Modul Steckbrief

Titel	Sicherheit im Internet: Do's und Don'ts
Keywords	Internet, Sicherheit, online, offline, Passwörter, Privatsphäre
Bereitgestellt von	Internet Web Solutions
Sprache	Deutsch

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

Ziele / Lernergebnisse

Am Ende dieses Moduls werden Sie:

- die Bedeutung eines verantwortungsvollen Online-Verhaltens zu verstehen
- Erkennen allgemeiner Online-Risiken
- Erkennen Sie die Vorteile des Internets
- Lernen Sie die besten Praktiken zur Online-Sicherheit
- Entwicklung digitaler Kompetenzen

Beschreibung

Dieser Kurs bietet einen umfassenden Überblick über den sicheren Umgang mit dem Internet und gibt praktische Ratschläge, was im Internet zu tun und zu lassen ist. Dazu gehören Tipps zu sicheren Verbindungen, zur Passwortverwaltung, zu Datenschutzeinstellungen für soziale Medien, zu sicheren Online-Einkaufspraktiken und zum Erkennen und Vermeiden von Betrug und Abzocke. Wenn Sie diese Richtlinien befolgen, können Sie sich sicher in der Online-Welt bewegen und sich vor potenziellen Bedrohungen schützen.

Inhaltsindex (3 Stufen)

Modul: Sicherheit im Internet: Do's und Don'ts
Unit 1: Einführung in die Online-Sicherheit
1.1. Was bedeutet es, online sicher zu sein?
1.2. Welche Risiken birgt die unsichere Internetnavigation?
1.3. Warum sollten Sie trotz dieser Risiken nicht aufhören, im Internet zu surfen?

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 2: Gebote und Verbote im Internet
2.1. Sichere Verbindungen
2.2. Passwörter
2.3. Datenschutz und soziale Medien
2.4. Online-Einkauf
2.5. Betrügereien und Schwindel

Unit 3: Bonus-Track: Offline-Do's und Don'ts
3.1. Digitale Geräte

Inhalt entwickelt

Modul: Sicherheit im Internet: Do's und Don'ts

Unit 1: Einführung in die Online-Sicherheit

Abschnitt 1.1: Was bedeutet es, online sicher zu sein?
Sicher im Internet zu sein bedeutet, Vorsichtsmaßnahmen zu ergreifen und sich bei der Nutzung des Internets verantwortungsvoll zu verhalten. Dazu gehört es, die **potenziellen Risiken und Bedrohungen** im Zusammenhang mit Online-Aktivitäten zu verstehen und zu bewältigen, um persönliche Daten, finanzielle Ressourcen und das allgemeine Wohlbefinden zu schützen.

Der Cyberspace ist wie eine Autobahn: Man muss ihn sicher befahren, um Unfälle zu vermeiden. Genau wie das Anlegen des Sicherheitsgurtes können einige grundlegende Sicherheitsmaßnahmen im Internet dazu beitragen, dass Ihr Online-Erlebnis sicher und angenehm ist.

Die Sicherheit im Internet ist aus mehreren Gründen wichtig. Es hilft, **Ihre persönlichen Daten** davor zu schützen, in die falschen Hände zu geraten. Persönliche Daten wie Ihr Name, Ihre Adresse, Ihre Telefonnummer und finanzielle Informationen können für Identitätsdiebstahl, Betrug oder andere bösartige Aktivitäten verwendet werden, wenn Cyberkriminelle darauf zugreifen. Ihre Online-Präsenz trägt zu Ihrem Ruf bei, sowohl persönlich als auch beruflich.

Wenn Sie online sicher sind, können Sie **die Verbreitung unangemessener oder schädlicher Inhalte verhindern**, die sich negativ auf Ihr Image und Ihre Beziehungen auswirken können. Die Gewährleistung Ihrer Online-Sicherheit garantiert den **Schutz Ihrer Privatsphäre** und **schützt Sie vor finanziellen Betrügereien und Scams**.

