apricot for parents

Programm und Material zur Medienkompetenz für Erwachsenenbildner

ANHANG 6:
SICHERHEIT UND DATENSCHUTZ

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 6: Soziale Netzwerke sicher nutzen

1. Unterschiedliche E-Mail-Adressen und sichere Passwörter

Für die Accounts der verschiedenen sozialen Netzwerke sollte man nach Möglichkeit unterschiedliche E-Mail-Adressen verwenden. Dies erschwert, dass die Informationen, die man auf den jeweiligen Seiten gibt, zu einem umfassenden Profil zusammengestellt werden können. Für die unterschiedlichen E-Mail-Adressen können Freemail-Accounts genutzt werden. Diese Accounts sollten gelegentlich abgerufen werden, damit sie aktiviert bleiben. Bei der Wahl des Anbieters sollte darauf geachtet werden, dass der Anbieter die E-Mail-Adresse nicht verfallen lässt und an einen neuen Nutzer wieder vergibt. Ansonsten besteht das Risiko, dass ein anderer Nutzer diese E-Mail-Adresse übernimmt und damit Zugriff auf das zugeordnete soziale Netzwerk erhält.

Auch das Verwenden von unterschiedlichen und sicheren Passwörtern für die einzelnen Dienste wie Facebook oder Twitter sind empfehlenswert. Für das Passwort gilt: Je länger, desto besser. Es sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Ein Passwortmanager, wie z. B. keepass.info, kann die Handhabung unterschiedlicher Passwörter erleichtern. Auf keinen Fall das Passwort an Dritte weitergeben.

2. Zwei-Faktor-Authentisierung

Mit der Zwei-Faktor-Authentisierung wird die Sicherheit noch etwas weiter verstärkt. Das bedeutet: Als erster Faktor kommt ein starkes Passwort (Kategorie Wissen) zum Einsatz. Als zweiter Faktor kommt für die zusätzliche Authentisierung z.B. ein Sicherheitstoken, also eine Hardware-Komponente wie ein Schlüssel, eine Chipkarte oder ein spezieller USB-Stick, zum Einsatz (Kategorie Besitz). Auch eine vom Anbieter versendete SMS kann genutzt werden. Damit besteht ein wesentlich besserer Schutz für das Nutzerkonto. Für einen unautorisierten Zugang müssten Dritte über beide Faktoren verfügen, also sowohl über das Wissen des Passworts als auch den Besitz des Gerätes.

3. Vorsicht bei der Installation von Apps, Add-Ons oder Plug-Ins

Viele soziale Netzwerke erlauben es, Anwendungen von Drittanbietern zu installieren, z.B. Spiele. Allerdings erstellen auch Online-Kriminelle solche Anwendungen und nutzen diese aus, um Zugriff auf das Profil zu erhalten. Vor der Installation sollten der Anbieter und Quellen auf ihre Vertrauenswürdigkeit geprüft werden.

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

4. Besondere Vorsicht bei mobiler Nutzung

Soziale Netzwerke werden oft über mobile Geräte wie Smartphones oder Tablets genutzt. Dafür stellen die Betreiber oder Drittanbieter Apps zur Verfügung. Diese Apps nutzen häufig auf dem Mobilgerät vorhandene sensible Daten, z.B. Adressbuch, Fotos, Videos oder Standortangaben. Außerdem ist das mobile Gerät in der Regel anschließend stets automatisch in dem sozialen Netzwerk angemeldet. Bei Verlust des Gerätes kann dies ausgenutzt werden, indem sich der Finder oder Dieb als der Besitzer ausgibt. Daher möglichst keine Passwörter auf mobilen Geräten speichern und anstatt über die App direkt über die Webseite des sozialen Netzwerkes an- und abmelden.

