfe bei der regelmäßigen Überprüfung Ihrer Online-Konten an und helfen Sie ihnen, wenn sie verdächtige Aktivitäten vermuten oder Sicherheitsprobleme haben. Halten Sie sich über die neuesten Online-Bedrohungen auf dem Laufenden und bieten Sie kontinuierliche Anleitung und Unterstützung. Zeigen Sie ihnen zum Beispiel, wie sie ihre jüngsten Kontoaktivitäten und Anmeldungen auf verschiedenen Plattformen überprüfen können.

Persönliche Informationen: Bringen Sie Ihren Kindern bei, vorsichtig zu sein, wenn sie persönliche Informationen online weitergeben, und die Menge der Informationen, die sie veröffentlichen, zu begrenzen. Begrenzen Sie die Menge der Informationen, die sie veröffentlichen, wie Adressen, Telefonnummern oder Schulinformationen. Dies fördert die Privatsphäre und die Bedeutung des Schutzes der eigenen Online-Identität.

Sichern Sie wichtige Daten: Erstellen Sie regelmäßig Sicherungskopien wichtiger Daten, um den Verlust im Falle einer Sicherheitsverletzung oder eines Geräteausfalls zu verhindern**.**

4.2 Bewährte Verfahren aus aller Welt

4.2.1 Cyber Europe

Seit 2010 ENISA hat organisiert Cyber Europe[4], eine Reihe von Übungen zum Management von Cybervorfällen und -krisen mit spannenden Szenarien, die sich an realen Ereignissen orientieren und von europäischen Cybersicherheitsexperten entwickelt wurden. Alle zwei Jahre arbeiten öffentliche und private Sektoren aus EU- und EWR-Ländern sowie europäische Organe, Einrichtungen und Agenturen zusammen, um ihre bestehenden technischen und operativen Fähigkeiten zu stärken.

Die Übung Cyber Europe dauert zwei Tage und simuliert groß angelegte Cybersicherheitsvorfälle, die sich zu Cyberkrisen ausweiten, die die gesamte EU betreffen. Die Teilnehmer an dieser Übung werden in der Lage sein, fortgeschrittene technische Cybersicherheitsvorfälle zu analysieren und mit komplexen Situationen der Geschäftskontinuität und des Krisenmanagements umzugehen, die eine Koordinierung und Zusammenarbeit von der lokalen bis zur EU-Ebene erfordern.

Die Cyber Europe-Übungsreihe zielt darauf ab, die Bereitschaft Europas zur Bewältigung groß angelegter Cybersicherheitsvorfälle und -krisen zu verbessern, indem sie den Teilnehmern die Möglichkeit gibt, ihre Bereitschaft in der gesamten EU zu testen und zu verbessern, Vertrauen innerhalb des Cybersicherheitsökosystems der EU aufzubauen und Schulungsmöglichkeiten zu bieten.

Die Teilnahme an Cyber Europe bietet eine hervorragende Gelegenheit:

- Das Bewusstsein für Cyberfragen zu schärfen.
- Verfahren für das Cyber-Krisenmanagement zu entwickeln und/oder zu erproben.
- Die Kommunikation innerhalb der Cyber-Reaktionskette zu verbessern.
- Eine gemeinsame Sprache zu schaffen und das Verständnis füreinander zu verbessern.
- Eine Vielzahl individueller und kollektiver Resilienzfähigkeiten und -fertigkeiten zu entwickeln.
- Analyse komplexer technischer Cybersicherheitsvorfälle; Bewältigung komplexer Situationen der Geschäftskontinuität und des Krisenmanagements.

4.2.2 Anpassung von Schnittstelle und Technologie

Japan ist ein Vorreiter bei der Anpassung von Technologien und Geräten, um sie für ältere Menschen zugänglicher zu machen. So verfügen einige japanische Smartphones und Tablets über einfachere Benutzeroberflächen und verbesserte Zugänglichkeitsfunktionen, die die Nutzung für Menschen mit begrenzten digitalen Fähigkeiten erleichtern. Andere Länder und Technologiehersteller könnten solche Maßnahmen ergreifen, um sicherzustellen, dass ältere Erwachsene digitale Geräte sicher und effektiv nutzen können. Die Übernahme dieser Verfahren durch andere Länder und Technologiehersteller kann sicherstellen, dass ältere Erwachsene Zugang zu benutzerfreundlicheren digitalen Geräten haben, was ihre Online-Sicherheit und -Teilnahme verbessert.