Ein sicheres Online-Verhalten hilft auch dabei, **Fälle von Cybermobbing und Belästigung zu vermeiden**. Durch die Umsetzung von Sicherheitsmaßnahmen können Sie das Risiko verringern, schädlichen Personen oder Situationen zu begegnen, die zu emotionalem Leid oder Schaden führen können. Die Online-Sicherheit ist auch für den

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.

Schutz von Kindern und die Gewährleistung ihres Wohlbefindens in der digitalen Welt entscheidend.

Abschnitt 1.2: Welche Risiken birgt die unsichere Internetnavigation?

Eine unsichere Internetnavigation birgt Risiken für ältere Menschen. Sie sind möglicherweise weniger vertraut mit Online-Plattformen und Bedrohungen, weshalb es wichtig ist, die spezifischen Risiken zu verstehen, denen sie ausgesetzt sind.

Einige häufige Risiken sind:

- **Phishing und Betrug**: Ältere Menschen sind anfälliger für Phishing-E-Mails, betrügerische Websites und Telefonbetrügereien, bei denen Betrüger sie zur Preisgabe vertraulicher Informationen verleiten.
- **Identitätsdiebstahl**: Eine unsichere Internetnavigation erhöht das Risiko des Diebstahls persönlicher Daten und der Identität, was zu finanziellen Verlusten und Störungen im Leben der Betroffenen führt.
- **Finanzieller Betrug**: Ältere Menschen werden mit gefälschten Investitionsplänen, Lotteriebetrügereien oder betrügerischen Einkäufen angesprochen, wobei ihr Vertrauen und ihre Verletzlichkeit ausgenutzt werden.
- **Malware und Viren**: Unsicheres Navigieren im Internet kann zum unbeabsichtigten Herunterladen von Schadsoftware führen, die die Sicherheit des Geräts und persönliche Daten gefährdet.
- **Online-Belästigung und Cybermobbing**: Ältere Menschen können aufgrund von Online-Belästigung unter emotionalem Stress und Problemen des geistigen Wohlbefindens leiden.
- **Verstöße gegen den Datenschutz**: Unzureichende Datenschutzpraktiken können persönliche Informationen preisgeben, was zu Identitätsdiebstahl oder unerwünschten Anfragen führen kann.
- **Betrug beim technischen Support**: Ältere Menschen sind anfälliger für Betrügereien, bei denen sich Betrüger*innen als Vertreter*innen des technischen Kundendienstes ausgeben.
- **Mangelnde digitale Kompetenz: Die** unsichere Internetnutzung wird durch die mangelnde digitale Kompetenz älterer Menschen noch verschlimmert, was sie anfälliger für Bedrohungen und Betrug macht.

Ältere Menschen sollten sich dieser Risiken bewusst sein und proaktiv Maßnahmen ergreifen, um sie zu vermeiden, indem sie beispielsweise Hilfe und Unterstützung von vertrauten Personen suchen oder Bedenken bei den zuständigen Behörden oder Plattformen melden.

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.

Abschnitt 1.3: Warum sollten Sie trotz dieser Risiken nicht aufhören, im Internet zu surfen?

Sicherheit im Internet ist wichtig, aber sie muss nicht stressig sein. Sensibilisierung ist ein wichtiger erster Schritt, um sich zusammen mit einer zuverlässigen Antiviren-Software (viele davon sind kostenlos!) zu schützen.

Sie sollten trotz der Online-Risiken nicht völlig auf das Internet verzichten, denn das Netz kann enorme Vorteile für Ihr Wohlbefinden und Ihre soziale Integration haben. Das Internet bietet eine riesige Menge an **Informationen und Ressourcen**, von denen Sie stark profitieren können. Es bietet Zugang zu Nachrichten, Bildungsmaterialien, Gesundheitsressourcen, Kommunikationsmitteln und verschiedenen Online-Diensten.

