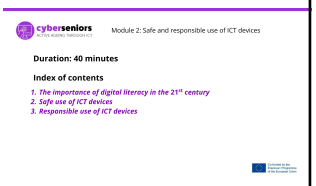
cyberseniors
ACTIVE AGEING THROUGH ICT

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

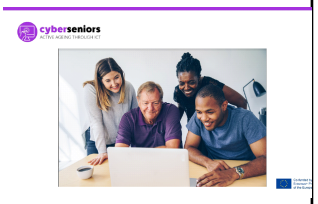
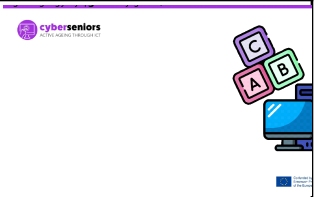
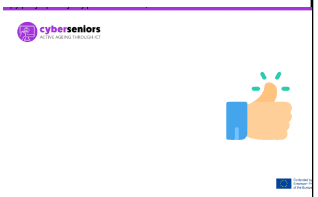
# Ausbildungsleitfaden

## Modul 2/ Sichere und verantwortungsvolle Nutzung von IKT-Geräten

| Vor der Sitzung |
|---|
| • Halten Sie alle notwendigen Materialien bereit (Computer, Präsentation, Pendrive, etc.).<br>• Bereiten Sie Ihre Präsentation gut vor<br>• eine positive und motivierende Einstellung haben<br>• Pünktlich sein |

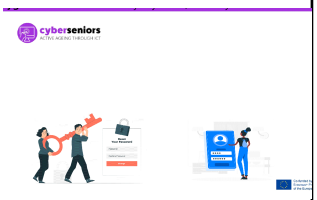
| Während der Ausbildung | | |
|---|---|---|
| Dauer | **Hauptsitzung - 40 Minuten** | Relevante Präsentationsfolie |
| 2 Min. | Während der Sitzung:<br><br>• Begrüßen Sie Ihr Publikum und stellen Sie sich vor, um eine gute Atmosphäre zu schaffen.<br>• Achten Sie stets auf die Einhaltung der Zeit, damit Sie den gesamten Stoff behandeln können.<br>• Lassen Sie am Ende etwas Zeit, um Zweifel und Fragen zu klären<br>• Handeln Sie mit Einfühlungsvermögen, Geduld und Nähe<br>• Versuchen Sie sicherzustellen, dass Ihr Publikum Ihren Erklärungen folgt |  |
| 3 Min. | Wir werden erklären, dass Cyberseniors ein von der Europäischen Kommission im Rahmen des Erasmus+-Programms kofinanziertes Projekt ist, dessen Hauptziel es ist, Schulungsressourcen für Menschen über 55 Jahre zu schaffen, die den Umgang mit einem Smartphone und nützliche Anwendungen für ein aktives Altern und eine größere Autonomie vermitteln.<br>Wir erinnern daran, dass alle Informationen sowie diese Ressourcen unter www.ciberseniors.org verfügbar sind.<br><br>Wir werden das Inhaltsverzeichnis der heutigen Sitzung erläutern und auch über den Inhalt der 4 Module (insgesamt 4 Stunden Schulung) informieren<br><br>1. Einführung in die Nutzung von Smartphone/Tablet<br>2. Sichere und verantwortungsvolle Nutzung von Informations- und Kommunikationstechnologien (IKT) |  |

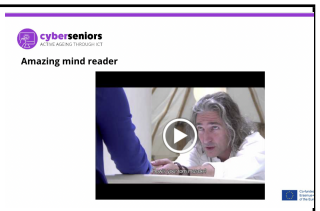
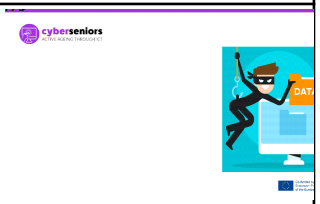
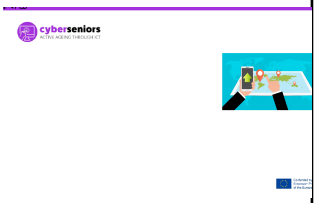
Die Unterstützung der Europäischen Kommission für die Erstellung dieses Dokuments stellt keine Billigung des Inhalts dar, der ausschließlich die Ansichten der Autoren widerspiegelt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.

