Programm und Material zur
Medienkompetenz für Erwachsenenbildner

ANHANG 4:
TECHNISCHE MÖGLICHKEITEN

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

Project APRICOT:
Attentive parental education for wise being and cobeing
in changing times

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

Der Inhalt wurde vom Projektpartnern in dem Projekt APRICOT unter der Koordination und Verantwortung von *Šiuolaikinių didaktikų centras*/ Modern *Didactics Centre* (LT) konzipiert und entwickelt.

Vielen Dank an alle Partner für ihre wertvollen Beiträge:

Apricot Training Management Ltd. (UK)
ItF Institut Kassel e.V. – Frauencomputerschule (DE)
Planeta Ciencias (ES)

Redaktionelle Koordinatorin: Daiva Penkauskienė

Autoren: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Redaktion: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė

November 2021

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

6.1 Anhang 4: Technische Möglichkeiten

1. Antivirus Programme

Ein Virus für Ihren PC ist so ähnlich wie für Sie eine Grippe. Ein Computervirus ist ein Programm oder ein Programmcode, der Ihren Computer beschädigen soll, indem er Systemdateien beschädigt, Ressourcen verschwendet, Daten zerstört oder anderweitig gefährlich ist. Viren können sich selbst replizieren, also sich ohne Zustimmung des Benutzers in Dateien oder auf andere Computer kopieren.

Es ist wichtig den PC vor Computerviren zu schützen. Hierzu eignen sich Anti-Viren-Programme oder Viren-Scanner. Insbesondere werden Windows-Rechner wegen ihrer weiten Verbreitung am häufigsten angegriffen. Ein Programm zum Schutz des eigenen Rechners ist daher empfehlenswert, um nicht versehentlich gefährliche Dateien an andere weiterzugeben.

Antiviren-Software überprüft neue Dateien, Anhänge von E-Mails und den gesamten Computer auf Anzeichen von Virusinfektionen. Das Programm vergleicht die Daten auf Ihrem Rechner mit den Signaturen bekannter Schadprogramme. Da täglich neue Varianten von Computerschädlingen auftreten, müssen die Signaturen immer auf dem aktuellsten Stand sein. Deshalb muss die Software regelmäßig aktualisiert werden (updaten). Das geht entweder über die automatische Update-Funktion Ihres Programms. Oder die Updates werden direkt von der Herstellerseite heruntergeladen.

Statt einer Installation eines vollständigen Antiviren-Programms kann auch als Alternative ein Online-Virenscanner eingesetzt werden. Online werden immer die neuesten Updates zur Verfügung gestellt, so dass die Virensignaturen immer auf dem aktuellsten Stand sind. Allerdings sind Online-Virenscanner nicht identisch umfangreich wie ein vollständiges Antiviren-Paket und reichen nicht aus, um dieses zu ersetzen. Wenn auf dem PC allein ein Online-Scanner als Schutz eingesetzt wird, fehlt der Hintergrund-Wächter. Der Hintergrund-Wächter überprüft jede auf dem Rechner bearbeitete/ausgeführte Datei. Um einen ähnlichen Effekt bei einem Online-Virenscanner zu erzielen, müssten die neu hinzukommenden Dateien durch den Online-Scanner überprüft werden.

2. Online-Virenscanner haben noch zwei weitere Nachteile:

Sie setzen voraus, dass AciveX[1] aktiviert haben. Generell sollte ActiveX im Browser soweit möglich vermieden werden, denn es enthält keine Schutzmechanismen.

[1] Ist eine Art Programmierschnittstelle, die es Programmen erlaubt auf lokale oder aus dem Internet geladene Controls zuzugreifen. Diese Controls sind kleine ausführbare Programme bzw. Programmteile, die einzelne Funktionen ausführen.

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

Wenn der konkrete Verdacht besteht, dass der PC bereits infiziert ist, sollte die Internetnutzung weitestgehend vermieden werden. Denn über jede Online-Verbindung verbreitet sich der Schädling noch weiter aus. Und falls der PC einen sogenannten Dialer eingefangen haben sollte, könnte im schlimmsten Fall die Einwahl ins Internet über eine teure Nummer erfolgen.

WICHTIG: Virensignaturen immer auf dem neuesten Stand halten!

3. Wie können Kinder vor Gefahren im Internet geschützt werden?

Durch den richtigen Umgang mit dem Internet profitiert die ganze Familie. Erwachsene sollten immer mit gutem Beispiel vorangehen. Smartphone, Tablet und PC nicht dauerhaft in Anwesenheit der Kinder nutzen, den richtigen Umgang mit den Geräten zeigen, die Gefahren und vor allem auch die Vorteile des Internets erklären. Kinder im eigenständigen, kontrollierten Umgang unterstützen, damit sie verantwortungsbewusst damit umgehen.

Durch folgende Sicherheitsmaßnahmen behalten Sie den Überblick.

4. Kindersicherung

Kinder kommen bereits im frühen Alter durch PC, Smartphones und Tablets mit zahlreichen Internetdiensten in Berührung. Viele Apps und Webseiten sind durchaus lehrreich, helfen den Kleinen oder machen einfach Spaß zu spielen. Auf der anderen Seite bietet das Internet aber auch Gefahren wie Pornografie, Gewalt oder Glücksspiele, vor denen wir unsere Kinder schützen möchten. Daher ist die Kindersicherung von großer Bedeutung.