Was die **sozialen Kontakte angeht**, so ermöglicht das Internet, mit Familie, Freunden und Gemeinschaften in Verbindung zu bleiben, vor allem wenn physische Mobilität oder Entfernung ein Hindernis darstellen. Soziale Medienplattformen, Videoanrufe und Online-Foren ermöglichen es, Beziehungen zu pflegen, Erfahrungen auszutauschen und Isolation oder Einsamkeit zu bekämpfen. Online-Plattformen bieten Komfort und **Unabhängigkeit** für alle Menschen in verschiedenen Bereichen des täglichen Lebens. Sie können **online einkaufen, auf Online-Bankdienste zugreifen, Termine vereinbaren und Medikamente bestellen, was** mehr Bequemlichkeit bietet und **die Notwendigkeit von Reisen oder Hilfe verringert**.

Das Navigieren ist auch eine Quelle der **kognitiven Stimulation und des geistigen Engagements**, da es die Möglichkeit bietet, zu lernen, zu spielen, an virtuellen Hobbys oder Gemeinschaften teilzunehmen und geistig aktiv zu bleiben, was zum allgemeinen Wohlbefinden beitragen kann.

Wenn Sie sich im Internet zurechtfinden und sichere Online-Praktiken anwenden, können Sie **digitale Kompetenzen entwickeln**, Ihr Selbstvertrauen stärken und sich ein Gefühl der **Selbstbestimmung** bewahren. Das Internet bietet eine Fülle von **Lernressourcen**, darunter Online-Kurse, Tutorials und Bildungsplattformen. Sie können neue Interessen erkunden, sich neue Fähigkeiten aneignen und an Möglichkeiten des lebenslangen Lernens teilnehmen, was Ihre persönliche Entwicklung und intellektuelle Stimulation fördert.

Es ist zwar wichtig, sich der Online-Risiken bewusst zu sein und Vorsichtsmaßnahmen zu ergreifen, aber ein **vollständiger Verzicht auf das Internet kann zu Isolation, eingeschränktem Zugang zu Ressourcen und verpassten Chancen führen**.

Unit 2: Gebote und Verbote im Internet

Abschnitt 2.1: Sichere Verbindungen

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.

Do's:

Verwenden Sie sichere Wi-Fi-Netzwerke: Verbinden Sie sich wann immer möglich mit sicheren und vertrauenswürdigen Wi-Fi-Netzwerken. Diese Netzwerke erfordern in der Regel ein Kennwort und eine Verschlüsselung und bieten eine sicherere Umgebung zum Surfen. Vermeiden Sie den Zugriff auf sensible Konten oder die Durchführung von Finanztransaktionen über öffentliche Wi-Fi-Netzwerke.

Überprüfen Sie die Sicherheit der Website: Vergewissern Sie sich vor der Eingabe vertraulicher Daten oder vor Online-Transaktionen, dass die Website über eine sichere Verbindung verfügt. Achten Sie auf "https://" in der Adresse der Website und ein Vorhängeschloss-Symbol in der Adressleiste des Browsers.

Halten Sie die Software auf dem neuesten Stand: Aktualisieren Sie regelmäßig das Betriebssystem Ihres Geräts, die Webbrowser und die Sicherheitssoftware. Software-Updates enthalten oft Sicherheits-Patches, die vor bekannten Sicherheitslücken schützen.

Verwenden Sie einen Firewall-Schutz: Aktivieren und warten Sie eine Firewall auf Ihrem Computer oder Router, um eine Barriere gegen unbefugten Zugriff und potenzielle Bedrohungen aus dem Internet zu schaffen.

Verbote:

Geben Sie keine sensiblen Informationen weiter: Vermeiden Sie die Eingabe sensibler Informationen wie Passwörter, Kreditkartendaten oder Sozialversicherungsnummern.

Vermeiden Sie verdächtige Websites: Vermeiden Sie den Besuch verdächtiger oder unbekannter Websites. Bleiben Sie bei Ihren Online-Aktivitäten auf seriösen und vertrauenswürdigen Websites.

Ignorieren Sie keine Browser-Warnungen: Achten Sie auf Browserwarnungen und Hinweise auf potenzielle Sicherheitsrisiken oder nicht vertrauenswürdige Websites.

Keine automatische Verbindung zu Netzwerken herstellen: Deaktivieren Sie die automatische Verbindungsfunktion auf Ihren Geräten, da sie sich möglicherweise automatisch und ohne Ihr Wissen mit ungesicherten Netzwerken verbinden.

