Modul Steckbrief

Titel	Cybersicherheit für Senior*innen: Tools für eine sichere Navigation
Keywords	Cybersicherheit, Online-Sicherheit, digitale Abhängigkeit, sicheres Surfen, Gesundheitstechnologie
Bereitgestellt von	Croatian Telecom Inc.
Sprache	Deutsch

Schulungsbereich (X, falls zutreffend)	
	Informationskompetenz
	Kommunikation und Kollaboration
x	Sicherheit
	Problemlösung

Ziele / Lernergebnisse

Zielsetzung: Ziel dieser Schulung ist es, Senioren über Cybersicherheit aufzuklären und ihnen die notwendigen Werkzeuge und Kenntnisse zu vermitteln, damit sie sich sicher in der Online-Welt bewegen können.
Lernergebnisse - Am Ende dieser Schulung werden die Teilnehmer in der Lage sein:

- die Bedeutung der Cybersicherheit zu verstehen
- Erkennen gängiger Cyber-Bedrohungen
- Sicheres Surfen im Internet
- Schutz persönlicher Informationen
- Reagieren auf Cybervorfälle
- Digitale Technologien für Gesundheit und Wohlbefinden nutzen

Beschreibung

Diese Schulung vermittelt Senior*innen das nötige Wissen und die Werkzeuge, um sich sicher in der Online-Welt zu bewegen. Die Teilnehmer*innen lernen etwas über Cybersicherheitsrisiken und erkennen gängige Bedrohungen. Sie lernen, wie sie sicher im Internet surfen und ihre E-Mails schützen können, wie sie ihre persönlichen Geräte absichern, ihre persönlichen Daten schützen und sicher bleiben. Die Schulung befasst sich auch mit der Reaktion auf Zwischenfälle und damit, wie wichtig es ist, sich über neue Cyber-Bedrohungen auf dem Laufenden zu halten. Sie werden auch in der Lage sein, digitale Technologien in Bezug auf ihre Gesundheit und ihr Wohlergehen sicher zu nutzen, fundierte Entscheidungen zu treffen und die damit verbundenen Möglichkeiten auszuschöpfen. Am Ende werden Sie in der Lage sein, sich selbst und Ihre persönlichen Daten online zu schützen.

Inhaltsindex (3 Stufen)

Modul: Cybersicherheit für Senior*innen: Tools für eine sichere Navigation

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Unit 1: Einführung in die Cybersicherheit
1.1. Verständnis von Cybersicherheitsrisiken
1.2. Häufige Arten von Cyber-Bedrohungen
1.3. Bedeutung der Cybersicherheit für Senioren

Unit 2: Sicheres Surfen im Internet
2.1. Bewährte Praktiken, um sich in der digitalen Umgebung zu schützen
2.2. Verbesserung der Online-Sicherheit mit sicheren Browsing-Tools

Unit 3: Gesundheit und Wohlbefinden im digitalen Zeitalter
3.1. Risiken von übermäßiger Bildschirmzeit und digitaler Abhängigkeit
3.2. Gesundheit und digitale Werkzeuge

Inhalt entwickelt

Modul: Cybersicherheit für Senior*innen: Tools für eine sichere Navigation

Unit 1: Einführung in die Cybersicherheit
Abschnitt 1.1: Verständnis der Cybersicherheitsrisiken
Betrachten Sie Cybersicherheitsrisiken als potenzielle Gefahren, wenn Sie online gehen. So wie Sie in der physischen Welt Vorkehrungen treffen, um sicher zu sein, z. B. indem Sie Ihre Türen abschließen, hilft es Ihnen, in der digitalen Welt sicher zu bleiben, wenn Sie sich der Cyberrisiken bewusst sind. Zu diesen Risiken gehören z. B. Hacker, die versuchen, Ihre persönlichen Daten zu stehlen, Betrüger*innen, die Sie dazu verleiten, Ihr Geld herauszugeben, oder Viren, die Ihren Computer schädigen können. Darüber hinaus legt die Cybersicherheit den Schwerpunkt auf die Kultivierung einer sicherheitsbewussten Kultur durch die Förderung des Bewusstseins und die Aufklärung über sichere Online-Praktiken.
Wenn Sie sich über diese Risiken informieren, können Sie sich besser schützen. Das ist so, als würden Sie die Anzeichen für einen rutschigen Boden kennen, damit Sie vorsichtig gehen und nicht stürzen. Wir werden häufige Cyber-Risiken erörtern und wie man sie erkennt, damit Sie sich in der Online-Welt sicher bewegen und fundierte Entscheidungen treffen können, um sich und Ihre Daten zu schützen. Denken Sie daran: Wissen ist Macht, und wenn Sie die Risiken der Cybersicherheit verstehen, machen Sie einen wichtigen Schritt, um sich online zu schützen.

