apricot for parents

Programm und Material zur Medienkompetenz für Erwachsenenbildner

ANHANG 5:
SERIÖSES SURFEN

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

Anhang 5: Seriöses Surfen

1. Merkmale einer seriösen Internetquelle[1]

1. Geben Sie den Namen der gesuchten Webseite in eine Suchmaschine ein. Anhand der Ergebnisse kann schon eine Vorentscheidung gefällt werden. Zum Beispiel, wenn sie die Suchmaschine Google verwenden. Benutzerbewertungen von vielbesuchten Seiten werden in den Suchergebnissen oben angezeigt. Sehen Sie sich Bewertungen und Feedback von Quellen an, die nichts mit der Webseite zu tun haben.
2. Beginnt eine Webseite mit „https“, dann ist diese in der Regel sicherer und daher vertrauenswürdiger als eine Seite mit „http“. Trotzdem kann eine „https“-Verbindung immer noch unzuverlässig sein. Überprüfen Sie am besten, ob die Webseite auch andere Mittel nutzt. Achten Sie darauf, dass insbesondere die Zahlungsseite der Webseite eine "https"-Seite ist.
3. „Sichere“ Webseiten zeigen ein grünes Schloss links neben der URL der Webseite an. Prüfen Sie den Sicherheitsstatus der Webseite in der Adressleiste. Durch einen Klick auf das Schloss, können Sie weitere Details zu der Webseite prüfen, z.B. die Zertifizierung und die Art der verwendeten Verschlüsselung.
4. Selbst nach der Feststellung, dass die Verbindung sicher ist, sollten Sie auf die folgenden Warnzeichen achten:
   a. Mehrere Bindestriche oder Symbole im Namen der Domain.
   b. Domainnamen, die echte Firmen imitieren (z. B. "Amaz0n" oder "NikeOutlet").
   c. Einmalige Seiten, die die Vorlagen glaubwürdiger Seiten nutzen (z. B. "visihow").
   d. Domainendungen wie ".biz" und ".info". Diese Seiten sind tendenziell nicht seriös.
   e. Denken Sie auch daran, dass ".com" und ".net"-Seiten, die am einfachsten zu beziehenden Domainendungen sind, auch wenn sie nicht unbedingt unseriös sind. Als solche tragen sie aber nicht die gleiche Glaubwürdigkeit wie eine Webseite mit der Domainendung ".edu" (für Bildungsinstitute) oder ".gov" (Regierung).
5. Achten Sie auf die Sprache auf der Webseite. Viele falsch buchstabierte (oder fehlende) Wörter, generell eine schlechte Grammatik oder seltsam formulierte Sätze sind ein Hinweis auf unseriöse Seiten. Stellen Sie diese Seiten auch in Frage, selbst wenn die fragliche Webseite von der technischen Seite her seriös zu sein scheint.

[1] Quelle: https://de.wikihow.com/Herausfinden-ob-eine-Webseite-seriös-ist am 26.05.2020