Im europäischen Raum gibt es mehrere Kurse, die ältere Menschen für die Nutzung dieser Hilfsmittel sensibilisieren sollen. So bietet beispielsweise der Verband ACDA in Paris kostengünstige Kurse

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

an, um ältere Menschen in die Welt der Technologie einzuführen. Die Kurse dieser Vereinigung bieten die Möglichkeit, die Bedienung eines Computers von Grund auf zu erlernen. Die Entdeckung von Computereinheiten, Anwendungen und Dateiformaten. Danach können die Teilnehmer fortgeschrittenere Fähigkeiten erwerben, wie z. B. das Verwalten und Organisieren der eigenen Mailbox und das Erlernen der Verwendung von Word, um ein schriftliches Dokument zu bearbeiten[5].

4.2.3 Helplines und spezialisierter Unterstützung

Singapur hat eine eigene Helpline für Senioren eingerichtet, die mit Problemen der digitalen Sicherheit konfrontiert sind. Diese Helpline bietet Beratung und technische Unterstützung bei der Lösung von Problemen mit der Cybersicherheit. Andere Länder könnten die Einführung ähnlicher Dienste in Betracht ziehen, um einen direkten und sicheren Kommunikationskanal für Senioren zu schaffen, die Online-Hilfe benötigen. Diese Dienste bieten älteren Menschen einen direkten und sicheren Kommunikationskanal, um Hilfe bei Cybersicherheitsproblemen, wie Online-Betrug oder Malware, zu erhalten. Die Einführung ähnlicher Dienste in anderen Ländern kann ein wichtiges Unterstützungsnetzwerk zum Schutz älterer Menschen in der digitalen Welt sein.

Im europäischen Raum hat beispielsweise die Vereinigung AGE UK[6] die Unterstützung älterer Menschen, die am stärksten von digitaler Ausgrenzung bedroht sind, zur Priorität erklärt.

Neben der Bereitstellung von Dienstleistungen für die ältere Bevölkerung werden sich die Kurse speziell darauf konzentrieren, einer Hochrisikogruppe den Zugang zur digitalen Welt zu erleichtern. Obwohl die Kernkomponenten des Programms bei der Arbeit mit diesen Hochrisikogruppen weitgehend unverändert bleiben, werden wahrscheinlich einige Anpassungen notwendig sein, um sicherzustellen, dass das Programm für diejenigen, die es am meisten brauchen, zugänglich und effektiv bleibt.

Die Hochrisikodienste des Digital Champion Programms richten sich an ältere Menschen, die:

- Demenz und/oder Gedächtnisverlust haben.
- Ein geringes Einkommen haben.
- Allein leben.
- Mobilitätsprobleme haben.
- Ans Haus gebunden sind.

4.2.4 Sensibilisierungskampagnen und Bildung

Länder wie Australien und Kanada haben Kampagnen zur Cybersicherheit und Programme zur Aufklärung über digitale Sicherheit für ältere Erwachsene durchgeführt. Diese Kampagnen informieren über gängige Cyberbedrohungen, geben Tipps, wie man sich vor Online-Betrug schützen kann, und zeigen, wie wichtig es ist, seine Geräte auf dem neuesten Stand zu halten. Die Regierungen können mit lokalen Organisationen, Gemeindezentren und Freiwilligengruppen zusammenarbeiten, um die ältere Bevölkerung zu erreichen und ihr digitale Kenntnisse zu vermitteln. Diese Informations- und Aufklärungskampagnen zielen darauf ab, ältere Menschen durch Aufklärung über digitale Sicherheit zu stärken. Sie werden darin geschult, Online-Betrug zu erkennen und zu vermeiden, ihre persönlichen Daten zu schützen und

[5] http://www.aucoursdesages.fr/cours.php

[6] https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

Sicherheitstools wie Antivirenprogramme und sichere Passwörter zu verwenden. Sie werden auch über die Risiken bei der Nutzung sozialer Medien und die Bedeutung der richtigen Online-Datenschutzeinstellungen informiert. Der oben genannte Verband ACDA in Paris bietet ebenfalls Kurse zum Thema digitale Sicherheit an.