1.2. Häufige Arten von Cyber-Bedrohungen
In dieser Lektion werden wir uns mit den gängigen Arten von Cyber-Bedrohungen befassen, d. h. mit den verschiedenen Methoden, mit denen böswillige Akteure versuchen, Ihnen oder Ihrem Computer Schaden zuzufügen, wenn Sie das Internet nutzen. Wenn Sie diese Bedrohungen verstehen, können Sie sich schützen und mögliche Schäden vermeiden. Lassen Sie es uns in einfachen Worten ausdrücken.

Stellen Sie sich Cyber-Bedrohungen als hinterhältige Tricks oder Fallen vor, die böse Menschen im Internet benutzen. Sie wollen Ihre persönlichen Daten stehlen, Ihren Computer mit schädlicher Software infizieren oder Sie mit einem Trick dazu bringen,

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ihnen Ihr Geld zu geben. Zu den häufigsten Arten von Cyber-Bedrohungen gehören Phishing, Malware und Identitätsdiebstahl.

Phishing ist eine gefälschte E-Mail oder Nachricht, die vorgibt, von einer Person zu stammen, der Sie vertrauen, die aber versucht, Sie dazu zu bringen, Ihre persönlichen Daten preiszugeben. Es ist so, als würde sich jemand als Freund ausgeben, um an Ihre Geheimnisse zu gelangen. Häufig vorkommende Phishing-Nachrichten sind: gefälschte E-Mails von der Bank, falsche Meldungen über Gewinne aus Glücksspielen oder Gratisgewinne, gefälschte Konten von Anbietern von IT- oder Zahlungsdiensten oder Internetshops, falsche Bestätigungen angeblicher Bestellungen oder falsche Zahlungserinnerungen, falsche Nachrichten über Datenschutzrichtlinien oder Bedingungen, die man akzeptieren sollte.
Die Phishing-E-Mail-Nachricht kann lauten: Ihre Kreditkarte ist abgelaufen, Ihr Konto ist abgelaufen, vorübergehend gesperrt, oder bestätigen Sie Ihre Anmeldedaten. Layout (Corporate Design), Absenderadresse oder die direkte Begrüßung des Nutzers können den Eindruck erwecken, dass es sich um eine E-Mail einer Bank oder eines anderen Dienstleisters handelt. E-Mail-Nachrichten im HTML-Format zeigen dem Empfänger einen "legalen" Link an, der im Hintergrund einen versteckten Link enthält, der direkt zu betrügerischen oder bösartigen Inhalten führt.
Malware ist wie ein Virus, der Ihren Computer infizieren und Schaden anrichten kann. Sie kann Ihren Computer verlangsamen oder sogar Ihre persönlichen Daten stehlen.
Von Identitätsdiebstahl spricht man, wenn jemand Ihre persönlichen Daten wie Ihren Namen, Ihre Adresse oder Ihre Kreditkartendaten stiehlt und sie ohne Ihre Zustimmung verwendet. Jemand gibt sich als Sie aus und verwendet Ihr Geld oder kauft Dinge in Ihrem Namen.
Identitätsdiebe können in ihre E-Mail-Nachrichten auch Schadprogramme wie Viren integrieren
oder Trojaner-Software als Link, Anhang oder Quellcode in einer E-Mail-Nachricht im HTML-Format. Schon ein Klick auf das Bild in der Phishing-Nachricht kann schwerwiegende Folgen haben. Betrüger*innen, die Identitäten stehlen, verwenden oft Adressen, die sich nur geringfügig von den Originaladressen unterscheiden. Ein Identitätsdieb kann Zeichen ersetzen, um gefälschte URLs zu erstellen. Beispielsweise kann anstelle der Originaladressen wie http://www.onlinebank.com.hr eine gefälschte Darstellung mit einer Adresse wie http://www.on1inebank.com.hr verwendet werden.
Wie erkennt man, ob etwas bösartig ist?