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

6. Werbeanzeigen können ebenfalls ein Hinweis auf unseriöse Seiten sein. Seien Sie achtsam, wenn Sie Werbeanzeigen der folgenden Art bemerken:
   a. Werbeanzeigen, die die gesamte Seite einnehmen.
   b. Werbeanzeigen, bei denen Sie eine Umfrage ausfüllen (oder etwas Anderes machen) müssen, bevor es weitergeht.
   c. Werbeanzeigen, bei denen Sie auf eine andere Seite weitergeleitet werden.
   d. Nicht jugendfreie oder anzügliche Werbeanzeigen.
7. Achten Sie darauf, ob eine "Kontakt"-Seite vorhanden ist. Die meisten Webseiten haben eine Kontaktseite, über die Sie den Eigentümer der Webseite erreichen können. Rufen Sie wenn möglich die bereitgestellte Nummer an oder schreiben Sie an die angegebene E-Mail-Adresse, um die Seriosität der Webseite zu überprüfen. Wenn die fragliche Webseite keine Kontaktseite hat, ist das ein sofortiges Warnzeichen.
8. Benutzen Sie eine Who-is-who Seite, um herauszufinden, wer die Domain der Webseite registriert hat. Bisher mussten bei allen Domains Kontaktinformationen der Person oder der Firma hinterlegt sein. Diese Informationen finden Sie bei den meisten Domain-Registrationsseiten oder bei https://whois.check-domain.net// (englisch: https://who.is/). Aufgrund der Datenschutz-Grundverordnung (DSGVO) werden allerdings bei Abfragen nur noch der Status der Domain ausgegeben.
9. Ein fehlendes oder unvollständiges Impressum2 ist ebenfalls ein Hinweis. Gewerbliche Anbieter sind nach § 5 Telemediengesetz verpflichtet, Namen und Anschrift sowie bei juristischen Personen zudem die Rechtsform im Impressum anzugeben.
   Als gewerblicher Anbieter gilt bereits, wer nur eine einzige bezahlte Anzeige auf seiner Website anzeigt.
10. Layout[3] und Navigation können Hinweise auf einen unseriösen Anbieter geben. Seriöse Seiten haben eher ein klares und übersichtliches Layout und über die Navigation können Sie sich schnell und weitgehend intuitiv auf der Webseite orientieren. Eine unübersichtliche Webseite könnte auch dazu führen, dass Sie auf einen kostenpflichtigen Link klicken. Achten Sie daher auf Ihr Bauchgefühl.

Rufen Sie keine Links von unbekannten oder unseriösen Quellen auf!

Führen Sie Downloads nur aus sicheren Quellen aus!

[2] Quelle: https://karrierebibel.de/unseriose-webseiten-erkennen/#Unserioese-Webseiten-erkennen am 25.04.2020

[3] https://karrierebibel.de/unseriose-webseiten-erkennen/#Unserioese-Webseiten-erkennen from 25.04.2020

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

2. Gefahren erkennen und meiden

Das Internet ist aus dem Alltag nicht mehr weg zu denken. Allerdings werden die Gefahren, die das Internet birgt, häufig verdrängt. Diese Gefahren können gerade für jüngere Kinder gravierende negative Wirkungen haben. Insbesondere stellt die Anonymität eine große Gefahr dar. Im Internet kann eine andere Identität angenommen werden. Erwachsene können sich in Chats als Kinder oder Jugendliche ausgeben und mit Kindern kommunizieren. Die Minderjährigen können dann Opfer von Bedrängung oder sogar sexueller Belästigung werden. Wenn ein Täter oder eine Täterin Minderjährige dazu überredet, unangemessene Fotos von sich zu schicken oder sich mit dem oder der Unbekannten zu treffen, kann es sehr gefährlich werden.

Eine Folge dieser Anonymität kann Cybermobbing, Sexting und Hate Speech (Hassrede) sein. Dagegen gibt es leider keine Filter oder Apps. Gerade hier ist die Medienkompetenz und kritisches Denken der Eltern und der Kinder gefragt.

3. Rechte im Internet

Es ist sehr einfach aus dem Internet Texte zu kopieren, Musik und Filme herunterzuladen oder fremde Bilder zu verwenden. Dies ist jedoch rechtlich nicht erlaubt.

Um Fotos oder Videos im Internet zu veröffentlichen, müssen Sie von allen Personen, die auf den Fotos oder Videos zu sehen sind, die Zustimmung einholen. Das gilt auch für Personen, die nur von hinten aufgenommen worden sind oder mit Filtern verfremdet wurden.

Entdecken Sie Bilder von Ihnen oder von Ihrem Kind, die unrechtmäßig im Netz veröffentlicht worden sind, sollten Sie diese als Beweismaterial aufbewahren und die Websitebetreiber dazu auffordern, die Bilder zu löschen.

