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 sich online sicher verhalten können. Es werden Themen wie Risiken und Verantwortlichkeiten, Schutz persönlicher Daten, Fehlinformationen und schädliche Inhalte, digitales Urheber*innenrecht und wirksame sowie unwirksame Praktiken gegen Cybermobbing online 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 vorgestellt.
- 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 sichern 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 1 Risiken Online

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.

Folgende Themen werden diskutiert:

- verschiedene Bedrohungen für Hard- und Software
- verschiedene Bedrohungen für Daten und Informationen
- Arten von Cyberkriminalität, Malware, finanzielle Verluste und Identitätsdiebstahl, Internetbetrug
- Online Rechte und Verantwortlichkeiten

THEMA 1 Risiken Online

MeLDE

BEDROHUNGEN FÜR HARDWARE UND SOFTWARE

THREATS TO HARDWARE

Meltdown

Der Meltdown-Angriff nutzt kritische Schwachstellen in modernen Prozessoren aus, indem er es einem Prozess ermöglicht, den gesamten Speicher in einem bestimmten System zu lesen und so die grundlegendste Isolierung zwischen Anwendungen und dem Betriebssystem zu umgehen. Ein Merkmal moderner CPUs ist, dass sie in der Lage sind, Befehle und Operationen ungeordnet auszuführen. Dies ist nützlich, wenn es um die Beschleunigung der Datenverarbeitung geht, aber es öffnet auch ein Fenster für die transiente Ausführung, in dem unbefugter Zugriff auf den Kernbereich erlaubt wird.

Row hammer

Der Row-Hammer-Angriff nutzt elektrische Interaktionen zwischen benachbarten Speicherzellen in dynamischen DRAMs (Dynamic Random Access Memory) mit hoher Dichte aus, um Speicherfehler zu verursachen. Wenn ein Gegner mit eingeschränkten Rechten auf den DRAM einer Zielmaschine mit bestimmten Mustern zugreift, kann er Bit-Flips in Speichergebieten auslösen, die keine Berechtigung zum direkten Zugriff haben. Dieses Problem lässt sich nicht mit einem Software-Patch lösen. Die einzig mögliche Lösung ist der Austausch aller DDR-DRAM-Module.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR HARDWARE UND SOFTWARE

Computer mit herkömmlichem BIOS

Ältere PCs mit herkömmlichem BIOS sind nicht mit Secure Boot kompatibel. Letzteres ist ein Merkmal von UEFI (Unified Extensible Firmware Interface), einer modernen Lösung für eine Low-Level-Software auf neueren Hauptplatinen, die beim Hochfahren eines PCs beginnt, bevor das Betriebssystem gebootet wird. Secure Boot hilft zu verhindern, dass Malware während des Boot-Prozesses auf einen Computer geladen wird, indem das System auf Gültigkeit überprüft wird. Die UEFI unterstützt auch Netzwerkfunktionen direkt in ihrer Firmware, die bei der Fehlerbehebung und Konfiguration aus der Ferne hilfreich sein können.

Alte Router

Viele Router, die Kund*innen von Internet Service Providern (ISP) auf der ganzen Welt zur Verfügung gestellt bekommen, weisen schwerwiegende Mängel auf, die es Hacker*innen aus der Ferne ermöglichen, die Kontrolle über sie zu übernehmen. Die meisten Router haben einen "Directory Traversal"-Fehler in einer Firmware-Komponente namens webproc.cgi, die es Hacker*innen erlaubt, sensible Konfigurationsdaten, einschließlich administrativer Zugangsdaten, zu extrahieren. Sobald ein Router einmal beeinträchtigt ist, kann er für Denial-of-Service-Angriffe (DDoS) oder für die Zertifizierung von Berechtigungsnachweisen verwendet werden. Sie können auch dazu verwendet werden, die Quelle illegaler Aktivitäten zu verbergen, da der Datenverkehr eher von zufälligen Adressen als von seinem wahren Ursprung zu kommen scheint.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR HARDWARE UND SOFTWARE

