MEDIENKOMPETENZ IM DIGITALEN ZEITALTER: UNTERSTÜTZUNG VON LEHRKRÄFTEN

MeLDE

Erasmus+ Emphasys CENTRE UNIVERSITY OF WOLVERHAMPTON ANT BÜRGERHAUS ENNOHAUS DEMOKRITOS

MODUL 4 - E-SICHERHEIT

BESCHREIBUNG

Ziel dieses Moduls ist es, Lehrer*innen mit einer Reihe von Szenarien und Möglichkeiten vertraut zu machen, wie sie online sicher bleiben können. Es werden Themen wie Risiken und Verantwortlichkeiten online, Schutz persönlicher Daten, Online-Fehlinformationen und schädliche Inhalte, digitales Urheber*innenrecht und wirksame sowie unwirksame Praktiken gegen Cybermobbing erörtert.

MODUL 4 - E-SICHERHEIT

LISTE DER THEMEN

THEMA 1 RISIKEN UND VERANTWORTLICHKEITEN ONLINE

THEMA 2 SCHUTZ PERSÖNLICHER DATEN

THEMA 3 DIGITALES URHEBER*INNENRECHT

THEMA 4 ONLINE-FEHLINFORMATIONEN UND SCHÄDLICHE INHALTE

THEMA 5 CYBERMOBBING

MODUL 4 - E-SICHERHEIT

LEHRPLAN

THEMA 1 Risiken Online

- Es wird eine Vielzahl potenzieller Bedrohungen für Hard- und Software, einschließlich Computerviren, Adware und Spyware und wie man sie überwinden kann, besprochen.
- Es werden Bedrohungen für Daten/Informationen besprochen.
- Es werden verschiedene Möglichkeiten Internet-Betrug zu melden behandelt.
- Es werden die eigenen Online-Rechte und -Verantwortlichkeiten besprochen und diskutiert.

THEMA 2 Schutz personenbezogener Daten

- Es wird besprochen, wie man sichere Passwörter erstellt und diese sicher und fern von Betrüger*innen aufbewahrt.

- Es wird besprochen, wie wichtig es ist, immer über eine aktualisierte Anti-Malware-Software und ein aktualisiertes Betriebssystem zu verfügen.

- Es wird besprochen, dass auch mobile Geräte gehackt werden können und wie man Smartphones sicher halten kann.

- Es wird besprochen, wie man böswillige E-Mails erkennen kann und, was zu tun ist, wenn man feststellt, dass man auf einen Link geklickt und ein Passwort weitergegeben hat.

- Es werden Möglichkeiten zum Schutz persönlicher Daten auf Social-Networking-Sites besprochen.

THEMA 3 Digitale Urheber*innenrechte

- Es werden neue rechtliche und politische Entwicklungen im Urheber*innenrecht und wie es sich an die digitale Welt angepasst hat, besprochen.
- Es wird besprochen, wie digitaler Content, der von Lehrer*innen oder Schüler*innen erstellt und veröffentlicht wird, geschützt werden kann.
- Es wird besprochen, was Plagiate sind und wie sie im digitalen Zeitalter vermieden werden können, wenn die Inhalte von unzähligen Quellen auf vielfältige Weise genutzt und wiederverwendet werden können.
- Es wird eine Reihe von Open-Access-Quellen diskutiert und besprochen, wann digitaler Content für Bildungszwecke verwendet und wiederverwendet werden kann.
- Es sollte in Gruppen gearbeitet werden, um ein digitales, leicht lesbares Kurzhandbuch für Schulen zu erstellen.

MODUL 4 - E-SICHERHEIT

LEHRPLAN

THEMA 4 Online-Desinformation und gefährlicher Content

- Es wird der Unterschied zwischen echten und gefälschten Webseiten besprochen.

- Es wird besprochen, wie man gefälschte Webseiten erkennt wie man diese melden kann.

- Es wird diskutiert, was "Fake News" sind und wie man sie bewertet, identifiziert und meldet.

- Es wird diskutiert, warum es wichtig ist, gefälschte Webseiten zu melden und was für schädliche Auswirkungen sie auf die Demokratie, die Gesellschaft und die Einzelperson haben können.

THEMA 5 Cybermobbing

- Es wird besprochen, was Cybermobbing ist und warum es wichtig ist, dagegen vorzugehen.

- Es wird zwischen verschiedenen Formen des Cybermobbings differenziert.