Abschnitt 2.2: Passwörter

Do's:

Erstellen Sie sichere und eindeutige Passwörter: Verwenden Sie sichere und eindeutige Passwörter für jedes Online-Konto. Es sollte eine Kombination aus Groß-

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.

und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Vermeiden Sie die Verwendung von erratbaren Informationen wie Geburtstagen oder Namen.

Wählen Sie lange Passwörter: Entscheiden Sie sich für längere Passwörter, da diese im Allgemeinen sicherer sind. Sie sollten mindestens 12 Zeichen lang sein. Ziehen Sie Passphrasen in Erwägung: eine Reihe von Wörtern oder einen Satz, der leichter zu merken, aber für andere schwer zu erraten ist. Zum Beispiel: "MeineLieblingsfarbeIstBlau".

Aktivieren Sie die Zwei-Faktoren-Authentifizierung (2FA): Aktivieren Sie, wann immer möglich, die Zwei-Faktor-Authentifizierung für Ihre Online-Konten. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen, indem ein zweiter Verifizierungsschritt erforderlich ist, z. B. ein eindeutiger Code, der an Ihr Mobilgerät gesendet wird.

Passwörter regelmäßig aktualisieren: Ändern Sie Ihre Passwörter regelmäßig, am besten alle paar Monate.

Verbote:

Passwörter nicht wiederverwenden: Verwenden Sie niemals dasselbe Passwort für mehrere Konten. Wenn ein Konto kompromittiert wird, kann es möglicherweise auch Zugang zu anderen Konten gewähren. Verwenden Sie für jeden Online-Dienst und jede Plattform ein eigenes Passwort.

Vermeiden Sie gängige Passwörter: Vermeiden Sie gängige oder einfache Passwörter wie "123456", "password" oder "qwerty". Diese Passwörter sind oft das Ziel von Hackern und können leicht geknackt werden.

Passwörter nicht weitergeben oder aufschreiben: Geben Sie Ihre Passwörter nicht an andere weiter, auch nicht an Verwandte oder Freunde. Vermeiden Sie es außerdem, Passwörter auf Notizzetteln aufzuschreiben oder sie in leicht zugänglichen digitalen Dateien zu speichern.

Speichern Sie keine Passwörter in Browsern: Speichern Sie keine Passwörter in Webbrowsern oder verwenden Sie nicht die "Remember Me"-Funktion. Das mag zwar bequem sein, stellt aber ein Sicherheitsrisiko dar, wenn sich jemand unbefugt Zugang zu Ihrem Gerät verschafft.

Abschnitt 2.3: Datenschutz und soziale Medien
Do's:

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.

Prüfen Sie die Datenschutzeinstellungen: Machen Sie sich mit den Datenschutzeinstellungen der von Ihnen genutzten Social-Media-Plattformen vertraut. Passen Sie die Einstellungen an, um zu kontrollieren, wer Ihr Profil, Ihre Beiträge und Ihre persönlichen Informationen sehen kann. Erwägen Sie, den Zugriff auf vertrauenswürdige Freunde und Familienmitglieder zu beschränken.

Seien Sie selektiv bei Freundschaftsanfragen: Seien Sie vorsichtig, wenn Sie Freundschaftsanfragen oder Verbindungsanfragen von unbekannten Personen annehmen. Überprüfen Sie die Identität der Person, bevor Sie ihre Anfrage annehmen.

Denken Sie nach, bevor Sie teilen: Seien Sie vorsichtig, wenn Sie persönliche Informationen, Fotos oder Updates auf sozialen Medienplattformen teilen. Vermeiden Sie es, sensible Details wie Ihre vollständige Adresse, Telefonnummer oder finanzielle Informationen öffentlich zu teilen.

Regelmäßige Überprüfung und Aktualisierung der Freundesliste: Überprüfen Sie regelmäßig Ihre Freundes- oder Verbindungsliste auf sozialen Medienplattformen. Entfernen Sie Personen, denen Sie nicht mehr vertrauen oder die Sie nicht mehr erkennen.