BEDROHUNGEN FÜR SOFTWARE

Computervirus

Ein Computervirus ist eine der häufigsten Bedrohungen für die Cybersicherheit. Ein Computervirus ist eine Art von bösartigem Code oder Programm, das geschrieben wurde, um die Funktionsweise eines Computers zu verändern, das so konzipiert ist, dass es sich von Wirt zu Wirt verbreitet und die Fähigkeit besitzt, sich selbst zu replizieren. Er wird oft als E-Mail-Anhang verschickt oder von bestimmten Webseiten heruntergeladen mit der Absicht, den Host-Computer zu infizieren. Sobald die Umstände dazu führen, dass der Computer oder das Gerät den Viruscode ausführt, ist er in der Lage, Spam zu versenden, die Sicherheitseinstellungen des Geräts zu deaktivieren, Daten, einschließlich persönlicher Informationen wie Passwörter, zu beschädigen und zu stehlen. Viren können sogar so weit gehen, dass sie alles auf Ihrer HDD, SSD oder SD-Karte des angegriffenen Geräts löschen.

Adware

Als Adware gilt jede Software, die dazu dient, Daten über die Surfgewohnheiten von Personen zu verfolgen und ihnen auf dieser Grundlage Werbung und Pop-ups anzuzeigen. Adware sammelt Daten mit dem Einverständnis der Benutzenden und ist sogar eine legitime Einnahmequelle für Unternehmen, die es den Benutzenden erlauben, ihre Software kostenlos auszuprobieren, aber mit Werbung, die während der Benutzung der Software angezeigt wird. Die Klausel der Werbesoftware ist oft in den zugehörigen Dokumenten der Nutzungsvereinbarung versteckt, aber sie kann überprüft werden, indem man alles, was bei der Installation der Software akzeptiert wurde, sorgfältig liest. Das Vorhandensein von Werbesoftware auf einem Computer wird nur durch die Pop-up-Fenster bemerkbar. Manchmal kann sie den Prozessor des Computers und die Geschwindigkeit der Internetverbindung verlangsamen. Wenn Werbesoftware ohne Zustimmung heruntergeladen wird, gilt sie als bösartig.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR HARDWARE UND SOFTWARE

Spyware

Spyware funktioniert ähnlich wie Adware, wird aber ohne Wissen auf dem Computer installiert. Es wird als eine Software bezeichnet, die einen Computer in irgendeiner Weise verändert, indem sie sich selbst installiert oder einige Daten auf dem Computer zum späteren Abruf speichert. Sie kann Keylogger enthalten, die persönliche Daten wie E-Mail-Adressen, Passwörter und sogar Kreditkartennummern aufzeichnen, was sie wegen des hohen Risikos von Identitätsdiebstahl gefährlich macht.

Ungepatchte oder veraltete Betriebssysteme/Software/Browser

Software hat einen kurzen Lebenszyklus, der durch ständige Aktualisierungen und Upgrades aufrechterhalten wird. Ungepatchte oder veraltete Betriebssysteme/Software/Browser können die Sicherheit der Nutzer*innen durch Fehler und Lücken in Systemen, die noch nicht entdeckt und gepatcht wurden, potenziell gefährden. Ungepatchte oder veraltete Systeme sind für Hacker*innen leicht zugänglich, so dass sie die Sicherheitslücken auf Systemebene ausnutzen können. Außerdem sind veraltete Systeme Lösegeld-Angriffen ausgesetzt, was bedeutet, dass eine Form von Malware das System angreifen, die Dateien der*des Benutzenden verschlüsseln und ein Lösegeld für die Wiederherstellung des Zugriffs auf die Daten gegen Bezahlung verlangen kann.