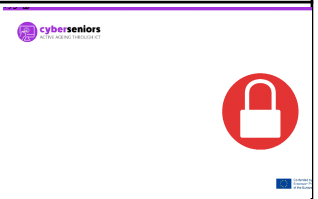
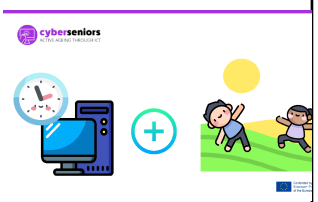
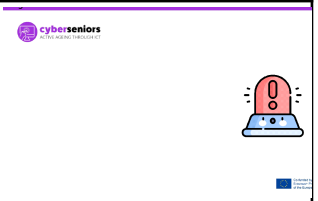
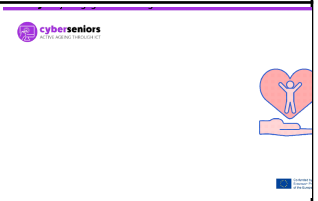
| | | |
|---|---|---|
| | 3. IKT-Anwendungen für Handys und Tablets I (Freizeit, Gesundheit, Kommunikation)<br>4. IKT-Anwendungen für Mobiltelefone und Tablets II (Bankwesen, täglicher Bedarf und Erreichbarkeit, öffentliche Verwaltung | |
| 10 Min. | Die Entwicklung der digitalen Technologie hat die Art und Weise verändert, wie wir mit anderen Menschen interagieren und wie wir unsere täglichen Aktivitäten durchführen.<br><br>Digitale Kompetenz ist eine grundlegende Fähigkeit für uns alle, um zu lernen, wie man sich in der heutigen digitalisierten Welt zurechtfindet und sich an die sich ändernden Bedürfnisse anpasst. |  |
| | - Zeitgenössischer täglicher Bedarf<br>- E-Mail<br>- Virtuelle Kommunikation<br>- Digitale Transaktionen<br>- Telefonische Mahnungen |  |
| | Digitale Kompetenz bezieht sich auf:<br>- Die erforderlichen Fähigkeiten zur Erlangung digitaler Kompetenzen;<br>- Die sichere und kritische Nutzung von Informations- und Kommunikationstechnologien (IKT) für Arbeit, Freizeit, Lernen und Kommunikation (Eurostat Glossar, 2019);<br>- Die Vertrautheit mit den Grundlagen der digitalen Sicherheit und der Nutzung von autorisierten Inhalten. |  |
| | Digitale Kompetenz hat diese Vorteile:<br><br>- Sie eröffnet eine Welt voller Möglichkeiten;<br>- Sie verbindet die Menschen;<br>- Es ermöglicht uns, Dinge aus der Ferne zu erledigen (sehr wichtig bei COVID19)<br>- Sie verbessert unsere Fähigkeiten und ermöglicht lebenslanges Lernen;<br>- Sie fördert die Unabhängigkeit und die Eigenverantwortung; |  |

Die Unterstützung der Europäischen Kommission für die Erstellung dieses Dokuments stellt keine Billigung des Inhalts dar, der ausschließlich die Ansichten der Autoren widerspiegelt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.

| | | |
|---|---|---|
| 15 Minuten | Dies sind einige der häufigsten Arten von Bedrohungen, die darauf abzielen, **sich als eine** andere Person **auszugeben**, um Daten zu stehlen oder die Daten eines Servers zu verändern. Phishing-Techniken nutzen auch Identitätsbetrug, um uns glauben zu machen, dass wir unsere Daten an eine vertrauenswürdige Website senden, während der Hacker sie in Wirklichkeit erhält, z. B. indem er sich über Facebook ausgibt, um unser Passwort zu stehlen.<br><br>**Ein Trojaner** ist eine als nützlich getarnte Software, die uns vorgaukelt, dass wir sie installieren, um Zugang zu unseren Daten zu erhalten oder unseren Computer in ein Botnetz einzubinden. Er kann als alles Mögliche getarnt sein: Office-Suiten, Antivirenprogramme, Bankensoftware usw. Aus diesem Grund ist es wichtig, dass wir jeder Software, die wir installieren, misstrauen. Wir sollten nur Software aus zuverlässigen Quellen (App-Stores) installieren und jede Software, die wir installieren, mit einem Antivirusprogramm überprüfen.<br><br>**SPAM:** Der Begriff Spam ist sehr weit gefasst und umfasst jede unerwünschte Kommunikation mit einer Person, die nicht mehr existiert und wiederholt werden kann oder nicht. In der Regel wird er per E-Mail verschickt, kann aber auch auf anderem Wege erfolgen, z. B. per Whatsapp, SMS, Telefonanruf usw. Der Zweck kann darin bestehen, an Website-Informationen zu gelangen, Daten zu stehlen, Schadsoftware zu installieren usw.<br><br>**Social Engineering** nutzt unsere menschliche Schwäche aus, anderen zu vertrauen und so die notwendigen Informationen für einen Angriff zu erhalten. Zum Beispiel... ein "Support"-Anruf, bei dem wir nach einem Service-Passwort gefragt werden, um ein Problem zu lösen. Unter Social Engineering versteht man auch das Studium der öffentlichen Informationen eines Benutzers (soziale Netzwerke, persönliche Websites usw.), um an relevante Informationen für einen Angriff zu gelangen... z. B. veröffentlichen wir den Namen unseres Haustiers auf Facebook mit allgemeiner Sichtbarkeit. Ein vermeintlicher Angreifer wird diese Informationen in die Liste der Passwörter aufnehmen, mit denen er/sie versuchen wird, in die Konten einzudringen.<br><br>**Phishing**: Phishing ist eine Technik, die zur Installation von Malware, zum Diebstahl von Daten oder Geld durch E-Mail-Nachrichten, Websites, Telefonanrufe (Vishing) oder SMS (Smishing) führt, die in Aussehen und Kontext legitim |  |