Ein weiterer Verband, der sich auf die digitale Sensibilisierung konzentriert, ist die Orange Foundation, die gefährdete Gruppen über die neuesten Technologien informiert und sie zu einer sichereren digitalen Nutzung anleitet. Darüber hinaus organisiert die Orange Stiftung in ganz Frankreich eine Reihe kostenloser digitaler Schulungskurse für junge Menschen und Frauen, die oft arbeitslos sind, über keine Qualifikation verfügen und sich manchmal in prekären Situationen befinden. Indem sie diese Menschen in digitalen Fertigkeiten schulen, helfen sie ihnen, sich neu zu sozialisieren, einen Job zu suchen, die professionelle Nutzung der digitalen Technologie zu übernehmen, ein Unternehmen zu entwickeln oder die digitale Technologie sogar zu ihrem Beruf zu machen.

4.2.5 Finanzielle Schutzprogramme

Länder wie das Vereinigte Königreich und die USA[7] haben Maßnahmen zum Schutz von Rentnern vor Online-Finanzbetrug eingeführt. Zu diesen Maßnahmen gehören Haftungsgrenzen für Betrugsopfer und Rechtsmittel zur Wiedererlangung gestohlener Gelder. Andere Länder können sich an diesen Initiativen orientieren und sie an ihre Finanzsysteme anpassen, um Senioren vor möglichen finanziellen Verlusten zu schützen. Finanzieller Schutz für ältere Erwachsene ist ein wichtiger Bestandteil der digitalen Sicherheit. Programme, die speziell darauf ausgerichtet sind, Online-Finanzbetrug zu verhindern und abzuschwächen, können dieser Bevölkerungsgruppe ein höheres Maß an Sicherheit bieten. So kann die Haftung der Betrugsopfer begrenzt und ein Mechanismus zur Wiedererlangung gestohlener Gelder geschaffen werden. Diese Maßnahmen schützen nicht nur das finanzielle Wohlergehen älterer Menschen, sondern vermitteln auch die klare Botschaft, dass ihr Wohlergehen und ihre finanzielle Sicherheit ernst genommen werden.

In Europa ist die Festlegung von Haftungsbeschränkungen für Betrugsopfer ein wesentlicher Aspekt des Schutzes des finanziellen Wohlergehens älterer Menschen. Wenn Betrugsopfer für die von ihnen erlittenen finanziellen Verluste haftbar gemacht werden, kann dies schwerwiegende Folgen haben, einschließlich des finanziellen Ruins und emotionaler Not. Durch die Einführung einer Politik, die angemessene Haftungsgrenzen festlegt, erkennt die Gesellschaft die besondere Gefährdung älterer Menschen an und versucht, die ihnen auferlegte Belastung zu verringern. Diese Maßnahme bietet ein Sicherheitsnetz, das gewährleistet, dass ältere Erwachsene nicht zu Unrecht mit den Folgen betrügerischer Handlungen belastet werden. Die Festlegung von Haftungsbeschränkungen für Betrugsopfer ist ein wesentlicher Aspekt der Sicherung des finanziellen Wohlstands älterer Menschen. Auf europäischer Ebene gibt es zahlreiche Vereinigungen, die sich dem Schutz älterer Menschen widmen, die häufig Opfer von Online-Betrügereien werden, denen es an Bewusstsein mangelt und die finanzielle Verluste erleiden können. Einer dieser Verbände ist Marketing Management IO (MMIO), eine zertifizierte Agentur in Spanien und Frankreich.[8]

Wenn Betrugsopfer für ihre finanziellen Verluste zur Rechenschaft gezogen werden, kann dies schwerwiegende Folgen haben. Daher ist die Sensibilisierung so wichtig. Durch die Einführung von

[7] https://www.bankofamerica.com/signature-services/elder-financial-services/

[8] https://www.marketing-management.io/blog/formation-digital-marketing

Maßnahmen, die angemessene Haftungsgrenzen festlegen, erkennt die Gesellschaft die besondere Verletzlichkeit älterer Menschen an und versucht, die Belastung für sie zu verringern. Diese Maßnahme bietet ein Sicherheitsnetz, das gewährleistet, dass ältere Menschen nicht zu Unrecht durch die Folgen betrügerischer Aktivitäten belastet werden.