5. Kontaktanfragen

Identitätsdiebstahl gehört zu den Risiken des digitalen Zeitalters. Kontaktanfragen sollten mit Vorsicht angenommen werden. Wenn zweifelhafte Anfragen von Bekannten eingehen, auf jeden Fall die Vertrauenswürdigkeit dieser Nachrichten überprüfen. Grundsätzlich nur Personen in die Freundes- oder Kontaktliste aufnehmen, die aus der realen Welt bekannt sind. Unbekannte könnten böswillige Absichten haben. "Falsche Freunde" können mithilfe übernommener oder gefälschter Accounts eine fremde Identität annehmen und diese möglicherweise für Straftaten oder illegale Online-Geschäfte missbrauchen.

6. Jeden Klick auf Links oder Buttons vorher abwägen

Online-Kriminelle nutzen soziale Netzwerke, um Nutzer mit Postings oder Links in Chats auf präparierte Webseiten zu locken. Diese Webseiten werden dann dazu genutzt, um Zugangsdaten abzugreifen oder Geräte mit Schadsoftware infizieren zu können. Ein unbedarftes Klicken kann dazu führen, dass sich Schadsoftware auf dem Gerät installiert. Diese Schadsoftware kann beispielsweise unbemerkt die Kamera des Gerätes einschalten, Gespräche durch das Mikrofon aufzeichnen oder auch den Standort abfragen. Adressbuch, Fotos oder Videos, die auf dem Gerät gespeichert sind, können unbemerkt in fremde Hände gelangen.

7. Privatsphäre schützen

Jedes soziale Netzwerk bietet zahlreiche Einstellungen zum Schutz der Privatsphäre. Diese Einstellungen können dazu genutzt werden, um nur Freunden das eigene Profil zu zeigen und Postings zuzulassen. Die enge Verzahnung der Betreiber sozialer Netzwerke mit anderen Internetdiensten sollte bedacht werden. Dadurch kann ein sehr umfangreiches Profil über den/die Anwender:in erstellt werden. Sie sollten gelegentlich eine Online-Suche nach der eigenen Person oder Familienmitgliedern führen um herauszufinden, welche Informationen im Netz über Sie auffindbar sind. Auch die Sicherheitseinstellungen der genutzten Social Media Accounts sollten Sie in

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

regelmäßigen Abständen prüfen und dabei auch die Verknüpfung zu anderen Konten beachten. Anbieter sozialer Netzwerke könnten diese Einstellungen von sich aus ändern.

Geben Sie keine persönlichen Informationen im Netz an. Einmal im Internet veröffentlichte Informationen lassen sich nur sehr schwer oder nie wieder löschen.

8. Cyberstalker und Hasskommentare melden

- Beim Betreiber des sozialen Netzwerkes Personen, die belästigen oder beleidigen, melden. Die Betreiber können dem Missbrauch nachgehen und unseriöse Profile löschen.
- Bei offensichtlichen oder vermuteten Straftaten von der Polizei beraten lassen.
- Betroffene informieren und gegebenenfalls Anzeige erstatten.

9. Account löschen

Wenn ein Account nicht mehr genutzt wird, Daten bei Bedarf außerhalb des Netzwerkes sichern und dann den Account löschen.

Datenschutzbestimmungen und Allgemeinen Geschäftsbedingungen (AGB) lesen

10. Rechte und Pflichten

Soziale Netzwerke werden von gewinnorientierten Unternehmen betrieben, die sich zumeist durch Werbung finanzieren. Die AGB geben Aufschluss darüber, wie der Anbieter mit Ihren persönlichen Daten umgeht und wie diese an die Werbewirtschaft weitergegeben werden. Vor dem Anlegen eines Profils die AGB und Bestimmungen zum Datenschutz gründlich durchlesen.

Einige soziale Netzwerke (wie z.B. Facebook) räumen sich an Ihren Veröffentlichungen Nutzungsrechte ein. Dadurch werden zum Beispiel die Nutzungsrechte an Fotos und Videos an den Betreiber des sozialen Netzwerkes übertragen. Außerdem ist es durchaus üblich, dass gewährte Nutzungsrechte auch dann bestehen bleiben, wenn der Nutzer das Netzwerk verlassen und das Profil gelöscht hat. Also vor der Veröffentlichung gut überlegen. Es sollte auch darauf geachtet werden, dass die Rechte Dritter durch das Posten von Bildern, Texten oder Videos nicht verletzt werden.