Verbote:

Klicken Sie nicht auf verdächtige Links: Seien Sie vorsichtig, wenn Sie auf Links klicken, die in sozialen Medien geteilt werden, insbesondere auf solche von unbekannten oder verdächtigen Quellen. Diese Links können zu Phishing-Websites oder Malware-Downloads führen. Überprüfen Sie die Quelle, bevor Sie klicken.

Seien Sie vorsichtig bei Anwendungen von Drittanbietern: Seien Sie wählerisch, wenn Sie Anwendungen von Drittanbietern, die Zugriff auf Ihre Konten in sozialen Medien verlangen, Berechtigungen erteilen. Prüfen Sie die angeforderten Berechtigungen und berücksichtigen Sie die Glaubwürdigkeit der Anwendung, bevor Sie den Zugriff gewähren.

Vermeiden Sie die Bekanntgabe persönlicher Ereignisse: Vermeiden Sie es, bevorstehende Urlaube oder längere Abwesenheit von zu Hause auf Social-Media-Plattformen anzukündigen. Dies könnte potenzielle Einbrecher oder Kriminelle darauf aufmerksam machen, dass Ihr Haus unbewohnt ist.

Abschnitt 2.4: Online-Einkauf
Do's:

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.

Kaufen Sie auf vertrauenswürdigen Websites ein: Halten Sie sich beim Einkaufen an seriöse und bekannte Online-Händler. Achten Sie auf Websites mit positiven Kundenrezensionen und sicheren Zahlungsoptionen wie Kreditkarten oder seriösen Zahlungsplattformen.

Überprüfen Sie die Sicherheit der Website: Vergewissern Sie sich vor der Eingabe von Zahlungs- oder persönlichen Daten, dass die Website über eine sichere Verbindung verfügt. Achten Sie auf "https://" in der Adresse der Website und ein Vorhängeschloss-Symbol in der Adressleiste des Browsers.

Behalten Sie den Überblick über Ihre Transaktionen: Führen Sie Aufzeichnungen über Ihre Online-Einkaufstransaktionen, einschließlich Auftragsbestätigungen, Quittungen und Kontrollnummern. So können Sie Lieferungen nachverfolgen und eventuell auftretende Probleme lösen.

Verbote:

Geben Sie keine unnötigen Informationen weiter: Seien Sie vorsichtig mit der Weitergabe unnötiger persönlicher Informationen während des Bestellvorgangs. Einzelhändler verlangen in der Regel grundlegende Angaben wie Lieferadresse und Zahlungsinformationen.

Vorsicht vor Phishing-E-Mails oder Links: Seien Sie misstrauisch gegenüber E-Mails oder Nachrichten, die vorgeben, von Online-Händlern zu stammen, vor allem, wenn sie nach persönlichen Daten fragen oder Sie auf verdächtige Links klicken lassen.

Vermeiden Sie ungesicherte Wi-Fi-Netzwerke für Transaktionen: Vermeiden Sie bei Online-Einkäufen die Nutzung ungesicherter oder öffentlicher Wi-Fi-Netzwerke. Diese Netzwerke können anfällig für Hacker sein, die Ihre persönlichen und finanziellen Daten abfangen könnten.

Fallen Sie nicht auf Betrügereien mit falschen Namen herein: Seien Sie vorsichtig bei Online-Verkäufern, die sich als seriöse Marken ausgeben oder mit betrügerischen Methoden versuchen, an Ihre persönlichen oder finanziellen Daten zu gelangen. Überprüfen Sie die Echtheit des Verkäufers und seiner Website, bevor Sie einen Kauf tätigen.

Abschnitt 2.5: Betrügereien und Schwindel
Do's:

Seien Sie skeptisch und wachsam: Bewahren Sie sich eine gesunde Skepsis, wenn Sie unaufgefordert E-Mails, Anrufe oder Nachrichten erhalten, in denen Sie um persönliche Informationen gebeten oder seltsame Angebote gemacht werden.

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.

Überprüfen Sie die Legitimität der Quelle, bevor Sie Informationen weitergeben oder finanzielle Verpflichtungen eingehen.