THEMA 1 Risiken Online

MeLDE

BEDROHUNGEN FÜR HARDWARE UND SOFTWARE

METHODEN ZUM SCHUTZ DES COMPUTERS:

- Firewall eingeschaltet lassen
- Antiviren-Software installieren oder aktualisieren
- Anti-Spyware-Technologie installieren oder aktualisieren
- Betriebssystem auf dem neuesten Stand halten
- Vorsicht beim Herunterladen
- Computer ausschalten
- Systeme und Software regelmäßig patchen, um zu verhindern, dass Cyberkriminelle bekannte Schwachstellen für Angriffe ausnutzen
- Dateien und Software nur von seriösen Webseiten herunterladen
- Links, E-Mails oder Anhänge von unbekannten und verdächtigen Absendern nicht öffnen

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

CYBERCRIME

Hacking

Computer-Hacker*innen sind nicht autorisierte Nutzer*innen, die in Computersysteme einbrechen, um Informationen zu stehlen, zu verändern oder zu zerstören, oftmals durch die Installation gefährlicher Malware ohne das Wissen oder die Zustimmung der betroffenen Person. Jede Person, die einen mit dem Internet verbundenen Computer benutzt, ist anfällig für die von Computer-Hacker*innen ausgehenden Bedrohungen. Während ein Computer mit dem Internet verbunden ist, überträgt Malware, die ein*e Hacker*in auf dem PC installiert haben könnte, persönliche und finanzielle Informationen still und heimlich, ohne das Wissen oder die Zustimmung der betroffenen Person.

Keylogging

Eine der besten Methoden zur Erfassung von Passwörtern ist die ferngesteuerte Protokollierung von Tastenanschlägen, bekannt als Keylogging, d.h. die Verwendung von Software oder Hardware zur Aufzeichnung von Eingaben, während diese in den Computer eingegeben werden. Ein Keylogger ist eine Funktion, die Tastatureingaben auf einem Computer aufzeichnet. Auf dieser grundlegenden Ebene betrachtet, sieht ein Keylogger absolut harmlos aus. In den Händen einer*s Hackers*in oder Cyberkriminellen ist ein Keylogger jedoch ein wirkungsvolles Instrument, um Informationen zu stehlen. Keylogger sind eine ernsthafte Bedrohung für Nutzer*innen und deren Daten, da sie die Tasteneingaben verfolgen, um Passwörter und andere sensible Informationen zu erfassen. Dadurch haben Hacker*innen den Vorteil, dass sie Zugriff auf PIN-Codes und Kontonummern, Passwörter für Online-Shopping-Webseiten, E-Mail-IDs, Logins und andere vertrauliche Informationen erhalten.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

Pharming

Pharming ist eine Wortkreuzung aus den Wörtern "Phishing" und "Farming" und ist eine betrügerische Praxis, bei der ein bösartiger Code auf einem PC installiert wird und Nutzer*innen ohne ihr Wissen oder Zustimmung auf betrügerische Webseiten umleitet. Pharming nutzt die Grundlagen der Funktionsweise des Internet-Browsing aus. Die Buchstabenfolge, die eine Internet-Adresse wie www.google.com bildet, muss von einem DNS-Server in eine IP-Adresse umgewandelt werden, damit die Verbindung zustande kommt. Pharming greift diesen Prozess durch die Installation eines Virus oder Trojaners durch Hacker*innen auf dem Computer einer Person an, der die Host-Dateien des Computers so verändert, dass der Datenverkehr von seinem beabsichtigten Ziel weg auf eine gefälschte Webseite gelenkt wird. Die unrechtmäßigen Webseiten können dazu benutzt werden, Viren oder Trojaner auf dem Computer zu installieren; oder sie könnten ein Versuch sein, persönliche und finanzielle Informationen zwecks Identitätsdiebstahl zu sammeln.