Soziale Netzwerke haben zudem Verhaltensregeln (Netiquette), die zu beachten sind.

Unter der Netiquette versteht man Regeln, die für den Großteil der Menschen selbstverständlich sind. Nahezu jedes Forum und jede Webseite, jeder Chat-Room etc. hat seine eigene Netiquette. Die Richtlinien sind allerdings größtenteils gleich.

- Erst lesen, dann denken, dann posten
- Text kurz halten

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

- Immer daran denken, dass gegenüber auch „nur“ ein Mensch sitzt
- Gesetzliche Regelungen beachten
- Mit „Du“ oder „Sie“ schreiben?
- Höflich und tolerant sein
- Kein übermäßiger Gebrauch der Shift-Taste oder von Satzzeichen wie Ausrufezeichen
- Keine verbalen Attacken
- Rechtschreibung beachten!
- Satzzeichen verwenden!
- „Danke“ sagen schadet keinem
- Keinen Spam und keine Romane
- Kein übermäßiger Gebrauch von Smileys
- Keine Diskriminierungen, sexistische oder rassistische Sprüche
- Keine persönlichen Daten, Telefonnummern oder Werbung veröffentlichen

In Foren ist es häufig in der Netiquette geregelt, dass zunächst die Suchfunktion verwendet wird, bevor man eine Frage stellt. So wird in den meisten Fällen verhindert, dass eine bereits gestellte Frage immer wieder neu verfasst wird.

Je nach Portal, Blog etc. kann die Liste der Regeln variieren. In der Regel wird die Netiquette auch bei Facebook, in E-Mails und an anderen Positionen verwendet, an denen man eigene Texte und Kommentare im Netz verfassen kann.

11. Persönliche Angriffe und Cyberbullying

Soziale Medien, Messenger-Dienste und andere Apps ermöglichen, bzw. erleichtern Cyberbullying und Cyberstalking. Sie bieten oft nicht nur die Plattformen an, auf denen das Mobbing bzw. Stalking stattfindet, sondern machen auch private Informationen der Nutzenden öffentlich zugänglich.

12. Cyber-Mobbing

Cyber-Mobbing ist das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum. Der Täter („Bully“) sucht sich ein Opfer, das sich nicht oder nur schwer gegen die Übergriffe zur Wehr setzen kann. Der Täter nutzt dieses Machtungleichgewicht und führt somit sein Opfer in die soziale Isolation.

Cyber-Mobbing findet in sozialen Netzwerken, in Video-Portalen und über Smartphones durch Instant-Messaging-Anwendungen wie WhatsApp, lästige Anrufe etc. statt. Der Bully handelt in der Regel anonym und das Opfer weiß nicht, von wem genau die Angriffe stammen. Umgekehrt verhält es sich bei Kindern und Jugendlichen, die sich meist aus dem „realen“ persönlichen Umfeld kennen. Die Opfer haben deshalb fast immer einen Verdacht, wer hinter den Attacken stecken könnte.

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

13. Unterschiede von Cyber-Mobbing und klassischem Mobbing

Cyber-Mobbing unterscheidet sich in einigen Punkten vom Mobbing in der realen Welt.

- Cyber-Mobbing endet nicht nach der Schule oder der Arbeit. Denn Cyber-Mobbing kann über das Internet 24 Stunden am Tag stattfinden. Sie können dich sogar zu Hause belästigen.
- Das Ausmaß von Cyber-Mobbing ist größer als das des Mobbing in der realen Welt, weil
  - das Publikum unüberschaubar groß ist
  - Inhalte sich extrem schnell verbreiten
  - Inhalte, die man längst vergessen hat, können immer wieder an die Öffentlichkeit gelangen
  - Bullies können anonym agieren:

Der Täter zeigt sich seinem Opfer nicht direkt. Nicht zu wissen, wer die Täter sind, kann einem Opfer Angst machen und es verunsichern. Der Täter sieht die Reaktionen des Opfers auf eine verletzende Äußerung oder ein respektloses Bild nicht und ist sich daher möglicherweise nicht über das Ausmaß der Auswirkungen seiner Angriffe im Klaren.