Marketing Management IO (MMIO) umfasst Themen wie Internet-Möglichkeiten, natürliche Referenzierung, Online-Sichtbarkeit, Content Marketing und Umsatzsteigerung. Die Konzepte sind vereinfacht und die Aktionen sind kostenlos. Es sind auch Bonus-Ressourcen verfügbar.

Der Kurs umfasst 5 Lektionen mit Videos. Facebook bietet eine Plattform mit kostenlosem Zugang zu über 70 Online-Kursen. Diese Kurse befassen sich speziell mit der Nutzung von Facebook zur Verbesserung Ihrer Online-Präsenz und Ihres Geschäftsumsatzes, der Sicherheit und der Bekanntheit.

4.2.6 Zusammenarbeit mit der Technologiebranche

Einige Länder, wie z. B. die Vereinigten Staaten, haben sich mit Technologieunternehmen zusammengetan, um die Herausforderungen der digitalen Sicherheit im Zusammenhang mit der alternden Bevölkerung zu bewältigen. Diese Zusammenarbeit kann die Verbesserung von Sicherheitssoftware, die Verbesserung der Betrugserkennung und die Implementierung von Sicherheitsfunktionen in digitale Produkte und Dienstleistungen umfassen. Die Zusammenarbeit mit der Technologiebranche kann ein effektiver Weg sein, um sich über die neuesten Sicherheitsbedrohungen und Lösungen auf dem Laufenden zu halten, wie z. B. die Implementierung fortschrittlicher Sicherheitstechnologien, die Verbesserung der Betrugserkennung und die Förderung von Sicherheitspraktiken für digitale Produkte und Dienstleistungen, die sich an ältere Menschen richten. Die Zusammenarbeit mit der Technologiebranche gewährleistet eine schnellere und aktuellere Reaktion auf digitale Bedrohungen.

In anderen Ländern wie Frankreich und England gibt es Kurse zur digitalen Sicherheit, die älteren Menschen helfen sollen, Verteidigungstechnologien zu verstehen; die angebotenen Kurse ermöglichen es ihnen, eine Grundlage für die Digitalisierung zu schaffen und zu verstehen, wie sie sicher im Internet navigieren können.

So bietet Konexio [9] beispielsweise Schulungen zu digitalen Kompetenzen an - von den grundlegendsten bis zu den fortgeschrittensten -, um die soziale und berufliche Integration zu fördern. Innovativ, auf der Grundlage praktischer Fallstudien und mit einer starken Betonung auf transversalen und relationalen Fähigkeiten oder Soft Skills, zielen unsere Schulungen darauf ab, jeden in die Lage zu versetzen, an der Digitalisierung der Gesellschaft teilzunehmen. Sie bieten verschiedene Ausbildungen an: digitale Kompetenzen, Webdesigner, System- und Netzwerktechniker, digitale Helfer. Das Programm konzentriert sich auf das Erlernen der Soft Skills und der sozialen Codes der Berufswelt durch Workshops. Es bietet auch die Möglichkeit, über unser Netzwerk direkt mit der Berufswelt in Kontakt zu treten. Es bietet ein regelmäßiges Follow-up und persönliche Unterstützung, um den Lernenden zu helfen, Fortschritte zu machen und eventuelle Schwierigkeiten zu lösen.

[9] https://www.konexio.eu/formations.html

4.2.7 Internationale Ressourcen, Berichte und Initiativen

Diese Ressourcen bieten wertvolle Hinweise und bewährte Verfahren zur Verbesserung der digitalen Sicherheit in der Erwachsenenbildung in der EU.