- GEFÄLSCHTE ABSENDERADRESSE

Fahren Sie mit der Maus über die Adresse des Absenders. Enthält die E-Mail-Adresse verdächtige Elemente? Gibt es Rechtschreibfehler in der Adresse, auch wenn sie unbedeutend sind?

- ERSUCHEN UM VERTRAULICHE DATEN

Fordert Sie der in der E-Mail enthaltene Link zur Eingabe persönlicher Daten auf? Werden Sie aufgefordert, vertrauliche Informationen wie PINs oder Passwörter anzugeben?
DRINGLICHKEIT

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

- Fordert die E-Mail Sie zu sofortigem oder dringendem Handeln auf? Enthält die Nachricht eine Drohung oder eine Warnung?
- LINKS ZU GEFÄLSCHTEN WEBSITES

Welche URL wird angezeigt, wenn Sie mit der Maus auf einen Link klicken? Handelt es sich um eine sichere Seite (die URL sollte mit "https://" beginnen) und ist sie verschlüsselt (Schlosssymbol vor der URL)?

- SELTSAME FORMULIERUNGEN UND RECHTSCHREIBFEHLER

Ist die E-Mail-Begrüßung allgemein gehalten? Enthält sie Rechtschreibfehler, falsche Zeichensetzung oder Sonderzeichen?

Wenn Sie sich über diese häufigen Arten von Cyber-Bedrohungen informieren, können Sie sie erkennen und Schritte unternehmen, um sich zu schützen. Wir werden Strategien erörtern, um sicher zu bleiben und zu vermeiden, dass Sie diesen Bedrohungen zum Opfer fallen, damit Sie die Online-Welt mit Vertrauen und Seelenfrieden genießen können.

1.3. Bedeutung der Cybersicherheit für Senior*innen

Betrachten Sie die Cybersicherheit als Ihren persönlichen Bodyguard in der digitalen Welt, der sich um Ihr Wohlergehen kümmert. Es ist, als hätte man jemanden, der über einen wacht und dafür sorgt, dass die persönlichen Daten und Geräte sicher bleiben. Um Cybersicherheit zu gewährleisten, müssen wir sichere Online-Gewohnheiten praktizieren, z. B. sichere und eindeutige Passwörter erstellen, vorsichtig sein, wenn wir auf verdächtige Links klicken oder Dateien von unbekannten Quellen herunterladen, und unsere Geräte und Software auf dem neuesten Stand halten.

- Bestätigen Sie niemals Ihre Kontonummer, Ihr Passwort oder andere geheime Informationen, wenn Sie in einer E-Mail-Nachricht dazu aufgefordert werden. Echte Banken und Unternehmen würden dies aus Sicherheitsgründen niemals tun.
- Prüfen Sie den Sicherheitsstatus von Websites, bevor Sie Ihre persönlichen Daten eingeben. HTTPS ist keine Garantie dafür, dass eine Website echt ist. Klicken Sie auf das Vorhängeschloss-Symbol, das neben der URL in Ihrem Browser angezeigt wird, um das Sicherheitszertifikat der Website zu überprüfen.
- Der Glaube an die Unfehlbarkeit der Technik kann Raum für Phishing-Angriffe lassen. Ein gesundes Maß an Misstrauen hindert Angreifer daran, Ihre Identität zu stehlen und sich Zugang zu Ihren Konten und Informationssystemen zu verschaffen.