14. Facetten des Mobbings

Mobbing hat verschiedene Facetten:

- **Schikane**:
  Wiederholtes Senden von beleidigenden und verletzenden Nachrichten über E-Mail, SMS, Instant-Messenger oder in Chats.
- **Verleumdung / Gerüchte**:
  Verbreiten von Gerüchten über Internet- und Mobiltelefondienste an einen großen Personenkreis.
- **Bloßstellen**:
  Informationen, die ursprünglich im Vertrauen einer bestimmten Person zugänglich gemacht wurden, werden an weitere Personen gesandt, um das Opfer zu kompromittieren.
- **Ausschluss/Ignorieren**:
  Bewusster Ausschluss von sozialen Aktivitäten, Gruppen, Chats etc.

15. Einfluss von Cyber-Mobbing auf die Web-Kultur

Das Internet führt dazu, dass sich die Kommunikation mit anderen Menschen massiv verändert. Es ist einerseits eine positive Entwicklung, dass man jederzeit problemlos erreichbar ist oder mal schnell nachsehen kann, was die Freundin / der Freund geschrieben hat. Oder welches Foto gerade gepostet wurde. Andererseits lassen sich aber auch negative Tendenzen feststellen, die diese neue „Online-Kommunikations-Kultur“ mit sich bringt.

16. Schnelllebigkeit

Die Übertragungsgeschwindigkeit des Internets ist schneller geworden und auch das mobile Internet wird stetig in seiner Leistungsfähigkeit verbessert. Die Informationen erreichen auch unterwegs in immer kürzeren Zeitabständen die Nutzer:innen. Allerdings haben sich auch die Nutzer:innen daran angepasst. Die Kommunikation wird schneller und rastloser. Ein Tag offline bedeutet: am folgenden Tag sind etliche Nachrichten von Freunden, Bekannten oder Kollegen auf dem Computer oder Smartphone.

Diese Geschwindigkeit führt allerdings auch dazu, dass Posts, Bilder oder Videos spontan geteilt und versendet werden. Nicht nur positive, sondern auch für eine Person unvorteilhafte Momentaufnahmen oder herabwürdigende Kommentare. Diese Informationen verbreiten sich sehr schnell über verschiedene Dienste an einen unüberschaubar großen Personenkreis.

17. Anonymität & Distanz

Die Anonymität begünstigt eine enthemmte Online-Kommunikation. Wer anonym im Netz unterwegs ist, muss kaum mit negativen Konsequenzen für sein Tun rechnen. Außerdem kann über die Online-Kommunikation die direkte Reaktion des Gegenübers nicht gesehen werden, Videochat ausgenommen. Der/die Nutzer:in kann deshalb oft nicht einschätzen, wie seine Äußerungen bei anderen Nutzer:innen ankommen, weil er/sie nicht sieht, wie der/die Andere in Mimik und Gestik reagiert. Da man dem Anderen nicht von Angesicht zu Angesicht begegnet, ist es leicht, andere online zu verletzen.

18. Übermäßiges Mitteilen persönlicher Informationen

Soziale Netzwerke und viele Dienste, wie WhatsApp, Twitter, Ask.fm etc. leben davon, dass die Nutzer:innen vieles mit anderen teilen. Kinder und Jugendliche lassen sich leicht dazu verleiten, vieles über sich preiszugeben, denn sie wollen austesten, wie man bei Gleichaltrigen ankommen. Allerdings ist das Feedback von Anderen auf gepostete Fotos, Videos und andere Beiträge nicht immer positiv und der/die Nutzer:in gerät durch seine Selbstdarstellung bei anderen in Verruf und wird schikaniert.