Sensibilisieren Sie Ihre Kinder für die Nutzung des Internets und stellen Sie auf Ihrem PC die Kindersicherung ein. Es gibt viele verschiedene Kinderschutz-Programme, die verhindern, dass Ihre Kinder unkontrolliert im Internet surfen.

Ein Beispiel dazu ist der Internet-Sitter für Kinder: **"Parents Friend".**

Das kostenlose Kinderschutz-Programm "Parents Friend“ ist ein Programm, um unerlaubte Programmstarts zu verhindern, protokolliert alle Tastenanschläge (Tastaturspion) sowie aufgesuchte Browserseiten Es läuft versteckt im Hintergrund. Das Protokoll kann automatisch als Email versandt werden (Aktivitätenprotokoll). Es können zeitliche Begrenzungen für Tage und Wochen eingestellt werden. Diese Begrenzungen beziehen sich sowohl auf die Internet- als auch die Computernutzung.

Ein Logbuch protokolliert alle Aktionen Ihres Kindes: Welche Webseiten hat Ihr Sohn besucht und welche Programme benutzt Ihre Tochter? Dazu können Sie in regelmäßigen Abständen automatische Screenshots erstellen lassen.

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

5. E-Mail-Adresse für Ihr Kind

Möchte Ihr Kind eine eigene E-Mail-Adresse haben, um mit Freunden und Verwandten zu schreiben, sollten Sie ein sicheres Konto einrichten. Hierfür gibt es spezielle Mail-Anbieter wie ***mail4kidz***, ***grundschulpost*** oder ***kidsmail24***. Sie alle erlauben es dem Kind nur mit vorher festgelegten Kontakten zu kommunizieren. So wird verhindert, dass Fremde Kontakt aufnehmen oder Werbung und Spam zugestellt wird.

Oder erstellen Sie ein Google-Konto für Ihr Kind und verwalten Sie es mit Family Link. Mit Google-Konten erhalten Kinder Zugang zu Google-Produkten wie Suche, Chrome und Google Mail, und Sie können grundlegende digitale Grundregeln aufstellen, um sie zu überwachen.

6. Kindersicherung für das Smartphone und Tablet

Besonders Smartphones und Tablets ziehen Kinder magisch an. Die Geräte verfügen über einen uneingeschränkten Internetzugriff und einen kostenpflichtigen App-Store. Eine Kindersicherung ist auch hier eine sinnvolle Lösung:

- **App-Store:**

  Im Google Play Store gibt es in den Einstellungen eine Jugendschutzeinstellung. Dort legen Sie eine Altersbeschränkung fest, die spezielle Inhalte blockiert.

- **Eingeschränktes Benutzerprofil:**

  Auf Android-Tablets ist die Einrichtung eines eingeschränkten Nutzerprofils möglich. Dort können Sie selbst bestimmen, welche Apps genutzt werden dürfen. Sie können sogar unterschiedliche Profile anlegen, wenn mehrere Kinder das Tablet nutzen. Diese Funktion ist leider nicht für alle Android-Versionen und Smartphones verfügbar.

- **Zoodles Child-Modus:**

  Diese App zur Kindersicherung bietet ebenfalls die Möglichkeit, die Benutzer-oberfläche ganz einfach kindersicher zu gestalten. Es werden unangemessene Apps und kostenpflichtige Nummern gesperrt. Die Funktion lässt sich ebenfalls mit mehreren Profilen für unterschiedliche Altersgruppen nutzen.

7. Kindersicherung bei Windows

Mit der Funktion ***Microsoft Family Safety*** können Sie Benutzerprofile unter Windows 10 anlegen, wodurch sich die Aktivitäten Ihres Kindes einschränken lassen. Sie haben die Möglichkeit Inhaltsbeschränkungen mit speziellen Filtern einzurichten, Webseiten und Kontakte zu blockieren. Außerdem erhalten Sie regelmäßig automatisierte Berichte per Mail, die Ihnen das Surfverhalten Ihres Kindes zeigen.

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

8. Filterprogramme

Filterprogramme sollen Kinder vor unerwünschten Inhalten im Internet schützen. Diese Programme arbeiten nach verschiedenen Methoden und sind unterschiedlich erfolgreich. Welches Filterprogramm von welchem Anbieter zu Ihrer Hardware und vor allem zum Alter und zur Reife Ihres Kindes passt, lässt sich pauschal nicht beantworten. Filterprogramme arbeiten oftmals mit Mechanismen wie „Whitelist“ und/oder „Blacklist“, so dass entweder nur kinder- und jugendfreundliche Seiten erreichbar sind bzw. jugendschutzrelevante Angebote ausgeblendet werden. Viele Programme können neben dem Zugriff auf das Web auch die gesamte Computernutzung beschränken – es empfiehlt sich daher oftmals, Benutzerkonten für alle Familienmitglieder anzulegen und vorab festzulegen, wie viele Stunden vor dem Rechner verbracht werden dürfen.

9. Einstellungs- und Kontrollmöglichkeiten der Browser

Eine weitere Möglichkeit, Kindersicherung einzustellen werden über die Browser gegeben. Zum Beispiel bietet Google Chrome „Family Link“ an und Internet Explorer nutzt die Funktion „Family Safety“ von Windows, um den Zugriff auf bestimmte Inhalte zu blockieren. Zur Aktivierung dieser Funktion muss der minderjährige Nutzer über ein eigenes Standardbenutzerkonto verfügen. Sie selbst müssen ein Administrator-Konto besitzen.

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