Bilden Sie sich weiter: Informieren Sie sich über gängige Online-Betrügereien und Betrugstaktiken, die auf ältere Menschen abzielen. Machen Sie sich mit den Anzeichen von Betrügereien vertraut, z. B. Zahlungsaufforderungen über unkonventionelle Methoden oder Druck, schnell zu handeln.

Überprüfen Sie die Identität der Kontaktperson: Wenn Einzelpersonen behaupten, Organisationen zu vertreten, fragen Sie nach offiziellen Kontaktinformationen und bestätigen Sie deren Authentizität, indem Sie sich direkt an die Organisation wenden und die verifizierten Kontaktdaten verwenden.

Wenden Sie sich an vertrauenswürdige Personen: Wenn Sie eine verdächtige Anfrage erhalten oder sich in einer ungewohnten Situation befinden, wenden Sie sich an ein vertrauenswürdiges Familienmitglied, einen Freund oder einen Fachmann.

Ignorieren Sie unaufgeforderte Anrufe und "Robocalls". Behandeln Sie unaufgeforderte Telefonanrufe mit Skepsis. Eine lebende Person oder eine aufgezeichnete Stimme gibt Ihnen falsche Informationen, die wichtig und zeitkritisch klingen. Sie behaupten vielleicht, ein Verwandter in Schwierigkeiten zu sein, dass die Garantie für Ihr Auto abläuft und eine Zahlung erforderlich ist, oder sie stellen sich als "technischer Support" vor und sagen Ihnen, dass Ihr PC gegen eine Gebühr repariert werden muss.

Verbote:

Überstürzen Sie nichts und fühlen Sie sich nicht unter Druck gesetzt: Betrüger*innen verwenden oft Taktiken, um ein Gefühl der Dringlichkeit oder des Drucks zu erzeugen und die Opfer zu schnellen, unüberlegten Entscheidungen zu zwingen. Nehmen Sie sich Zeit, stellen Sie Nachforschungen an und seien Sie vorsichtig, bevor Sie finanzielle Verpflichtungen eingehen.

Schicken Sie kein Geld an unbekannte Personen: Seien Sie vorsichtig bei Geldanfragen oder Überweisungen von Personen, die Sie nicht persönlich kennen. Überprüfen Sie die Identität und Legitimität der Person, bevor Sie finanzielle Transaktionen durchführen.

Klicken Sie nicht auf Links in E-Mails von unbekannten Absendern. Seien Sie vorsichtig bei seltsamen oder unerwarteten Nachrichten, selbst wenn sie von Personen stammen, die Sie kennen. Sie könnten bösartige oder Phishing-Links enthalten. Wenn eine Nachricht verdächtig aussieht, aber von einer Person zu

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.

stammen scheint, die Sie kennen und der Sie vertrauen, fragen Sie nach, bevor Sie darauf klicken.

Öffnen Sie keine Anhänge. Öffnen Sie keine Anhänge, die Sie nicht erwarten oder die von einem unbekannten Kontakt stammen - insbesondere, wenn sie die Erweiterung .exe oder .zip haben. Wenn die Datei(en) von einem Freund oder einem Familienmitglied zu stammen scheint (scheinen), fragen Sie sie, ob sie Ihnen etwas geschickt haben. Diese Sicherheitsregel gilt auch für Anhänge, die über Textnachrichten und soziale Medien verschickt werden.

Klicken Sie nicht auf Pop-up-Fenster auf Ihrem Telefon oder Computer. Eine gängige Popup-Masche ist Scareware, die mit Popup-Sicherheitswarnungen versucht, Sie dazu zu bringen, gefälschte Software herunterzuladen oder dafür zu bezahlen, die als echter Cybersicherheitsschutz getarnt ist. So erscheint beispielsweise eine Warnung, die Ihnen mitteilt, dass Ihr Gerät gefährdet ist und repariert werden muss. Wenn Sie den Support anrufen, bitten die Betrüger*innen Sie möglicherweise um Fernzugriff auf Ihren Computer und verlangen eine Gebühr. Eine weitere Malware-Technik ist die Verwendung trügerischer "Schließen"- oder "X"-Schaltflächen, die automatisch einen Virus installieren, wenn Sie darauf klicken.