An Open, Safe and Secure Cyberspace: Dieser Bericht bietet einen Überblick über die Cybersicherheitsstrategie der EU, die darauf abzielt, einen offenen, sicheren und geschützten Cyberraum in Europa zu fördern. Der Bericht enthält bewährte Verfahren zur Verbesserung der Cybersicherheit, einschließlich Risikomanagement, Reaktion auf Zwischenfälle und öffentlich-private Partnerschaften.

ENISA-Bericht über die Bedrohungslandschaft: Dieser Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) gibt einen Überblick über die aktuelle Bedrohungslage im Bereich der Cybersicherheit in Europa, einschließlich der häufigsten Arten von Cyberangriffen und der am meisten gefährdeten Sektoren. Der Bericht enthält bewährte Verfahren zur Vorbeugung und Abschwächung von Cyberangriffen, einschließlich Schulungen zum Sicherheitsbewusstsein, Schwachstellenmanagement und Reaktionsplanung bei Zwischenfällen.

NIS-Richtlinie und EU-Cybersicherheitsgesetz: Dieser Bericht bietet einen Überblick über den rechtlichen Rahmen der EU für Cybersicherheit, einschließlich der Richtlinie über Netz- und Informationssysteme (NIS) und des EU-Cybersicherheitsgesetzes. Der Bericht enthält bewährte Verfahren für die Einhaltung der rechtlichen Anforderungen, z. B. für die Meldung von Vorfällen und das Risikomanagement.

EU-Zertifizierungsrahmen für Cybersicherheit: Dieser Bericht bietet einen Überblick über den EU-Zertifizierungsrahmen für Cybersicherheit, der die Sicherheit und Vertrauenswürdigkeit digitaler Produkte und Dienstleistungen verbessern soll. Der Bericht enthält bewährte Verfahren für die Erlangung und Aufrechterhaltung von Cybersicherheitszertifizierungen, einschließlich Sicherheit durch Entwurf, Prüfung und Bewertung sowie laufende Überwachung und Bewertung.

Cybersicherheit für KMUs: Dieser Bericht enthält Leitlinien und bewährte Verfahren für kleine und mittlere Unternehmen (KMUs), wie sie ihre Cybersicherheit verbessern können. Der Bericht enthält Ratschläge zum Risikomanagement, zur Schulung des Sicherheitsbewusstseins, zur Entwicklung sicherer Software und zur Planung der Reaktion auf Vorfälle.

Digitale Fertigkeiten in der erwachsenen Bevölkerung: Dieser Bericht der Europäischen Kommission gibt einen Überblick über die digitalen Fähigkeiten der erwachsenen Bevölkerung in der EU. Er enthält einen Abschnitt über digitale Sicherheit, in dem hervorgehoben wird, dass Erwachsene über grundlegende Kenntnisse und Fähigkeiten verfügen müssen, um sich vor Cyber-Bedrohungen zu schützen.

Digitale Fertigkeiten für lebenslanges Lernen: Dieser Bericht der Europäischen Kommission enthält Leitlinien und bewährte Verfahren für die Entwicklung digitaler Kompetenzen bei Erwachsenen. Er enthält einen Abschnitt über digitale Sicherheit, der Ratschläge zum Risikomanagement, zum sicheren Surfen, zur Passwortverwaltung und zum Datenschutz gibt.

Das Cybersecurity for Digital Education Projekt: Dieses Projekt des European Schoolnet bietet Ressourcen und Schulungen zur Cybersicherheit für Lehrkräfte und Lernende in Europa. Das Projekt umfasst eine Reihe von Materialien, darunter Online-Kurse, Unterrichtspläne und Bewertungstools, die alle auf die Verbesserung der digitalen Sicherheit in der Bildung ausgerichtet sind.

Das Projekt Digitale Sicherheit für Senioren: Dieses Projekt der Agentur der Europäischen Union für Cybersicherheit (ENISA) bietet Ressourcen und Schulungen zur Cybersicherheit für Senioren. Das Projekt umfasst eine Reihe von Materialien, darunter Online-Kurse, Leitfäden und Videos, die alle auf die Verbesserung der digitalen Sicherheit bei älteren Erwachsenen abzielen.