Social Engineering

Unter Social Engineering versteht man im Zusammenhang mit Informationssicherheit den Einsatz von Täuschung, um Personen so zu manipulieren, dass sie vertrauliche oder persönliche Informationen preisgeben, die für betrügerische Zwecke verwendet werden können. Es werden dabei psychologische Manipulationen eingesetzt, um Nutzer*innen dazu zu verleiten, Sicherheitsfehler zu machen oder sensible Informationen preiszugeben. Die Täter*innen untersuchen zunächst das beabsichtigte Opfer, um die notwendigen Hintergrundinformationen zu sammeln, wie z. B. potentielle Eintrittspunkte und schwache Sicherheitsprotokolle, die für die Durchführung des Angriffs erforderlich sind. Dann versuchen sie das Vertrauen des Opfers zu gewinnen und Anreize für Aktionen zu schaffen, die die Sicherheitspraktiken durchbrechen, wie z. B. die Weitergabe sensibler Informationen oder die Gewährung des Zugangs zu kritischen Ressourcen. Was Social Engineering besonders gefährlich macht, ist, dass es auf menschlichem Versagen beruht und nicht auf Schwachstellen in Software und Betriebssystemen. Fehler, die von legitimen Nutzer*innen gemacht werden, sind viel weniger vorhersehbar, was es schwieriger macht, sie zu erkennen und zu verhindern als ein auf Malware basierender Angriff.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

DOS- und DDOS-Angriff

Ein Denial-of-Service-Angriff (DoS-Angriff) wird von einem Rechner und seiner Internetverbindung durchgeführt, indem eine Webseite mit Daten überflutet und es Nutzer*innen unmöglich gemacht wird, auf den Inhalt der überfluteten Webseite zuzugreifen.
Ein Distributed Denial of Service (DDoS)-Angriff ähnelt einem DoS-Angriff, ist aber wesentlich aggressiver. Es ist schwieriger, einen DDoS-Angriff zu überwinden. Er wird von mehreren Computern aus gestartet und die Anzahl der beteiligten Computer kann von einigen wenigen bis zu Tausenden oder sogar mehr reichen. Da es wahrscheinlich ist, dass nicht alle diese Computer der angreifenden Partie gehören, werden sie kompromittiert und dem Netzwerk durch Malware hinzugefügt. Diese Computer können über den gesamten Globus verteilt sein, und dieses Netzwerk aus Computern wird als Botnet bezeichnet. Da der Angriff von so vielen verschiedenen IP-Adressen gleichzeitig ausgeht, ist ein DDoS-Angriff für das Opfer viel schwieriger zu lokalisieren und abzuwehren.

Phishing

Phishing ist eine Methode des Social Engineering mit dem Ziel, an sensible Daten wie Passwörter, Benutzer*innennamen und Kreditkartennummern zu gelangen. Die Angriffe erfolgen häufig in Form von Sofortnachrichten oder Phishing-E-Mails, die so gestaltet sind, dass sie seriös und legitim erscheinen. Die Empfänger*innen der E-Mail werden dann dazu verleitet, einen bösartigen Link zu öffnen, der zur Installation von Malware auf dem Computer der betroffenen Person führt. Sie kann auch persönliche Informationen erhalten, die scheinbar von einer Bank gesendet wurde, die darum bittet, die Identität der Person zu überprüfen, indem sie private Informationen preisgibt.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

Spamming

Die Informationsflut im Internet mit unaufgeforderten oder irreführenden Nachrichten kann als **Spamming** bezeichnet werden. Spam wird meist für aggressive kommerzielle Werbung eingesetzt. Die häufigste Form ist E-Mail-Spamming, gefolgt von Suchmaschinen-Spamming. Erstere ist das Versenden unerwünschter E-Mails an eine wahllose Gruppe von Empfänger*innen. Letzteres ist die Modifizierung von HTML-Seiten, um die Chance zu erhöhen, dass diese unter den ersten Suchergebnissen platziert werden.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

MALWARE (BÖSARTIGE SOFTWARE)

Rogue-Sicherheits-Software

Rogue-Sicherheits-Software ist eine bösartige Software, die Nutzer*innen zu der Annahme verleitet, dass auf ihrem PC ein Computervirus installiert ist oder dass ihre Sicherheitsmaßnahmen nicht auf dem neuesten Stand sind. Dann bieten sie an, die angeblich benötigten Sicherheitseinstellungen zu installieren oder zu aktualisieren. Entweder bitten sie Nutzer*innen, ihr Programm herunterzuladen, um die angeblichen Viren zu entfernen, oder sie fordern sie auf, für ein Tool zu bezahlen. Beide Fälle führen dazu, dass tatsächlich Malware auf dem Computer des Opfers installiert wird.