Unit 3: Bonustrack: Offline-Do's und -Don'ts

Abschnitt 3.1: Digitale Geräte
Do's:

Sperren Sie Ihre Geräte. Stellen Sie sicher, dass Geräte mit Zugang zu sensiblen Daten automatisch gesperrt werden und zur Reaktivierung ein Passwort erfordern. Stellen Sie sicher, dass der heimische WLAN-Router und die Zugangspunkte mit eindeutigen Benutzernamen und Passwörtern konfiguriert sind, die nicht den Standardpasswörtern entsprechen.

Sichern Sie Ihre Geräte: Sorgen Sie dafür, dass Ihre digitalen Geräte, wie Smartphones, Tablets oder Laptops, physisch sicher sind. Bewahren Sie sie an einem sicheren und geschützten Ort auf, wenn sie nicht in Gebrauch sind.

Aktualisieren Sie regelmäßig die Software: Halten Sie das Betriebssystem und die Anwendungen auf Ihren Geräten auf dem neuesten Stand. Software-Updates enthalten oft wichtige Sicherheits-Patches, die vor Sicherheitslücken schützen und eine optimale Leistung gewährleisten.

Aktivieren Sie die Fernverfolgung und -sperrung: Aktivieren Sie die Funktionen zur Fernverfolgung und -sperrung auf Ihren Geräten, sofern verfügbar. Damit können Sie Ihr Gerät orten oder bei Verlust oder Diebstahl aus der Ferne sperren.

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.

Entsorgen Sie alte Geräte sicher: Achten Sie bei der Entsorgung alter digitaler Geräte darauf, dass alle persönlichen Daten vollständig von dem Gerät gelöscht werden. Führen Sie einen Werksreset durch oder verwenden Sie spezielle Software, um Ihre Daten sicher zu löschen.

Verbote:

Lassen Sie Ihre Geräte nicht unbeaufsichtigt: Vermeiden Sie es, Ihre digitalen Geräte an öffentlichen Orten wie Cafés oder öffentlichen Verkehrsmitteln unbeaufsichtigt zu lassen. Bewahren Sie sie immer in Sichtweite oder an einem sicheren Ort auf.

Installieren Sie keine nicht autorisierten Anwendungen: Vermeiden Sie das Herunterladen und Installieren von Anwendungen aus nicht vertrauenswürdigen Quellen. Halten Sie sich an offizielle App-Stores, wie den Google Play Store oder den Apple App Store, um das Risiko des Herunterladens bösartiger oder gefälschter Apps zu verringern.

5 Glossareinträge

Kennwort. Ein Kennwort ist eine geheime Zeichenkombination, die zur Authentifizierung und für den Zugriff auf ein Gerät oder ein Konto verwendet wird. Es wird empfohlen, ein sicheres Passwort festzulegen, um sensible Informationen zu schützen.
Soziale Medien. Soziale Medien beziehen sich auf Online-Plattformen und Technologien, die es Nutzern ermöglichen, Informationen, Ideen und Inhalte zu erstellen, zu teilen und mit anderen auszutauschen. Diese Plattformen beinhalten in der Regel nutzergenerierte Inhalte und erleichtern die Kommunikation, Vernetzung und Interaktion zwischen Einzelpersonen oder Gruppen.
Online-Sicherheit. Online-Sicherheit bezieht sich auf die Maßnahmen und Vorkehrungen, die zum Schutz von Personen und ihren persönlichen Daten bei der Nutzung des Internets und der Teilnahme an Online-Aktivitäten getroffen werden. Sie umfasst Praktiken und Richtlinien, die darauf abzielen, verschiedene Online-Risiken wie Cybermobbing, Identitätsdiebstahl, Betrug, Hacking und den Kontakt mit unangemessenen Inhalten zu verhindern. Die Online-Sicherheit umfasst das Verständnis und die Umsetzung von Strategien zum Schutz der Privatsphäre, der Sicherheit und des Wohlbefindens bei der Nutzung digitaler Plattformen.
Bösartige Apps. Bösartige Apps sind Anwendungen, die darauf ausgelegt sind, die Sicherheit eines Geräts oder der Daten eines Benutzers zu beeinträchtigen oder zu gefährden. Die Installation von Apps aus nicht vertrauenswürdigen Quellen erhöht