- Es wird besprochen, wie man Schüler*innen identifizieren kann, die Opfer von Cybermobbing auf unterschiedliche Weise geworden sind.

- Es wird eine Reihe von Maßnahmen behandelt, die Schülern*innen helfen können, die Opfer von Cybermobbing geworden sind.

- Es wird die Bedeutung einer Interventions- und Präventionsstrategie gegen Cybermobbing diskutiert und mit einer Ausarbeitung dessen für Schulen begonnen.

THEMA 2 Schutz personenbezogener Daten

KURZE BESCHREIBUNG DER UNTERTHEMEN

Dieser Unterthema soll Lehrer*innen mit den gebräuchlichsten Sicherheitsmaßnahmen vertraut machen, wie z. B. sichere Passwörter, Anti-Malware-Software, Datensicherung, Verschlüsselung, Firewall und sicheres Einkaufen. Es wird auch besprochen, wie man in sozialen Medien sicher bleibt, wie man seine mobilen Geräte sicher hält, wie man schädliche oder anstößige Inhalte in sozialen Medien vermeidet und wie man Fake News erkennt.

Folgende Themen werden besprochen:

- Erstellen sicherer Passwörter
- Aktualisierung der Anti-Malware-Software und des Betriebssystems
- Schwachstellen von mobilen Geräten und Wege sie sicher zu halten
- Bösartige E-Mails
- Möglichkeiten persönliche Daten in sozialen Netzwerken zu schützen

THEMA 2 Schutz personenbezogener Daten

ERSTELLEN SICHERER PASSWÖRTER

Die Erstellung sicherer Passwörter für Online-Konten ist eine der wirksamsten Möglichkeiten, persönliche Daten, Informationen und sich selbst vor Cyber-Angriffen zu schützen.

Um sichere Passwörter zu erstellen, sollte man Folgendes beachten:

- Passphrasen anstelle von Passwörtern verwenden
- Passwörter verwenden, die Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten
- Passwörter verwenden, die mehr als acht Zeichen lang sind
- leicht zu erratende Wörter oder alphanumerische Kombinationen (z. B. Namen von Kindern oder Haustieren, Geburtsdaten, Adressen, Sozialversicherungsnummern) vermeiden
- Wörter verwenden, die nicht aus einem Wörterbuch stammen.

THEMA 2 Schutz personenbezogener Daten

MeLDE

ERSTELLEN SICHERER PASSWÖRTER

Um Passwörter sicher aufzubewahren, sollte man Folgendes tun:
- Keine Passwörter auf dem Laptop oder Handy aufbewahren.

- Keine Passwörter im Browser speichern

- Keine Passwörter aufschreiben

- Falls eine andere Person einmaligen Zugang zu einem Account benötigt, sollte bei abgeschlossener Aufgabe das Passwort geändert werden

- Einen Passwortmanager verwenden, der einzelne Anmeldedaten mit anderen Personen teilen kann, ohne dass diese die Anmeldedaten tatsächlich einsehen können

- Nicht dasselbe Passwort für mehr als ein Konto verwenden

- Passwörter in logischen Gruppierungen sortieren

- Keine Kennwörter oder Kontoanmeldedaten über öffentliche oder ungesicherte Wi-Fi-Netzwerke senden

- Passwort ändern, sobald eine Sicherheitsverletzung gefunden und der Eindringling blockiert wird

AKTUALISIERUNG DER ANTI-MALWARE-SOFTWARE UND DER BETRIEBSSYSTEME

AKTUALISIERUNG DER ANTI-MALWARE-SOFTWARE

Da die Cyber-Kriminalität zunimmt, ist es wichtig, die neuesten Updates herunterzuladen und zu installieren. Angesichts der Tatsache, dass die meisten Anti-Malware-Unternehmen sehr schnell Schutz für neue Bedrohungen hinzufügen und ihren Kund*innen diesen aktualisierten Schutz zur Verfügung stellen, sowie der Tatsache, dass sich die meisten Bedrohungen relativ langsam verbreiten, bedeutet dies, dass die meisten Unternehmen und Einzelpersonen Zeit haben, sich vor diesen neuen Bedrohungen zu schützen, wenn man die Anti-Malware-Software auf dem neuesten Stand hält.