Koalition für digitale Fertigkeiten und Arbeitsplätze: Diese Initiative der Europäischen Kommission zielt darauf ab, die digitalen Fähigkeiten der Europäer zu verbessern, um ihnen die volle Teilnahme an der digitalen Wirtschaft zu ermöglichen. Sie umfasst eine Reihe von Ressourcen und Schulungsmöglichkeiten, auch zum Thema digitale Sicherheit.

4.3 Bewährte Verfahren in der Erwachsenenbildung zum Thema digitale Sicherheit

ENISA-Ausbildungsprogramm für Ausbilder

Alle Online-Schulungsmaterialien und Schulungskurse im Abschnitt "Schulungskurse für Cybersicherheitsspezialisten" basieren auf der Philosophie "Train the Trainer". Das "Train the Trainer"-Programm und die Philosophie zielen darauf ab, das Netzwerk der Ausbilder zu erweitern und einen besseren Informationsaustausch zu fördern. Dies dient mehreren Zwecken, unter anderem:

- Austausch von Schulungsmaterialien, um Zeit und Geld für Schulungen zu sparen,
- Schaffung regionaler Ausbildungsbemühungen,
- Förderung der Zusammenarbeit zwischen verschiedenen Ausbildungsanbietern,
- Förderung guter Ausbildungspraktiken,
- Verringerung von Wettbewerb und Doppelarbeit.

Das Online-Schulungsmaterial der ENISA wird ein Handbuch für Ausbilder, ein Toolset für Teilnehmer und virtuelle Maschinen zum Herunterladen enthalten. Dies ermöglicht es potenziellen Ausbildern, den Kurs vorzubereiten, und das Handbuch wird sie dabei unterstützen, die Teilnehmer durch den Kurs zu führen. Es enthält Spickzettel, mögliche kleine Tests, um festzustellen, ob die Kursteilnehmer die wichtigen Lektionen aus den Kursen verstanden haben, sowie zusätzliche Informationen oder Übungen, die der Ausbilder verwenden kann, um den Kurs interessanter oder anspruchsvoller zu gestalten.

Durch das gegenseitige Lernen von Erfolgen und Misserfolgen können sowohl Anfänger als auch erfahrene Ausbilder Schulungen besser konzipieren und durchführen, so dass sie erfolgreicher sind, mehr "Spaß" machen und bessere und länger anhaltende Ergebnisse erzielen.

TiK – Technology in Brief

Das Hightech-Projekt verfolgt einen generationenübergreifenden Ansatz durch die Ausbildung von jungen Freiwilligen (16 bis 30 Jahre) als so genannte "Tablet-Trainer", die nach einem speziellen Tablet-Education-Curriculum ausgebildet werden. Die Kurse zeichnen sich durch eine Vielzahl von Methoden und flexiblen Leitfragen und ein besonderes Engagement der jungen Trainer aus. Sie bieten niedrigschwellige Kurse ehrenamtlich für eine geringe Aufwandsentschädigung an. Die Weiterentwicklung der Kurse wird durch das Feedback der Teilnehmerinnen und Teilnehmer sowie der Trainerinnen und Trainer

gewährleistet, die auch eigene spezielle Materialien und barrierefreie Handreichungen für ältere Menschen erarbeitet haben.

Die Kurse sind für Interessierte leicht erreichbar und es wird auf eine breite geografische Verteilung der "TiK-Module" und der Informationen auf www.digitaleseniorinnen.at geachtet. Teilnehmer der Kurse sind Personen und insbesondere wirtschaftlich benachteiligte Frauen mit niedrigem Bildungsniveau. Bis Ende 2018 haben mehr als 2000 Personen mit den Modulen gelernt und weitere 1000 Personen haben am Kursprogramm teilgenommen. Der älteste Teilnehmer, der gerade an einem Kurs teilnimmt, ist 97 Jahre alt, er wird von einem jungen Mann in einem Pflegeheim ausgebildet. Das Projekt wurde mehrfach auf Bundes- und Landesebene ausgezeichnet.

