MEDIENKOMPETENZ IM DIGITALEN ZEITALTER: UNTERSTÜTZUNG VON LEHRKRÄFTEN

MeLDE

Erasmus+ Emphasys CENTRE UNIVERSITY OF WOLVERHAMPTON ANTI 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 5 Cybermobbing

KURZE BESCHREIBUNG DER UNTERTHEMEN

In diesem Unterthema werden Lehrer*innen in eine Reihe von Risiken eingeführt, denen sie online begegnen können. Es werden sowohl Risiken als auch Verantwortlichkeiten in der digitalen Welt diskutiert. Das Thema wird verschiedene Bedrohungen für Hard- und Software sowie für Daten/Informationen wie Arten von Cyberkriminalität, Malware, finanzielle Verluste und Identitätsdiebstahl, Internetbetrug abdecken und Einzelpersonen beibringen, wie sie sich vor diesen Risiken schützen und wie Schüler*innen über diese Bedrohungen aufgeklärt werden können.

Die folgenden Themen werden besprochen:

- Was ist Cybermobbing
- Verschiedene Arten von Cybermobbing
- Erkennen welche Schüler*innen von Cybermobbing betroffen sind
- Möglichkeiten betroffenen Schüler*innen zu helfen
- Präventionstage gegen Cybermobbing in der Schule zu veranstalten

THEMA 5 Cybermobbing

WAS IST CYBERMOBBING?

Cybermobbing ist Mobbing, das über digitale Kommunikationsmittel (z. B. Internet, Smartphones usw.) stattfindet, um eine andere Person wütend, traurig oder verängstigt zu machen.

Cybermobbing kann über SMS, Apps oder online in sozialen Medien, Foren oder Spielen stattfinden, wo Menschen Inhalte ansehen, daran teilnehmen oder sie teilen können.

Cybermobbing kann das Senden, Posten oder Teilen von negativen, schädlichen, demütigenden, peinlichen, falschen oder gemeinen Inhalten über eine andere Person beinhalten. Es kann das Teilen von persönlichen oder privaten Informationen über eine andere Person beinhalten, was zu Verlegenheit oder Erniedrigung führt.

Bestimmtes Cybermobbing überschreitet die Grenze zu ungesetzlichem oder kriminellem Verhalten.

THEMA 5 Cybermobbing

VERSCHIEDENE ARTEN VON CYBERMOBBING

Ermutigung zur Selbstverletzung - Einige Cybermobber drohen damit, ihre Opfer zu verletzen oder sie davon zu überzeugen, sich selbst zu verletzen. Es kann die schlimmste Art des Cybermobbing sein, weil es dazu führen kann, dass das Opfer sich durch Selbstmord das Leben nimmt.

Herabwürdigung - Die Verbreitung unwahrer oder schädlicher Gerüchte und Aussagen im Internet, die den Ruf einer Person schädigen. In der Regel handelt es sich bei diesen Angriffen um persönliche Angriffe, die bei den Opfern Wut auslösen, so dass sie ausfällig werden und sich schlecht verhalten.

Streiten - dazu gehört das Versenden wütender, grausamer, unhöflicher und vulgärer Nachrichten an eine oder mehrere Personen in einer privaten oder öffentlichen Online-Umgebung.

Happy Slapping - ein physischer Angriff auf eine Person als „Streich" oder „Scherz", während andere den Angriff filmen oder Fotos machen, die dann online verbreitet/gepostet werden.

THEMA 5 Cybermobbing

VERSCHIEDENE ARTEN VON CYBERMOBBING

Belästigung - Versenden einer fortlaufenden Reihe von verletzenden, beleidigenden Online-Nachrichten, die sich an eine Person richten.

Nachahmung - Vorgeben und Vortäuschen; sich als jemand anderes auszugeben und dann Informationen oder Ähnliches mit der Absicht, den Ruf einer Person zu schädigen, online zu versenden oder zu veröffentlichen.

Outing - Versenden oder Online-Posting von Material über eine Person, das sensible, private oder peinliche Informationen enthält.