Alle Bilder, Musik oder Filme sind urheberrechtlich geschützt. Sind Kopien von Kinofilmen im Netz veröffentlicht, ist auch der Download und die Verbreitung dieser Filme illegal und wird strafrechtlich verfolgt. Leider sehen viele das nicht als Diebstahl, da ja nichts Physisches gestohlen wird. Dennoch ist es ein Diebstahl von geistigem Eigentum. Laden Sie Ihre Musik/Filme von legalen Streaming Diensten, auch wenn sie meist nicht kostenlos sind. In Deutschland wird die Verletzung des Urheberrechts mit hohen Geldstrafen oder sogar mit Freiheitsstrafe bestraft.

Überprüfen Sie das Urheberrecht in Ihrem Land.

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

4. Kostenfalle: Werbung

Eine weitere Gefahr sind Werbeanzeigen. Diese Werbeanzeigen sind in Apps oder auf bestimmten Webseiten nicht sofort erkennbar. Mit einem falschen oder unüberlegten Klick können Sie auf Angeboten landen oder werden aufgefordert, eigene Daten anzugeben. Hinter dem Klick können auch Abonnements oder Käufe versteckt sein, z.B. Klingeltöne oder Hintergrundbilder. In Gratisspielen können Zusatzfunktionen oder neue Levels freigeschaltet werden. Diese Käufe werden über Ihre Mobilfunkanbieter in Rechnung gestellt, so genannte *WAP Billing*. Auch Kriminelle nutzen diese Art der Zahlung sehr häufig. Denn für viele Nutzer ist WAP Billing nicht übersichtlich genug.

5. Internetabhängigkeit

Das Internet bietet eine sehr große Anzahl an Angeboten, die rund um die Uhr genutzt werden können. Es gibt keine Unterscheidung von Tag und Nacht. Verbringt man aber zu viel Zeit in der digitalen Welt, verliert man irgendwann den Bezug zur realen Welt. Achten Sie auf die Nutzungszeiten und gehen Sie für Ihre Kinder mit gutem Beispiel voran.

6. Privatsphäre

Jeder muss selbst für die eigene Privatsphäre sorgen. Es werden zu schnell Fotos oder Telefonnummern im Internet geteilt. Denken Sie immer an den Spruch: „Das Internet vergisst nichts!“ Jeder hochgeladene Inhalt wird dort womöglich für immer irgendwo gespeichert sein. Überlegen Sie sich vor jedem Hochladen von Fotos oder persönlichen Informationen, ob Ihr Gegenüber diese Inhalte wirklich benötigt oder ob Sie das Teilen später einmal bereuen könnten. Tragen Sie weder die private Adresse noch die Kontonummer ohne Zögern und Abwägen irgendwo ein. Im schlimmsten Fall kann der Inhalt später Kosten verursachen oder negative Auswirkungen haben.

7. Cookies

Cookies sind Textinformationen, die der Browser automatisch speichert, wenn Webseiten besucht werden. Bei den Cookies handelt es sich um persönliche Informationen und Einstellungen von besuchten Webseiten. Die Cookies im Browser haben sowohl positive als auch negative Eigenschaften. Wenn eine Webseite immer wieder genutzt wird, sind Cookies von Vorteil, da ein erneutes Einloggen und die Eingabe von langen Passwörtern auf der besuchten Seite nicht benötigt wird. Der Nachteil ist, dass somit auch persönliche Daten gespeichert werden. Der Besuch auf einem Online-Shop auf dem Artikel angesehen wurden, führt dazu, dass anschließend auch passende Werbung auf anderen Webseiten angeboten werden.

Da Cookies sowohl Vorteile als auch Nachteile haben, stellt sich die Frage „Cookies akzeptieren oder blockieren?“.