Virenschreiber*innen und Entwickler*innen von bösartigen Codes finden ständig Wege, um die neuen Technologiefunktionen zu umgehen. Keine Antiviren- und Anti-Malware-Software installiert zu haben, ist fast genauso schlimm, wie schon lange Zeit eine Sicherheitssoftware zu verwenden und diese seither nicht oft aktualisiert zu haben. Solange Sicherheitssoftware nicht erneuert wird, sind Cyberkriminelle in der Lage, Fehler und Probleme zu finden, die sie ausnutzen können.

Wenn der eigene Computer oder Laptop mit einem Virus oder einer Malware infiziert ist, kann sich dieser nicht nur auf die Daten oder Festplatte auswirken, sondern sich über Netzwerkverbindungen oder E-Mails auch auf andere Geräte ausbreiten. Cyberkriminelle können persönliche Daten wie E-Mail-Adressen und Online-Konten nutzen, um im eigenen Namen Cyberverbrechen zu begehen. In einem solchen Fall wird man selbst möglicherweise zur Zahlung eines Lösegeldes aufgefordert, um sie zurückzubekommen. In schlimmeren Fällen kann es sogar passieren, dass man das Lösegeld zahlt und die Daten trotzdem nicht zurückbekommt.

THEMA 2 Schutz personenbezogener Daten

AKTUALISIERUNG DER ANTI-MALWARE-SOFTWARE UND DER BETRIEBSSYSTEME

AKTUALISIERUNG DES BETRIEBSSYSTEMS

Hacker*innen können eine Softwareschwachstelle, d. h. eine Sicherheitslücke/Schwäche, die in einem Softwareprogramm/ Betriebssystem gefunden wurde, ausnutzen, indem sie Codes schreiben, der auf die Schwachstelle abzielt, und die gestohlenen persönlichen Daten dazu verwenden, in dem geklauten Namen Verbrechen zu begehen oder die Daten im Darkweb zu verkaufen, um anderen zu ermöglichen, Verbrechen zu begehen.

Der Benutzer*innen eines aktualisierten Betriebssystems profitieren von den reparierten Sicherheitslücken, von den Software-Patches und von der Behebung oder Entfernung von Sicherheitsfehlern. Die Aktualisierung des Betriebssystems kann auch neue Funktionen zu den Geräten hinzufügen und veraltete entfernen.
Ein weiterer wichtiger Grund das Betriebssystem zu aktualisieren, besteht darin, nicht durch die Verwendung veralteter Programme und Anwendungen, die für Ihren Erfolg in der Schule, zu Hause, auf der Arbeit usw. entscheidend sind, in Sachen Technologie zurückzubleiben.

Außerdem werden nicht alle Betriebssysteme und jede komplexe Software fehlerfrei veröffentlicht. Aus diesem Grund sind Aktualisierungen oft wichtig, um die Fehler zu beheben, die nach der Veröffentlichung eines Betriebssystems/Programms/Anwendung entdeckt werden.

THEMA 2 Schutz personenbezogener Daten

SCHWACHSTELLEN VON MOBILEN GERÄTEN UND WEGE SIE SICHER ZU HALTEN

Hacker*innen zielen heutzutage auf Smartphones und mobile Geräte im Allgemeinen ab, um Zugang zu persönlichen Informationen aus Nachrichten, Facebook und anderen Social Media Apps, Bank- und Einkaufsdaten, E-Mails usw. zu erhalten.

Um einen solchen Angriff zu vermeiden oder zu umgehen, können Nutzer*innen von Smartphones und Mobilgeräten die folgenden Schritte befolgen:

Das Handy sperren - Alle Smartphones verfügen über eine Passwortschutzfunktion, diese sollte man benutzen und das Passwort alle drei bis sechs Monate ändern. Eine einfachere Alternative zu Passwörtern sind die Sperr-„Muster", Gesichts-, Stimm- oder Fingererkennung.

Tracking einschalten - Wenn das Smartphone gestohlen wird, kann man den Standort mit dieser Funktion ermitteln. Darüber hinaus kann man Handy mit einer Tracker-Anwendung aus der Ferne sperren.

Das Betriebssystem aktualisieren - Immer die neuesten Updates für das Smartphone herunterladen, um eventuelle Lücken im System zu schließen, die Hacker*innen entdecken könnten.

Vorsicht vor Apps - Immer darauf achten, dass eine App aus dem App Store (für iOS) oder von Google Play (für Android) heruntergeladen wird, da diese die Authentizität der angebotenen Apps überprüfen.