Täuschung - Täuschen, um sich peinliches Material zu beschaffen, das dann online veröffentlicht wird. Die Person gibt vor, mit dem Opfer eng befreundet zu sein und vermittelt so ein falsches Gefühl der Sicherheit, bevor das Vertrauen gebrochen wird.

THEMA 5 Cybermobbing

VERSCHIEDENE ARTEN VON CYBERMOBBING

Sockpuppets - Eine Person erstellt ein Fake-Konto und gewinnt das Vertrauen des Opfers, indem sie vorgibt, jemand zu sein, die sie nicht ist. Wenn das Opfer private Informationen preisgibt, teilt der*die „Puppenspieler*in" diese persönlichen Informationen mit anderen, die das Opfer schikanieren können.

Catfishing - Einrichten eines gefälschten Online-Profils mit dem Ziel, das Opfer in eine betrügerische Online-Romanze zu locken.

Doxing - Wenn ein Cybermobber ein Opfer online belästigt und bedroht, um sich zu rächen und die Privatsphäre des Opfers zu zerstören. Doxing gibt private Informationen (z. B. Sozialversicherungsnummern, Kreditkarten, Telefonnummern und andere persönliche Daten) an die Öffentlichkeit weiter.

Absichtliche Ausgrenzung einer Person aus einer Online-Gruppe. Dies gilt als eine indirekte Form des Cybermobbings.

THEMA 5 Cybermobbing

BETROFFENE SCHÜLER*INNEN ERKENNEN

Kinder und Jugendliche sprechen vielleicht nicht offen über ihre Erfahrungen mit Cybermobbing, aber man sollte z. B. auf Verhaltensänderungen achten. Einige Anzeichen, ob eine Person ein Opfer von Cybermobbing ist, sind die folgenden:

Depression - Wenn die Person sich zurückzieht oder depressiv und traurig wirkt, verliert sie ihr Interesse an Personen oder Aktivitäten, die sie früher genossen hat oder in denen sie schläft, während sie das normalerweise nicht tat.

Vermeidung sozialer Situationen - Wenn die Person soziale Situationen oder Freund*innen meidet, mit denen sie in der Vergangenheit gerne Zeit verbracht hat, oder wenn sie viel Zeit allein verbringt.

Geänderte Häufigkeit der Nutzung von digitalen Geräten - Wenn die Person plötzlich immer an ihrem Handy, in sozialen Medien (oder per SMS) unterwegs ist. Zusätzlich könnte auch ein plötzlicher Rückgang der Gerätebenutzung ein Warnzeichen sein.

Geheimhaltung - Wenn die Person ihr Gerät versteckt, wenn man in ihrer Nähe ist, könnte sie verbergen wollen, dass sie online schikaniert wird.

THEMA 5 Cybermobbing

BETROFFENE SCHÜLER*INNEN ERKENNEN

Erhöhte Emotionen - Wenn die Person verärgert oder wütend zu sein scheint, wenn sie online ist oder weint, könnte dies ein Warnzeichen dafür sein, dass sie im Internet schikaniert wird. Lachen ist zwar nichts Schlimmes, aber auch das könnte ein Zeichen dafür sein, dass die Person selber Cybermobbing betreibt oder es mitverfolgt.

Verdächtige Social-Media-Accountaktivitäten - Wenn die Person plötzlich ihre Social-Media-Accounts kündigt, könnte das ein Zeichen dafür sein, dass sie in Cybermobbing verwickelt ist. Wenn sie mehrere Konten zu haben scheint, kann das ebenso ein Warnzeichen dafür sein, dass sie jemanden schikaniert.

Verdächtige Fotos - Wenn man auf dem Smartphone Bilder des verdächtigen Opfers sieht, die erniedrigend und unangemessen sind, könnte dies ein Zeichen dafür sein, dass es sich um Cybermobbing handelt. Wenn man auf dem Smartphone eines*einer verdächtigen Mobbers*in Bilder von einer anderen Person sieht, die erniedrigend und unangemessen sind, könnte auch dies ein Zeichen sein.