Ein Trojanisches Pferd

Ein Trojanisches Pferd oder "Trojaner" ist ein bösartiger Angriffscode oder eine Software, die Nutzer*innen dazu verleitet, sie freiwillig auszuführen, indem sie sich hinter einem legitimen Programm verstecken. Sie verbreiten sich oft per E-Mail. Dabei tarnen sie sich meist als vertraute Personen. Wenn man dann auf die E-Mail und den beigefügten Anhang klickt, wird sofort Malware auf den Computer heruntergeladen. Trojaner verbreiten sich auch, wenn man auf eine gefälschte Werbung klickt. Sobald sich ein Trojaner auf dem Computer befindet, kann er die Passwörter aufzeichnen, indem er Tastenanschläge protokolliert, die Webcam übernimmt und sensible Daten auf stiehlt.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

Computerwürmer

Computerwürmer sind Teile von Malware-Programmen, die sich schnell replizieren und von einem Computer zum anderen verbreiten. Ein Wurm verbreitet sich von einem infizierten Computer aus, indem er sich selbst an alle Kontakte des Computers sendet und dann sofort an die Kontakte der anderen Computer. Die Übertragung von Würmern erfolgt häufig auch durch Ausnutzung von Software-Schwachstellen. Interessanterweise sind sie nicht immer darauf ausgelegt, Schaden anzurichten. Es gibt Würmer, die nur dazu bestimmt sind, sich zu verbreiten.

Rootkit

Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf Fernkontroll- und Verwaltungsebenen über einen Computer oder Computernetzwerke ermöglicht. Sobald der Fernzugriff möglich ist, kann das Rootkit eine Reihe von böswilligen Aktionen ausführen: Keylogging, Passwortdiebstahl und die Deaktivierung von Antivirenprogrammen. Rootkits werden installiert, indem sie sich in legitimer Software verstecken. Wenn man dieser Software die Erlaubnis erteilt, Änderungen an dem Betriebssystem vorzunehmen, installiert sich das Rootkit auf dem Computer und wartet darauf, dass der*die Hacker*in es aktiviert. Andere Möglichkeiten der Verbreitung von Rootkits sind Phishing-E-Mails, also bösartige Links oder Dateien sowie das Herunterladen von Software von verdächtigen Webseiten.

THEMA 1 Risiken Online

BEDROHUNGEN FÜR DATEN UND INFORMATIONEN

FINANZIELLE VERLUSTE

Informationssicherheit ist ein kritisches Problem für Einzelpersonen und Organisationen, da sie zu großen finanziellen Verlusten führt. Gestohlene Zahlungskarteninformationen, wie Name, Kartennummer und Ablaufdatum können für betrügerische Online-Käufe verwendet werden. Das Potenzial für schädliche Auswirkungen kann bei betrügerisch verwendeten Zahlungskarteninformationen viel größer sein, insbesondere wenn diese Daten mit der Kreditkarte einer*s Nutzer*in verknüpft sind.

IDENTITÄTSDIEBSTAHL

Identitätsdiebstahl, auch als Identitätsbetrug bekannt, ist ein Verbrechen, bei dem sich Betrüger*innen wichtige persönliche Daten wie Sozialversicherungs- oder Führerscheinnummern beschaffen, um sich als jemand anderes auszugeben. Die Informationen können verwendet werden, um Kredite, Waren und Dienstleistungen im Namen des Opfers zu erhalten oder um der Betrugsperson gefälschte Referenzen zur Verfügung zu stellen. Zusätzlich zur Schuldenaufnahme können Betrüger*innen in seltenen Fällen der Polizei falsche Ausweise vorlegen, ein Strafregister erstellen oder Haftbefehle für die Person, deren Identität gestohlen wurde, ausstellen lassen.