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

Cookies sind zwar nicht immer von Vorteil, dennoch werden sie in vielen Bereichen gebraucht. Es gibt die sogenannten „Tracking Cookies“ und die „Session Cookies“. Die Tracking Cookies werden zum Schalten von personalisierter Werbung eingesetzt und die „Session Cookies“ werden zum Beispiel beim Online-Banking für die aktuelle Sitzung genutzt. Sobald der Anwender sich ausloggt, werden diese sofort gelöscht. Viele Online-Inhalte basieren auf der Nutzung von Cookies. Einige Seiten lassen sich ohne Cookies nur eingeschränkt oder fast gar nicht nutzen.

In den Einstellungen des Browsers können Cookies komplett blockiert werden oder nur die von besuchten Webseiten bzw. alle Cookies zugelassen werden. Cookies von Drittanbietern können ohne Bedenken blockiert werden. Das Zulassen der Cookies von besuchten Webseiten ist ein gesunder Mittelweg aus Datenschutz und Nutzung der Vorteile, die das Akzeptieren mit sich bringt.

8. Empfehlungen für Eltern

Alle diese Gefahren schrecken vor der Nutzung des Internets ab. Am liebsten möchte man den Kindern den Umgang mit dem Internet verbieten. Das ist aber nicht möglich, denn das Internet ist aus unserem Alltag nicht mehr weg zu denken. Es wäre auch wenig sinnvoll. Denn die Vernetzung bringt ja auch allerlei Erleichterungen und Vorteile mit sich. Aber können Eltern mit diesen Gefahren umgehen?

Eine Empfehlung ist dabei die Kombination aus technischen Beschränkungen (siehe Kapitel 7.2) und der elterlichen Erziehung. Aber auch die Technik hat ihre Grenzen, deshalb ist es wichtig die Medienkompetenz der Kinder zu stärken.

Um die Medienkompetenz stärken zu können, sollte man die Welt der Kinder verstehen. Nur so kann das Bewusstsein der Kinder für den Umgang mit Medien gestärkt werden. Dabei sind folgende Fragen zu klären:

- Welche Anwendungen benutzt das Kind?
- Wie geht er/sie mit diesen Anwendungen um?
- Welche Spiele spielt er/sie gern?
- Welche Serien/Filme sind für ihn/sie interessant?

Diese Fragen lassen sich am besten beantworten, wenn Eltern ihren Kindern ihr Interesse bei allen digitalen Trends zeigen. Das Kind sollte frei und ohne Angst zeigen und erklären können, was es im Internet tut. Es wäre ein Fehler, wenn Eltern ihren Kindern auf den sozialen Netzwerken folgen oder versuchen, gemeinsam das nächste Computerspiel Level zu knacken.

Das eigene Medienverhalten dient dem Kind als Vorlage. Eltern sollten nicht den ganzen Tag auf Ihr Smartphone starren und die Abende vor dem Fernseher verbringen. Wenn Mediennutzung im Leben der Eltern eine sehr große Rolle spielt, dann wird sich das Kind daran orientieren.

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

Eltern sollten nicht schimpfen, wenn das Kind in eine Kostenfalle getappt ist, sondern vorbeugend unterstützen. Sie sollten mit dem Kind über die oben genannten Gefahren im Internet sprechen und praktische Beispiele geben, die für das Kind nachvollziehbar sind. Sie sollten das Kind auffordern, Inhalte kritisch zu hinterfragen und nicht alles zu glauben, was auf Plattformen oder Webseiten zu lesen ist. Kinder lernen im realen Leben wie sie mit ihren Mitmenschen umgehen sollen. Genau diese sozialen Prinzipien gelten auch in der digitalen Welt.

Eltern sollten dem Kind die Sicherheit geben, dass er/sie sich vertrauensvoll an Mutter/Vater wenden kann und auch soll. Eltern sollten die erste Person sein, der sich das Kind anvertraut, wenn es sich auf einer Seite nicht sicher oder von anderen angegriffen fühlt. Sie sind für das Kind die wichtigsten Vertrauenspersonen.

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