| | | |
|---|---|---|
| | erscheinen, uns aber auf eine Website führen können, auf der Daten gestohlen, die Installation von Malware erleichtert oder Geld von unseren Kreditkarten gestohlen wird.<br><br>**Adware**: ist eine Software, die uns Werbung in unseren Anwendungen oder auf den von uns besuchten Webseiten anzeigt, um durch unsere Klicks auf die Werbung Gewinne für den Ersteller der Malware zu erzielen.<br><br>**Spyware**: Es handelt sich um eine Software, die unsere Aktionen auf unserem Gerät ausspioniert. Wenn unser Gerät über Multimedia-Funktionen oder Standortsensoren verfügt, kann sie diese Informationen ausspionieren, Kameras oder Mikrofone aktivieren oder auf unseren Standort auf dem Handy zugreifen usw. | |
| | Die Hälfte der Senioren verwendet auf mindestens einem ihrer internetfähigen Geräte keine Passwortfunktion, so dass die Möglichkeit besteht, dass das Passwort von jedermann abgefangen werden kann.<br><br>Sperren Sie alle Ihre Geräte, einschließlich Computer, Tablet und Smartphone, mit sicheren Passwörtern. Das hält neugierige Blicke fern und ist ein Schutz, falls Ihre Geräte verloren gehen oder gestohlen werden.<br><br>Wie oft müssen Sie Ihre Kennwörter ändern?<br><br>Solange Sie nicht von einer Passwortverletzung erfahren, müssen Sie Ihre Passwörter nicht oft ändern, wenn jedes einzelne ein sicheres und eindeutiges Passwort ist.<br><br>Wenn Sie jedoch glauben, dass eines Ihrer Konten gehackt wurde, ändern Sie bitte umgehend Ihr Passwort. |  |
| | Bei der Erstellung von Beiträgen in sozialen Medien können Sie die Privatsphäre-Einstellungen wählen, um festzulegen, welches Publikum Ihren Beitrag sehen kann. Es können nur die Freunde sein, die Sie im sozialen Netzwerk hinzugefügt haben, es kann ein öffentlicher Beitrag für alle sein, oder es kann ein privater Beitrag nur für Sie sein. Sie können auch Ihren Standort angeben oder nicht. Achten Sie darauf, dass Ihre privaten Informationen nicht weitergegeben werden (Passwörter, Telefonnummer, E-Mail usw.)<br><br>*Wir werden das Video auf der nächsten Folie einfügen, um die Gefahr des freien Zugangs zu unseren Informationen, z. B. in sozialen Netzwerken, zu verdeutlichen. |  |