THEMA 2 Schutz personenbezogener Daten

SCHWACHSTELLEN VON MOBILEN GERÄTEN UND WEGE SIE SICHER ZU HALTEN

Vorsicht vor seltsamen Nachrichten - Keine Nachrichten von Fremden, einer unbekannten Nummer oder einer Nummer, die seltsam erscheint öffnen. Stattdessen sollten diese Nachrichten gelöscht werden; nicht auf Links in der Nachricht klicken oder Apps herunterladen.

Vorsicht vor kostenlosem WiFi – Vorsicht vor ungesicherten drahtlosen Netzwerken.
Wenn man nicht den Internetservice des eigenen Netzbetreibers, sondern eine WiFi-Verbindung nutzt, läuft man Gefahr, die Daten Hacker*innen auszusetzen. Man sollte also sicherstellen, dass die öffentliche Verbindung einem Unternehmen gehört, denn ein kostenloser WiFi-Hotspot könnte die Idee von Hacker*innen sein, persönliche, private Daten in überfüllten Bereichen zu stehlen.

Antivirenschutz verwenden - Das Smartphone verfügt über ein Betriebssystem, Programme (Apps), einen Internet-Browser und gilt somit als ein Computer, der vor Hacker*innen geschützt werden muss.

THEMA 2 Schutz personenbezogener Daten

MeLDE

BÖSARTIGE E-MAILS ERKENNEN

1. Der Absender ist falsch

- Prüfe, ob die Adresse mit dem Namen des Absenders übereinstimmt.
- Prüfe, ob die Geschäftsadresse des Absenders korrekt ist.
- Um das Obige überprüfen zu können, muss das E-Mail-Programm die E-Mail-Adresse des Absenders und nicht nur dessen Namen anzeigen.

2. Der Absender ist sich der eigenen Identität nicht bewusst.

- Prüfe, ob der Absender einen so anspricht, wie man es erwarten würden.
- Überprüfe, ob die Signatur des Absenders mit der Art und Weise übereinstimmt, wie die Person normalerweise ihre E-Mails signieren würde.
- Zum Beispiel würde eine Bank in einer E-Mail normalerweise den vollen Namen nennen, nicht nur in einer allgemeinen Art und Weise ("Sehr geehrter Kunde").

3. Eingebettete Links haben verdächtige URLs

- Fahre mit der Maus über die Links in einer E-Mail vor dem Öffnen. Überprüfe, ob die URL des Ziels mit der Webseite übereinstimmt, auf die die E-Mail verweist.

4. Die Rechtschreibung und Grammatik der Sprache sind ungewöhnlich.

- Überprüfe, ob die E-Mail voller Rechtschreib- und Grammatikfehler ist, als ob jemand einen Online-Übersetzungsprogramm verwendet hat.

5. Der Inhalt ist nicht glaubwürdig oder bizarr

- Wenn die E-Mail einen großen Gewinn für eine kleine Investition oder kostenlos verspricht, handelt es sich in der Regel um eine Phishing-E-Mail.

THEMA 2 Schutz personenbezogener Daten

MeLDE

WAS MAN MACHEN KANN WENN MAN AUF EINEN BÖSARTIGEN LINK GEKLICKT HAT

1. Keine persönlichen Daten eingeben, wenn dies verlangt wird.

2. Keine Zugangsdaten eingeben. Die Cyberkriminellen werden sie benutzen, um sich in das reale Konto einzuloggen.

3. Die Verbindung zum Internet so schnell wie möglich trennen, um eine eventuelle Malware-Infektion einzudämmen. Das Netzwerkkabel ausstecken, um die Netzwerkverbindung auf dem Gerät auszuschalten.

4. Das Gerät mit einer Antivirus- und/oder Antimalwaresoftware scannen. Während des Scans vom Internet getrennt bleiben.

5. Passwörter auf der Webseite ändern oder überall dort, wo die E-Mail mit demselben Passwort verwendet wird.

6. Dateien auf einem anderen Gerät sichern.

THEMA 2 Schutz personenbezogener Daten

MÖGLICHKEITEN PERSÖNLICHE DATEN IN SOZIALEN NETZWERKEN ZU SCHÜTZEN

1. Vermeide es, die Felder „über mich“ auszufüllen. Die meisten sozialen Netzwerke, wie z. B. Facebook, behalten ihre „Über mich"-Abschnitte optional. Erwäge, nur allgemeine Informationen anzugeben oder das Feld einfach leerzulassen.