19. Freunde versus Bekannte

Über soziale Netzwerke und Instant Messenger ist es sehr einfach, schnell und unkompliziert neue Bekanntschaften zu machen. Diese werden dann umgehend auf Facebook, WhatsApp und Co. hinzugefügt. Damit sammeln sich im Laufe der Zeit immer mehr Kontakte an, die aus verschiedensten Kontexten stammen. Es wird immer schwieriger den Überblick zu wahren. Es ist aber wichtig zu wissen, wer die Posts lesen, die Fotos sehen kann, denn nicht alles ist für alle Kontakte geeignet.

Viele soziale Netzwerke bieten den Nutzern die Option an, ihre Kontakte in verschiedene Gruppen zu sortieren. Die Beiträge, die der/die Nutzer:in hochlädt, können gezielt für die

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

einzelnen Gruppen (Freunde, Bekannte etc.) freigegeben werden. Auf diese Weise können unliebsame Reaktionen von Unbekannten oder losen Bekannten auf persönliche Beiträge vermieden werden.

20. Tipps für Eltern

Wie können Eltern erkennen, dass ihr Kind gemobbt wird?

Cyberbullying lässt sich bereits im Anfangsstadium erkennen und auch bekämpfen. Sollte man bemerken, dass das Kind sein Verhalten schlagartig verändert, muss Hilfe her. Anzeichen hierfür sind, wenn das Kind z.B.

- sich zurückhaltend verhält,
- die Lust an der Kommunikation verliert,
- die Onlinenutzung drastisch verändert,
- sich von der Außenwelt isoliert,
- aggressiv reagiert,
- viele Ausreden oder unerklärliche körperliche Beschwerden hat,
- sein/ihr Aussehen nach Vorbildern und Schönheitsidealen orientiert
- oder die eigene Situation herunterspielt.

Treten diese Symptome auf, sollten die Eltern sich sofort mit Ihrem Kind unterhalten, denn die Anfänge von Cyberbullying müssen sofort im Keim erstickt werden, um Schäden zu verhindern. Sollte das Kind bereits massiv gemobbt werden, ist es immer ratsam, einen Experten zu befragen. Online-Hilfen finden Sie bei Bündnis gegen Cybermobbing e.V. - Mobbing Internet/Netz (https://www.buendnis-gegen-cybermobbing.de) und Klicksafe (https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing).

(https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing).

21. Wie können Eltern ihren Kindern helfen?

Es ist wichtig, auf Mobbingopfer aktiv zuzugehen, über deren Probleme zu reden und eine erste emotionale Stütze zu bieten. Eltern sollten jedoch auch den Rat und die Meinung eines Experten/ einer Expertin hinzuzuziehen. Zum Beispiel die kostenlose Telefon-Seelsorge-Hotline. Diese Hotline ist 24 Stunden anonym erreichbar und hat entsprechend geschulte Ansprechpartner:innen. Es ist auch wichtig, sich den Problemen des Kindes zu stellen und offen zu agieren. Man sollte sich der Familie und den Freunden öffnen und gemeinsam besprechen, welche weiteren Schritte eingeleitet werden sollten.

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

22. Wie kann man sich vor Cyberbullying schützen?

Es gibt keine Garantie, dass man kein Opfer von Cyberbullying wird. Durch einfache, aber wirkungsvolle Methoden ist es möglich, die Gefahr zu senken. Wie immer gilt auch hier:

- nie zu viel von Ihrem Privatleben im Internet preisgeben,
- Privatsphäreneinstellungen und “Freunde” genau kontrollieren,
- Überlegen, mit wem oder was man im Internet macht,
- niemals im Internet öffentlich über Sorgen und Probleme sprechen,

Auch hier gilt: „Wissen ist Macht!“

Eltern sollten Ihre Kinder für den Umgang mit Cyberbullying sensibilisieren, in dem sie offen mit Ihrem Kind über Mobbing sprechen und die verschiedenen Varianten durchgehen. Ein sehr wichtiger Punkt ist, dass Eltern Ihrem Kind die Sicherheit geben, dass es sich jederzeit an sie wenden kann.

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