Unit 2: Sicheres Surfen im Internet

2.1. Bewährte Praktiken, um sich in der digitalen Umgebung zu schützen

- Üben Sie sichere Surfgewohnheiten: Halten Sie sich an vertrauenswürdige Websites, wenn Sie online einkaufen, Bankgeschäfte tätigen oder persönliche Daten weitergeben. Achten Sie auf das Vorhängeschloss-Symbol und "https://" in der Website-Adresse, die auf eine sichere Verbindung hinweisen.
- Seien Sie vorsichtig mit Social Engineering: Hüten Sie sich vor unaufgeforderten Anrufen, Nachrichten oder E-Mails, in denen nach persönlichen Daten oder

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

finanziellen Details gefragt wird. Seriöse Organisationen fragen nicht unaufgefordert nach solchen Informationen

- Sichern Sie Ihre Daten regelmäßig: Erstellen Sie Sicherungskopien Ihrer wichtigen Dateien und Daten auf einem separaten Speichergerät oder bei einem Cloud-Dienst. So schützen Sie sich vor Datenverlusten aufgrund von Hardwareausfällen, Diebstahl oder Ransomware-Angriffen.
- Aktivieren Sie die Zwei-Faktoren-Authentifizierung (2FA): Aktivieren Sie 2FA, wenn verfügbar. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen, indem zusätzlich zu Ihrem Passwort ein zweiter Verifizierungsschritt erforderlich ist, z. B. ein eindeutiger Code, der an Ihr Mobilgerät gesendet wird.
- Achten Sie auf die Weitergabe in sozialen Medien: Seien Sie vorsichtig, wenn Sie persönliche Informationen, Standortangaben oder Urlaubspläne auf sozialen Medienplattformen teilen. Wenn Sie zu viele Informationen weitergeben, können Cyber-Kriminelle oder potenzielle Einbrecher wertvolle Informationen erhalten.
- Sichern Sie Ihre mobilen Geräte: Verwenden Sie Sicherheitsfunktionen wie Passcodes, Fingerabdrücke oder Gesichtserkennung, um Ihre Smartphones und Tablets zu sperren. Installieren Sie seriöse Sicherheits-Apps, die Funktionen wie Fernverfolgung und Löschung bei Verlust oder Diebstahl bieten.
- Vertrauen Sie auf Ihre Instinkte: Wenn etwas zu schön ist, um wahr zu sein, oder Ihnen verdächtig vorkommt, vertrauen Sie auf Ihre Instinkte. Seien Sie skeptisch bei unerwarteten Angeboten, Geldforderungen oder dringenden Bitten um persönliche Informationen.
- Löschen Sie regelmäßig Ihre Browsing-Daten: Löschen Sie regelmäßig Ihren Browserverlauf, Cookies und zwischengespeicherte Daten. Dies trägt zum Schutz Ihrer Privatsphäre bei, da gespeicherte Informationen entfernt werden, auf die Unbefugte möglicherweise zugreifen könnten.

2.2. Verbesserung der Online-Sicherheit mit sicheren Browsing-Tools

Die Verbesserung der Online-Sicherheit mit sicheren Browsing-Tools ist ein wichtiger Aspekt der Cybersicherheit. Durch den Einsatz dieser Tools können Sie Ihre Privatsphäre schützen, Ihre persönlichen Daten sichern und das Risiko von Online-Bedrohungen verringern. Im Folgenden finden Sie einige wichtige Tipps, wie Sie Ihre Online-Sicherheit mit sicheren Browsing-Tools erhöhen können:

- Installieren und verwenden Sie einen vertrauenswürdigen Webbrowser: Wählen Sie einen seriösen Webbrowser, wie Google Chrome, Mozilla Firefox oder Microsoft Edge. Diese Browser legen Wert auf Sicherheit und veröffentlichen regelmäßig Updates, um Sicherheitslücken zu schließen.
- Aktivieren Sie die Sicherheitsfunktionen des Browsers: Machen Sie sich mit den Sicherheitsfunktionen Ihres Webbrowsers vertraut. Aktivieren Sie Funktionen wie Popup-Blocker, Safe-Browsing-Modus und Datenschutzeinstellungen, um Ihre Online-Sicherheit zu erhöhen.
- Aktivieren Sie den Phishing- und Malware-Schutz: Aktivieren Sie die integrierten Phishing- und Malware-Schutzfunktionen Ihres Webbrowsers. Diese Funktionen

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

können Sie vor verdächtigen Websites warnen und Sie davon abhalten, bekannte bösartige Websites zu besuchen.