2. Sich mit den Datenschutzeinstellungen vertraut machen und verschiedene Optionen ausprobieren, um herauszufinden, was den eigenen Präferenzen entspricht. Versuche, die Anzeige von Beiträgen auf bestimmte vertrauensvolle Personen zu beschränken. Denke daran, dass selbst wenn die Einstellungen auf „privat" gestellt sind, einige Fotos in der Google Bildersuche dennoch öffentlich angezeigt werden können. Wenn man also nicht möchte, dass die eigenen Bilder öffentlich gefunden werden, sollte man sie gar nicht erst veröffentlichen.

3. Sich selbst vergewissern, dass man Freunde hat, die einen kennen und denen man vertraut. Mit je mehr Personen man in sozialen Medien befreundet ist, desto schwieriger wird es, diese von den veröffentlichten Informationen zu kontrollieren. Zögere nicht, die „Block"-Funktion zu nutzen, wenn befürchtet wird, dass eine Person die eigenen Informationen ausnutzen könnte.

4. Vermeide es, die "location tagging"-Funktion zu verwenden. Einige Kriminelle könnten es ausnutzen und sogar schaden, wenn sie den eigenen Standort genau kennen. Manche Kriminelle könnten sogar in das Haus einbrechen, wenn sie wissen, dass man selbst nicht zuhause ist.

MÖGLICHKEITEN PERSÖNLICHE DATEN IN SOZIALEN NETZWERKEN ZU SCHÜTZEN

5. Nach Benutzung von einer Social Media-Webseite abmelden. Falls ein öffentliches oder auch ein privates Gerät zum Anmelden benutzt wurde, hilft die Abmeldung von einer Social-Media-Site sicherzustellen, dass das eigene Konto nicht von einer anderen Person gehackt wird, die Zugang zu dem Gerät hat, mit dem man angemeldet war, und z. B. Freund*innen verbal angreift, peinliche Inhalte im eigenen Namen veröffentlicht oder schlimmer noch, persönliche Daten, Passwörter ändert oder einen selbst sogar vom eigenen Konto aussperrt.

6. Sichere, private Passwörter erstellen. Starke Passwörter bestehen aus einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, die leicht zu merken, aber für andere Personen schwer zu erraten oder zu knacken sind. Vermeide die Verwendung einfacher und gebräuchlicher Passwörter wie Geburtsdaten, Jahrestage und Namen von Haustieren. Halte Passwörter geheim und schreibe sie nicht auf ein Papier in der Nähe des Geräts.

THEMA 2 Schutz personenbezogener Daten

MeLDE

QUELLEN UND REFERENZEN

- Protection of personal data. Retrieved from

  https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

- De Groot, J. (2019, December). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020. Retrieved from

  https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

- How to create a good password. Retrieved from

  https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/how-to-create-a-good-password/

- McDonald, J. (2006, October). The Importance of Updating Antivirus Definitions. Retrieved from

  https://www.symantec.com/connect/blogs/importance-updating-antivirus-definitions

- Graham-Smith, D. (2017, March). 12 ways to hack-proof your smartphone. Retrieved from

  https://www.theguardian.com/technology/2017/mar/26/12-ways-to-hack-proof-your-smartphone-privacy-data-thieveshttps://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-to-tell-if-your-smartphone-has-been-hacked/

MODUL 4 - E-SICHERHEIT

GLOSSAR

Begriff	Definition
PASSWORT	Ein geheimes Wort oder Ausdruck, der verwendet wird, um Zugang zu einem Gerät oder Webseiten usw. zu erhalten.
ANTI-MALWARE	Anti-Malware ist eine Art von Software-Programm, das entwickelt wurde, um bösartige Software (Malware) auf IT-Systemen sowie auf einzelnen Computergeräten zu verhindern, zu erkennen und zu entfernen.
ANTIVIRUS	Antiviren-Software ist eine Art von Programm, das entworfen und entwickelt wurde, um Computer vor Malware wie Viren, Computerwürmern, Spyware, Botnets, Rootkits, Keyloggern usw. zu schützen.
BÖSARTIGE URL	Eine bösartige URL ist ein Link, der mit dem Ziel erstellt wurde, Betrügereien, Angriffe und Betrug zu begünstigen.