Verletzende Kommentare - Wenn es gemeine Kommentare gibt, die jemanden belästigen oder in Verlegenheit bringen, kann das ein Zeichen dafür sein, dass sie cyberbelästigt wird.

THEMA 5 Cybermobbing

WIE MAN BETROFFENEN HELFEN KANN

Wenn jemand Opfer von Cybermobbing ist, sollte man als erstes die eigene Unterstützung signalisieren und die Person wissen lassen, dass sie das, was geschieht, nicht verdient und dass man gemeinsam daran arbeiten wird, das Mobbing zu stoppen.

Man sollte das Opfer immer dazu ermutigen, mit einem zu sprechen. Gleichzeitig sollte man aber auch respektieren, wenn die Person die Situation allein lösen möchte.

Danach sollte man die Situation dokumentieren, indem man Screenshots von Beiträgen, Texten, E-Mails, Nachrichten und Fotos des Mobbingvorfalls macht. Sobald man Beweise hat, wendet man sich an die Schule des Opfers, um nach einer eventuellen Präventionsstrategie zu fragen.

Man kann auch mit Technikanbieter*innen zusammenarbeiten, um zu sehen, ob sie in der Lage sind die belästigenden Inhalte zu blockieren. Die meisten Webseiten, die interaktive Kommunikation erlauben, haben in ihren Nutzungsbedingungen Maßnahmen zur Einschränkung von belästigender Kommunikation vorgesehen.

THEMA 5 Cybermobbing

WICHTIGKEIT VON PRÄVENTION-TAGEN GEGEN CYBERMOBBING IN DER SCHULE

Programme zur Prävention und Intervention bei Cybermobbing sind entscheidend und notwendig. Die negativen Auswirkungen lassen sich in vier Kategorien einteilen (psychologisch, physisch, sozial und akademisch).

- Was die negativen Auswirkungen auf das psychologische Wohlbefinden betrifft, so hat sich herausgestellt, dass die Beteiligung am Cybermobbing mit Depressionen, Angst, Stress, emotionalen Problemen, geringem Selbstwertgefühl und Selbstmordgedanken zusammenhängt.

- Jugendliche, die Opfer von Cybermobbing geworden sind, berichten auch über eine schlechte körperliche Gesundheit.

- Sowohl bei Cyber-Opfern als auch bei Cyber-Mobber*innen wurden soziale Schwierigkeiten in ihren Beziehungen festgestellt.

- Cybermobbing hatte außerdem oft negative Auswirkungen auf die akademische Leistung.

Aufgrund der weltweiten Prävalenz und der negativen Folgen des Cybermobbing wird vorgeschlagen, Präventions- und Interventionsmethoden anzuwenden, um Kinder und Jugendliche vom Cybermobbing abzuhalten, sowie Strategien, die den Cyber-Opfern helfen, mit den negativen Auswirkungen des Cybermobbing umzugehen.

THEMA 5 Cybermobbing

WICHTIGKEIT VON PRÄVENTIONS-TAGEN GEGEN CYBERMOBBING IN DER SCHULE

Einige Präventionsstrategien sind hier aufgelistet:

- Sensibilisierung für die Auswirkungen von Cybermobbing, damit die Schüler die Auswirkungen verstehen, die dies auf andere hat, und dies vermeiden. Diejenigen, die schikanieren, müssen die Auswirkungen ihrer Handlungen verstehen und können oft von einer Beratung profitieren.
- Finden Sie die richtige Antwort auf Cybermobbing, nicht indem Sie den Mobber bestrafen, sondern hören Sie den Schülern zu und lassen Sie das Ziel Teil der Lösung sein. Oft sind Techniken der restaurativen Gerechtigkeit, bei denen die Schüler miteinander sprechen, um die Auswirkungen des Vorfalls zu verstehen, effektiv.
- Entwickeln Sie Aktivitäten, die zur Selbstreflexion anregen, und bitten Sie die Kinder, zu identifizieren und auszudrücken, was sie denken und fühlen, und die Gedanken und Gefühle anderer zu berücksichtigen. Helfen Sie Kindern, emotionale Intelligenz zu entwickeln, damit sie Selbstbewusstsein und Selbstregulierungsfähigkeiten erlernen und lernen, wie sie Empathie für andere entwickeln können.
- Zeigen Sie, dass Ihr Klassenzimmer eine sichere, emotional fürsorgliche Umgebung mit gegenseitigem Respekt und Toleranz ist.