| | | |
|---|---|---|
| | Dieses Video zeigt einige der Bedrohungen, die wir bereits gesehen haben, und wie einige Cyberkriminelle vorgehen |  |
| | Bei der Kommunikation über soziale Netzwerke, Messaging und E-Mail sollten Sie darauf achten, dass Sie nicht auf Links klicken, die Ihnen von einer unbekannten Person zugesandt werden. Cyberkriminelle können sich z. B. als Facebook-Mitarbeiter oder als Sicherheitsdienst von Instagram ausgeben. Vertrauen Sie diesen Nachrichten nicht, wenn Sie sie über einen normalen Chat, einen Post oder von einer normalen Facebook-Seite erhalten. Sicherheitsmeldungen werden Ihnen über Benachrichtigungen zugesandt oder sind in den Einstellungen verfügbar. Mitarbeiter von sozialen Netzwerken werden Sie niemals nach Ihrem Passwort oder privaten Informationen fragen. |  |
| | Wenn Freunde oder Familienangehörige Sie bitten, ihnen in einem Notfall zu helfen, rufen Sie immer an, um mit ihnen persönlich zu sprechen und sich zu vergewissern, dass sie die Nachricht wirklich gesendet haben. Andernfalls könnten diese Nachrichten von Cyber-Kriminellen stammen.<br>Sie können ein Profil erstellen, das mit dem Profil Ihres Freundes oder Familienmitglieds identisch ist, und versuchen, Geld von Ihnen zu bekommen. |  |
| | Sie können das Google-Tool "Mein Telefon suchen" verwenden, wenn Sie in Ihrem Google (gmail)-Konto auf Ihrem Telefon angemeldet sind. Zunächst müssen Sie Google erlauben, Ihre Standortdaten, Geräteinformationen und Verbindungsereignisse zu verwenden, um Ihre Geräte und Ihr Zubehör zu orten.<br>Der Standort Ihres Geräts ist möglicherweise nicht immer genau, aber Sie sehen eine Karte des aktuellen Standorts Ihres Telefons. Daten zum Ladezustand und zur Verbindung mit dem Mobilfunknetz sind ebenfalls verfügbar.<br>Sie werden mehrere Möglichkeiten haben:<br>- Stellen Sie den Alarm auf Ihrem Telefon ein. Das Gerät klingelt fünf Minuten lang, auch wenn das Telefon im Stumm-Modus ist.<br>- Sperren Sie Ihr Telefon und melden Sie sich bei Ihrem Google-Konto ab. Sie können auch eine Textnachricht auf dem Telefondisplay anzeigen. |  |

| | | |
|---|---|---|
| | - Löschen Sie die Gerätedaten, indem Sie das Gerät auf die Werkseinstellungen zurücksetzen. Danach können Sie Ihr Gerät nicht mehr überwachen. | |
| | Tipps<br>- Sicherer Zugang zu Ihren Konten.<br>- Erst denken, dann handeln.<br>- Im Zweifelsfall prüfen.<br>- Sorgfältig teilen.<br>- Verwenden Sie Sicherheitssoftware.<br>- Konfigurieren Sie die Sicherheit Ihres Browsers.<br>- Verwenden Sie ein Antivirenprogramm (auch auf dem Handy).<br>- Abmelden.<br>- Bitten Sie um Hilfe. |  |
| 5 Min. | - Es ist notwendig, ein geistiges und körperliches Gleichgewicht zu halten.<br>- Verwalten Sie Ihre Interaktionen mit digitalen Tools<br>- Das digitale Wohlbefinden beeinflusst unser allgemeines Wohlbefinden und umgekehrt.<br><br>Am besten ist es, ein Gleichgewicht zwischen beiden "Welten" zu finden, um in jedem Bereich die beste Bereicherung und den größten Nutzen zu erzielen und gleichzeitig die Risiken einer übermäßigen Nutzung digitaler Werkzeuge zu verringern, die sich, wie wir gesehen haben, auf unterschiedliche Weise auswirken können.<br>Nutzen Sie die Technologie, um aktiv mit der physischen Welt und anderen Menschen in Kontakt zu treten. |  |
| | Dies sind einige Folgen des Technologiemissbrauchs |  |
| | - Verstehen und kontrollieren Sie Ihre technologischen Gewohnheiten<br>- Grenzen setzen<br>- Verwalten Sie Ihre Verbindungen besser<br>- Machen Sie regelmäßig Pausen<br>- Schlafen Sie gut und ruhen Sie sich aus, vermeiden Sie die Nutzung technischer Geräte vor dem Schlafengehen |  |
| **5 Minuten.** | **SCHLUSSFOLGERUNG** | |

| | | |
|---|---|---|
| | Wir geben ihnen bis zum Ende der Sitzung etwas Zeit, um etwaige Zweifel oder Bedenken bezüglich des heute Gesehenen auszuräumen. Wir schätzen ihre Teilnahme und ermutigen sie, zu Hause zu üben, damit sie nicht vergessen, was sie heute gelernt haben. |  |
| | | |

# ICH DANKE IHNEN VIELMALS

Die Unterstützung der Europäischen Kommission für die Erstellung dieses Dokuments stellt keine Billigung des Inhalts dar, der ausschließlich die Ansichten der Autoren widerspiegelt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.