- Bleiben Sie informiert und auf dem neuesten Stand: Informieren Sie sich über die neuesten Online-Bedrohungen und die besten Praktiken für sicheres Surfen. Lesen Sie regelmäßig verlässliche Quellen, wie z. B. seriöse Cybersicherheits-Websites oder Blogs, um über die sich entwickelnde Landschaft der Online-Sicherheit auf dem Laufenden zu bleiben.

Unit 3: Gesundheit und Wohlbefinden im digitalen Zeitalter

3.1. Risiken von übermäßiger Bildschirmzeit und digitaler Abhängigkeit

Um die Risiken von übermäßiger Bildschirmzeit und digitaler Abhängigkeit zu mindern, gibt es einige Strategien und Praktiken, die Sie berücksichtigen sollten:

- Begrenzen Sie die Bildschirmzeit: Legen Sie bestimmte Zeitlimits für die Bildschirmnutzung fest, sowohl für Freizeitaktivitäten als auch für arbeitsbezogene Aufgaben. Dies hilft, ein gesundes Gleichgewicht zwischen Bildschirmzeit und anderen Aktivitäten zu schaffen.
- Machen Sie regelmäßig Pausen: Bauen Sie regelmäßige Pausen vom Bildschirm in Ihren Tagesablauf ein. Stehen Sie auf, strecken Sie sich und gehen Sie körperlichen Aktivitäten oder Hobbys nach, die nichts mit digitalen Geräten zu tun haben.
- Praktizieren Sie Digital Detox: Legen Sie bestimmte Zeiträume fest, z. B. Wochenenden oder Abende, in denen Sie sich vollständig von digitalen Geräten abkoppeln. Nutzen Sie diese Zeit für Offline-Aktivitäten, verbringen Sie Zeit mit Ihren Lieben oder gehen Sie Ihren Hobbys nach.
- Achtsamer Umgang mit Technologie: Achten Sie darauf, wie Sie Technologie nutzen und welche Auswirkungen sie auf Ihr Wohlbefinden hat. Denken Sie über Ihre digitalen Gewohnheiten nach, bewerten Sie deren Auswirkungen auf Ihr Leben und treffen Sie bewusste Entscheidungen, um die negativen Folgen zu minimieren.
- Suchen Sie Unterstützung und Rechenschaftspflicht: Teilen Sie Ihre Bedenken mit vertrauenswürdigen Familienmitgliedern, Freunden oder Selbsthilfegruppen. Legen Sie eine gegenseitige Rechenschaftspflicht fest, um einen verantwortungsvollen Umgang mit der Technologie zu fördern und Unterstützung bei der Beibehaltung gesunder Gewohnheiten zu bieten.
- Setzen Sie digitale Grenzen: Legen Sie klare Grenzen für die Technologienutzung fest, z. B. das Abschalten von Benachrichtigungen zu bestimmten Zeiten, die Vermeidung von Bildschirmzeit vor dem Schlafengehen oder Richtlinien für die Gerätenutzung während der Familienmahlzeiten.

Denken Sie daran, dass es darum geht, ein gesundes Verhältnis zur Technologie zu entwickeln und sicherzustellen, dass sie Ihr Leben bereichert und nicht zu einer Quelle übermäßiger Abhängigkeit wird. Durch die Umsetzung dieser Strategien können Sie die mit übermäßiger Bildschirmnutzung verbundenen Risiken mindern und einen ausgewogeneren und erfüllteren Lebensstil fördern**.**

3.2. Gesundheit und digitale Werkzeuge

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Die Technologie bietet zahlreiche Möglichkeiten zur Unterstützung und Verbesserung Ihrer Gesundheit. Hier sind einige Möglichkeiten, wie die Technologie Ihnen bei Ihrer Gesundheit helfen kann:

- Zugang zu Informationen: Das Internet bietet eine Fülle von gesundheitsbezogenen Informationen, die es Ihnen ermöglichen, Symptome, Erkrankungen, Behandlungen und Präventionsmaßnahmen zu recherchieren. Zuverlässige Websites, Gesundheits-Apps und Online-Communitys können Sie dabei unterstützen, fundierte Entscheidungen über Ihre Gesundheit zu treffen.
- Gesundheitsüberwachung: Tragbare Geräte wie Fitness-Tracker und Smartwatches können verschiedene Aspekte Ihrer Gesundheit überwachen, darunter Herzfrequenz, Schlafverhalten, körperliche Aktivität und Kalorienverbrauch. Diese Geräte können wertvolle Einblicke in Ihr allgemeines Wohlbefinden geben und Ihnen helfen, Fortschritte bei der Erreichung Ihrer Gesundheitsziele zu verfolgen.
- Telemedizin und Fernkonsultationen: Telemedizinische Dienste ermöglichen es Ihnen, Fachkräfte des Gesundheitswesens aus der Ferne per Videoanruf oder Online-Chat zu konsultieren. Diese bequeme Methode spart Zeit und kann besonders bei Folgeterminen, Routineuntersuchungen oder nicht dringenden medizinischen Konsultationen von Vorteil sein.
- Verwaltung von Medikamenten: Mobile Apps und intelligente Pillenplaner können Ihnen bei der Verwaltung von Medikamenten helfen, indem sie Sie an die Einnahme von Pillen erinnern, Medikamentenpläne verfolgen und Sie über Nachfüllungen von Medikamenten informieren. Diese Technologie kann verhindern, dass die Einnahme von Medikamenten vergessen wird, und die Einhaltung von Medikamentenregimen fördern.
- Unterstützung für die psychische Gesundheit: Verschiedene Apps und Online-Plattformen für psychische Gesundheit bieten Ressourcen zur Bewältigung von Stress, Angst und Depression. Dazu gehören geführte Meditationen, Atemübungen, Stimmungsmessungen und Therapiesitzungen, die über digitale Plattformen durchgeführt werden.
- Verwaltung von Gesundheitsakten: Mit digitalen Gesundheitsakten und Patientenportalen können Sie auf Ihre Krankengeschichte, Testergebnisse und Terminpläne zugreifen und diese verwalten. Dies vereinfacht die Kommunikation mit den Gesundheitsdienstleistern und gewährleistet die Kontinuität der Versorgung.
- Unterstützung und Motivation: Online-Communities und Social-Media-Plattformen, die sich mit Gesundheit und Wellness beschäftigen, können Unterstützung, Motivation und Ermutigung bieten. Der Kontakt zu Gleichgesinnten kann das Gemeinschaftsgefühl fördern und Ihnen helfen, Ihre Gesundheitsziele zu verfolgen.
- Gesundheitsverfolgung und Datenanalyse: Die Technologie ermöglicht es Ihnen, Gesundheitsdaten wie Blutdruck, Blutzuckerspiegel oder Gewicht über einen längeren Zeitraum zu verfolgen und zu analysieren. Durch die Überwachung von Trends und Mustern können Sie verbesserungswürdige Bereiche erkennen und die notwendigen Anpassungen zur Optimierung Ihrer Gesundheit vornehmen.

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Denken Sie daran, dass Technologie zwar ein wertvolles Hilfsmittel zur Unterstützung Ihrer Gesundheit sein kann, dass es aber wichtig ist, sie mit Bedacht und in Verbindung mit professioneller medizinischer Beratung einzusetzen. Wenden Sie sich immer an medizinisches Fachpersonal, um eine genaue Diagnose, Behandlungsempfehlungen und persönliche Beratung zu erhalten.