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.

das Risiko, bösartige Apps herunterzuladen, die persönliche Informationen stehlen oder nicht autorisierte Aktionen durchführen können.
Sensible Informationen. Sensible Informationen sind alle Daten oder Details, die bei Offenlegung oder Zugriff durch Unbefugte ein Risiko für die Privatsphäre, die Sicherheit oder das Wohlergehen einer Person darstellen könnten. Dazu gehören persönlich identifizierbare Informationen (PII) wie vollständige Namen, Adressen, Telefonnummern, Sozialversicherungsnummern, Finanzinformationen, Anmeldedaten und medizinische Daten. Sensible Informationen müssen besonders geschützt und behandelt werden, um Missbrauch, Identitätsdiebstahl, Betrug oder andere schädliche Folgen zu verhindern.

5 Multiple-Choice-Fragen zur Selbsteinschätzung

Frage 1. Was braucht eine Wi-Fi-Verbindung, um sicher zu sein?
Option a: Die Daten müssen privat sein, mit Passwort und Verschlüsselung.
Option b: Erfordert unbegrenzte Datennutzung.
Option c: Erfordert eine hohe Internetgeschwindigkeit.
Option d: Erfordert, dass die Wi-Fi-Verbindung öffentlich ist.
Richtige Option: a

Frage 2. Warum ist es wichtig, die Software Ihres Geräts regelmäßig zu aktualisieren?
Option a: Weil es den Speicherplatz des Geräts vergrößert.
Option b: Weil es die Geräteoberfläche schön aussehen lässt.
Option c: Weil es Sie vor bekannten Schwachstellen und Sicherheitsbedrohungen schützt.
Option d: Weil es die Lebensdauer der Batterie des Geräts verlängert.
Richtige Option: c

Frage 3. Wie können Sie potenzielle Betrugsfälle erkennen?
Option a: Durch Ignorieren von Sicherheitswarnungen.
Option b: Durch die Weitergabe von persönlichen und finanziellen Informationen überall.
Option c: Schnelles Eingehen finanzieller Verpflichtungen.
Option d: Sich über gängige Online-Betrügereien informieren und wachsam bleiben.
Richtige Option: d

Frage 4. Wie können Sie ein sicheres Passwort erstellen?
Option a: Verwendung eines einzigen Wortes in Kleinbuchstaben, ohne Zahlen oder Sonderzeichen.
Option b: Einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
Option c: Wiederverwendung desselben Passworts für mehrere Konten.
Option d: Wählen Sie ein leicht zu erratendes Passwort und teilen Sie es mit Freunden, damit Sie es nicht verlieren.

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.

Richtige Option: b

Frage 5: Was sollten Sie beim Online-Einkauf tun, wenn eine Website keine sichere Verbindung hat?
Option a: Trotzdem mit dem Kauf fortfahren.
Option b: Am besten vermeiden Sie es, persönliche Daten oder Zahlungsinformationen auf dieser Website einzugeben, und tätigen den Kauf auf einer zuverlässigeren Website mit einer sicheren Verbindung.
Option c: Ich sollte eine andere Person bitten, ihre Daten zu verwenden und den Kauf für mich auf dieser Website zu tätigen.
Option d: Wenn ich den Kauf über ein öffentliches Wi-Fi-Netz tätige, ist es kein Problem, meine Daten mit dieser Website zu teilen.
Richtige Option: b

Bibliographie und weitere Referenzen

https://www.enisa.europa.eu/
http://www.eun.org/
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
https://www.microfocus.com/en-us/what-is/cyber-security
https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html
https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/
https://www.europol.europa.eu/wannacry-ransomware

Zugehöriges Material	BOOMER_OnlineSafety_IWS_DE
Referenz-Link	
Video im Powtoon-Format	https://youtu.be/PYixkF0A34c

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.