5 Schulung von Erwachsenen: Wie man digitale Resilienz aufbaut

Die Andragogik ist eine Lehre vom Lernen Erwachsener, die in den 1950er Jahren in Europa entstand, aber erst in den 1970er Jahren von Malcolm Knowles, einem amerikanischen Praktiker und Theoretiker der Erwachsenenbildung, als Theorie und Modell des Lernens Erwachsener entwickelt wurde, der Andragogik als "die Kunst und Wissenschaft, Erwachsenen beim Lernen zu helfen" definierte (Fidishun 2000). Fidishun (2000) schlug vor, dass andragogische Prinzipien bei der Gestaltung von Online-Kursen verwendet werden sollten, um "Flexibilität und die Fähigkeit der Lernenden zu fördern, sich durch die Lektionen zu bewegen, wann, wo und in ihrem eigenen Tempo".

5.1 Vier Prinzipien der Andragogik

In Anbetracht der Tatsache, dass Erwachsene ihre eigene, einzigartige Art des Lernens haben, gibt es 4 zentrale Prinzipien, die erklären, wie man am besten Schulungen für sie entwickelt.

- Wenn es um das Lernen geht, wollen oder müssen Erwachsene daran beteiligt sein, wie ihr Training geplant, geliefert und durchgeführt wird. Sie wollen selbst bestimmen, was, wann und wie sie lernen.
- Erwachsene gewinnen mehr, wenn sie frühere Erfahrungen in den Lernprozess einbringen können. Sie können auf das zurückgreifen, was sie bereits wissen, um ihrem Lernen einen größeren Kontext zu geben.
- Das Auswendiglernen von Fakten und Informationen ist für Erwachsene nicht der richtige Weg, um zu lernen. Sie müssen Probleme lösen und Überlegungen anstellen, um die Informationen, die ihnen präsentiert werden, bestmöglich zu verarbeiten.
- Erwachsene wollen wissen: "Wie kann ich diese Informationen jetzt nutzen?". Was sie lernen, muss in ihrem Leben anwendbar sein und sofort umgesetzt werden können.

5.2 Wie können Erwachsenentrainer Andragogik umsetzen?

Selbstgesteuertes Lernen ermöglichen

In der Vergangenheit war Lernen oft eine obligatorische Aktivität, die zu einer bestimmten Zeit stattfand. Mit Technologien wie einem Lernmanagementsystem können wir erwachsenen Lernenden jetzt ein viel selbstbestimmteres, unabhängiges Lernumfeld bieten. Wir können ihnen die Möglichkeit geben, sich zu trainieren, wann und wo sie wollen, ihnen eine Auswahl an Kursen anbieten, die sie belegen können, und ihnen ermöglichen, ihre eigenen Lernziele zu verfolgen.

Lernbeispiele aus der realen Welt verwenden

Wie die Theorie besagt, möchten Erwachsene wissen, wie die Schulung für sie unmittelbar anwendbar und von Nutzen ist. Wenn wir also Kursinhalte erstellen, sollten wir sie mit so vielen Beispielen aus der Praxis wie möglich versehen.

Wenn Sie erwachsene Lernende zu digitalem Wohlbefinden und/oder digitaler Sicherheit schulen, führen Sie sie Schritt für Schritt durch einen Arbeitsablauf, den sie tatsächlich nutzen werden, und erklären Sie ausdrücklich, wie und warum sie ihn nutzen werden. Erklären Sie, wie die Schulung helfen wird, und verwenden Sie dann echte Beispiele für die Schulung.

Erwachsene Lernende selbst herausfinden lassen

Da Erwachsene das Lösen von Problemen den reinen Fakten vorziehen, ist es eine gute Idee, bei der Erstellung von Inhalten nicht gleich alle Antworten zu präsentieren. Warum nicht stattdessen kreativ werden und Kurse erstellen, die das Gehirn der Lernenden anregen?

Wir können dies auf einfache Weise erreichen, indem wir Tests und Simulationen einbauen, die spezifische Probleme aufzeigen, mit denen die Lernenden konfrontiert werden könnten, und dann die erwachsenen Lernenden dazu bringen, ihre Fähigkeiten einzusetzen, um diese zu lösen.