5 Glossareinträge

Cybersicherheit bezieht sich auf die Praxis des Schutzes von Computersystemen, Netzwerken und digitalen Informationen vor unbefugtem Zugriff, Diebstahl und Schaden. Sie umfasst die Umsetzung von Maßnahmen zur Verhinderung von Cyber-Bedrohungen wie Hacking, Datenverletzungen und Malware-Angriffen. Ziel der Cybersicherheit ist es, die Vertraulichkeit, Integrität und Verfügbarkeit digitaler Werte zu gewährleisten und Einzelpersonen und Organisationen vor potenziellen Risiken und Schwachstellen in der vernetzten digitalen Welt zu schützen.

Unter Identitätsdiebstahl versteht man den betrügerischen Erwerb und die Verwendung von persönlichen Informationen einer Person, wie z. B. Name, Sozialversicherungsnummer oder finanzielle Details, ohne deren Zustimmung. Dabei gibt man sich als das Opfer aus, um verschiedene illegale Aktivitäten wie Finanzbetrug, unberechtigte Einkäufe oder andere Formen von identitätsbezogenen Straftaten zu begehen.

Social Engineering ist eine manipulative Technik, die von Cyberkriminellen eingesetzt wird, um Menschen zu täuschen und ihr Vertrauen und ihre Gefühle auszunutzen. Es beinhaltet eher psychologische Manipulation als technische Methoden, um Menschen dazu zu bringen, sensible Informationen preiszugeben oder Handlungen auszuführen, die ihre Sicherheit gefährden könnten. Beispiele für Social-Engineering-Techniken sind Phishing-E-Mails, Telefonbetrug, Vortäuschung falscher Tatsachen und Impersonation. Ziel des Social Engineering ist es, menschliches Verhalten zu manipulieren, um unbefugten Zugang zu Systemen, Netzwerken oder persönlichen Informationen zu erhalten.

5 Multiple-Choice-Fragen zur Selbsteinschätzung

1. Im Bereich der Cybersicherheit beziehen sich die Risiken auf:
a) Mögliche Gefahren beim Onlinegang.
b) Physische Sicherheitsmaßnahmen.
c) Vorkehrungen gegen rutschige Böden.
d) Sichere Online-Praktiken.
Richtige Option: a

2. Welche Arten von Cyber-Bedrohungen gibt es?
a) Physische Angriffe auf Computer.
b) Tricks oder Fallen, die von bösen Menschen im Internet verwendet werden.
c) Sicherheitsmaßnahmen für das Online-Shopping.
d) Strategien zum Schutz persönlicher Daten.
Richtige Option: b

3. Was ist Social Engineering?

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

a) Eine von Cyberkriminellen verwendete Technik.
b) Das Studium des menschlichen Verhaltens.
c) Ein sicheres Browsing-Tool.
d) Eine Art von Computervirus.
Richtige Option: a

4. **Wie können Sie die Online-Sicherheit mit Tools zum sicheren Surfen verbessern?**

a) Durch die Verwendung seriöser Webbrowser und die Aktivierung von Sicherheitsfunktionen.
b) Durch zunehmende Bildschirmzeit und digitale Abhängigkeit.
c) durch die Weitergabe persönlicher Informationen in sozialen Medien.
d) Durch Ignorieren von Phishing-E-Mails und Malware-Warnungen.
Richtige Option: a

5. **Welche Strategien gibt es, um die Risiken einer übermäßigen Bildschirmnutzung zu mindern?**

a) Begrenzung der Bildschirmzeit und regelmäßige Pausen.
b) Verstärkter Einsatz von Technologie für eine bessere Gesundheit.
c) Vollständiger Verzicht auf digitale Geräte.
d) Suche nach Unterstützung und Verantwortlichkeit.
Richtige Option: a

Bibliographie und weitere Referenzen

- https://staysafeonline.org/
- https://www.consumer.ftc.gov/topics/online-security
- https://www.cisa.gov/cybersecurity
- https://www.getsafeonline.org/
- https://us.norton.com/internetsecurity
- https://www.staysmartonline.gov.au/
- https://www.commonsense.org/education/digital-citizenship/privacy-and-security

Zugehöriges Material	BOOMER_Cyber_security_DE
Referenz-Link	
Video im Powtoon-Format	https://www.youtube.com/watch?v=lvLhhqDhZJY

Co-funded by the European Union

Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.