THEMA 5 Cybermobbing

WICHTIGKEIT VON PRÄVENTIONS-TAGEN GEGEN CYBERMOBBING IN DER SCHULE

Einige Interventionsstrategien sind hier angeführt:

- Wenn Sie glauben, dass ein Schüler im Internet gemobbt wird, sprechen Sie privat mit ihm, um danach zu fragen. Geben Sie ihm / ihr Unterstützung und Sicherheit.
- Helfen Sie dem Schüler, relevante Beweise für Cybermobbing auf seinen digitalen Geräten aufzubewahren.
- Informieren Sie den Schüler darüber, welche Maßnahmen er ergreifen kann, um sicherzustellen, dass Cybermobbing nicht erneut auftritt. Dies kann das Ändern von Passwörtern, Kontaktdaten, das Sperren von Profilen auf Websites sozialer Netzwerke oder das Online-Melden von Missbrauch umfassen.
- Stellen Sie sicher, dass der Schüler sich nicht revanchiert oder auf die Nachrichten von Cybermobbing antwortet.
- Ermutigen Sie den Schüler, persönliche Informationen im Internet geheim zu halten.
- Machen Sie Screenshots von Posts, Texten, E-Mails, Nachrichten und Fotos, die Mobbing enthalten, und drucken Sie Kopien aus, um sie bei Bedarf als Beweismittel zu verwenden.
- Wenn Sie glauben, dass ein Schüler im Internet gemobbt wird, sprechen Sie mit seinen Eltern darüber.
- Wenn der Elternteil des Täters nicht reagiert und das Verhalten anhält, lassen Sie sich von Ihren Managern beraten, was als Nächstes zu tun ist.

THEMA 5 Cybermobbing

MeLDE

QUELLEN UND REFERENZEN

- Bell, R. G., Lipinski, J., Crothers, L. M., & Kolbert, J. B. (2015). Identification and Treatment of Cyber Bullying. Int J Sch Cog Psychol, 2(117), 10-4172.
- Espelage, D. L., & Hong, J. S. (2017). Cyberbullying prevention and intervention efforts: current knowledge and future directions. The Canadian Journal of Psychiatry, 62(6), 374-380.
- Tanrikulu, I. (2018). Cyberbullying prevention and intervention programs in schools: A systematic review. School psychology international, 39(1), 74-91.
- Kraft, E. M., & Wang, J. (2009). Effectiveness of cyber bullying prevention strategies: A study on students' perspectives. International Journal of Cyber Criminology, 3(2).
- Hong, J. S., Kim, D. H., Thornberg, R., Kang, J. H., & Morgan, J. T. (2018). Correlates of direct and indirect forms of cyberbullying victimization involving South Korean adolescents: An ecological perspective. Computers in Human Behavior, 87, 327-336.
- What Is Cyberbullying. Retrieved from

  https://www.stopbullying.gov/cyberbullying/what-is-it
- Willard, N., Harris, N. What Is Cyberbullying? Everything Parents Need to Know About Bullying Online. Retrieved from

  https://www.parents.com/kids/problems/bullying/period-shaming-is-a-kind-of-bullying-parents-need-to-be-aware-of/
- Grace Johansen, A. What is cyberbullying and what are the warning signs?. Retrieved from

  https://us.norton.com/internetsecurity-kids-safety-what-is-cyberbullying.html

MODUL 4 - E-SICHERHEIT

GLOSSAR

Begriff	Definition
CYBERMOBBING	Die Verwendung elektronischer Kommunikation, um eine Person zu schikanieren, typischerweise durch das Versenden von Nachrichten einschüchternder oder bedrohlicher Art.