6 Fazit

Die digitale Sicherheit älterer Menschen ist ein zentrales Thema, das die Aufmerksamkeit und das Handeln der Regierungen und der Gesellschaft insgesamt erfordert. Durch die Umsetzung der oben genannten bewährten Verfahren können die Länder den digitalen Schutz und das Wohlbefinden ihrer alternden Bevölkerung verbessern. Bewusstseinsbildung, Bildung, gezielte Unterstützung, technologische Anpassung und die Zusammenarbeit mit der Industrie sind die wichtigsten Säulen, um eine sichere und positive Online-Erfahrung für ältere Erwachsene zu gewährleisten.

Das DigiWELL-Projekt zielt darauf ab, die Grundsätze des digitalen Wohlbefindens in die Erwachsenenbildung einzubeziehen. Seine Initiativen sind darauf ausgerichtet, einen Beitrag zu den allgemeinen Praktiken von Organisationen, Netzwerken und Initiativen der Erwachsenenbildung zu leisten. Das Projekt weiß, wie wichtig es ist, sich mit den Auswirkungen der Technologie auf die geistige Gesundheit, die Produktivität und das allgemeine Wohlbefinden von Erwachsenen im digitalen Zeitalter zu befassen. Das Hauptziel von DigiWELL besteht darin, erwachsene Lernende mit den Informationen, Fähigkeiten und Ressourcen auszustatten, die sie benötigen, um sich ethisch und gewissenhaft in der digitalen Welt zurechtzufinden. Das DigiWELL-Projekt umfasst auch die Entwicklung und Durchführung zusätzlicher Initiativen zur Befähigung erwachsener Lernender. Das Ziel dieser Aktivitäten ist es, eine unterstützende Umgebung zu schaffen, in der Erwachsene ihre Erfahrungen, Schwierigkeiten und Erfolge bei der Förderung des digitalen Wohlbefindens austauschen können.

In diesem Sinne bietet das DigiWELL-Projekt viele Möglichkeiten für Einzelpersonen und Organisationen für Erwachsene, sich der Bedeutung des digitalen Wohlbefindens bewusst zu werden und darüber aufzuklären, wie man das digitale Wohlbefinden von erwachsenen Einzelpersonen und Erwachsenenbildnern und -ausbildern fördern kann. Die Förderung des digitalen Wohlbefindens mit einem ganzheitlichen Ansatz ist viel besser möglich, wenn alle relevanten Parteien Maßnahmen ergreifen, um die Bedürfnisse des digitalen Wohlbefindens des Einzelnen zu unterstützen. Daher laden die in diesem Handbuch vorgestellten Informationen, Tipps und bewährten Verfahren Menschen und interessierte Organisationen dazu ein, Initiativen zu ergreifen, damit mehr von uns ein besseres digitales Wohlbefinden und auch ein stärkeres digitales Leben haben.

7 Referenzen

Für die Erstellung des Wörterbuchs wurden frei verfügbare Online-Ressourcen genutzt: Online-Wörterbücher, wissenschaftliche Artikel und Literatur aus den Bereichen Informationssicherheit, digitale Technologien und Dienstleistungen, digitales Wohlbefinden und digitale Resilienz sowie Begriffe und Definitionen aus dem Bereich Informationssicherheit.

1 BAI. Committee on National Security Systems (CNSS) Glossary (2015). In *BAI Information Security Consulting & Training [online]*. Retrieved from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Capterra Glossary*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Cybersecurity glossary of terms*. Global Knowledge. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Glossary*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Glossary*. The Digital Wellness Lab. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Online browsing platform (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Fifth edition.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, July 16). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Glossary of key information security terms*. NIST. Retrieved from: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Computer security: Principles and practice*. *Third edition.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *TVETipedia Glossary*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Teaching adult students to use computerized resources: Utilizing Lawler's keys to adult learning to make instruction more effective. *Information technology and libraries*, *19*(3), 157-157.

15 European Commission, Directorate-General for Education, Youth, Sport and Culture, Key competences for lifelong learning, Publications Office, 2019, https://data.europa.eu/doi/10.2766/569540.