THEMA 1 Risiken Online

MÖGLICHKEITEN INTERNET-BETRUG ZU MELDEN

- **Cyberkriminalität online melden**

https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

- **Einen Vorfall in der Informationssicherheit melden**

https://ec.europa.eu/growth/tools-databases/security-incidents_en

Internationalen Online-Betrug melden

https://www.econsumer.gov/#crnt

- **Cyberkriminalität in Großbritannien melden**

https://www.actionfraudalert.co.uk/Contact

- **Cyberkriminalität in Zypern melden**

https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm

- **Cyberkriminalität in Griechenland melden**

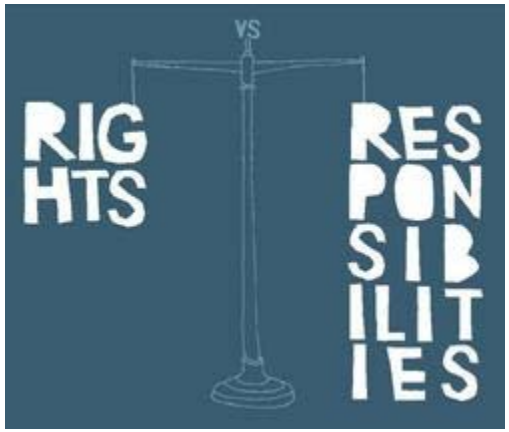
http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=

THEMA 1 Risiken Online

ONLINE RECHTE UND VERANTWORTLICHKEITEN

ONLINE-RECHTE

- Zugriff auf Wissen darüber, wie das Internet funktioniert und wie Informationen zugänglich sind
- Zugriff auf Wissen darüber, was Fakten sind und was nicht
- wissen, was Content und was Werbung ist
- Schutz der Privatsphäre
- Schutz vor Belästigung/Gewalt
- Sich körperlich, geistig und emotional sicher fühlen
- Kontrolle persönlicher Daten
- Einfaches Melden von verstörenden/störenden/schädlichen Online-Content an die Internet-Provider
- mit Freund*innen reden können
- An Diskussionen/Foren teilnehmen
- Neue Inhalte erstellen können

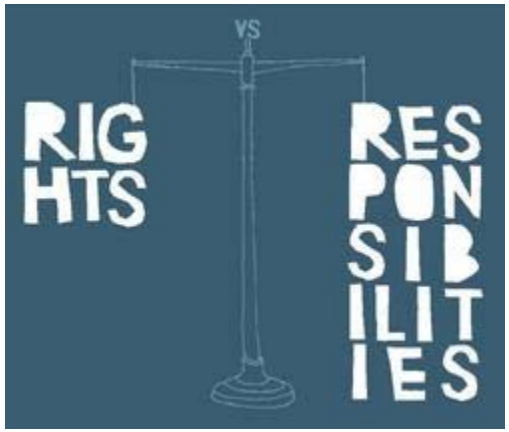


THEMA 1 Risiken Online

ONLINE RECHTE UND VERANTWORTLICHKEITEN

ONLINE-VERANTWORTLICHKEITEN

- Persönliche Daten und geistiges Eigentum anderer Nutzer*innen respektieren und diese Daten nicht ohne Zustimmung der Eigentümer*innen veröffentlichen
- Passwörter geheim halten und dementsprechend schwierige Passwörter wählen
- andere nicht belästigen/beschimpfen
- Fremde meiden und schädliches oder verdächtiges Verhalten melden
- die Identität und Werte anderer Nutzer*innen respektieren
- sich des eigenen digitalen Fußabdrucks bewusst sein und wie dieser Einfluss darauf hat, man selbst wahrgenommen wird und wen und was man selbst repräsentiert
- Anderen und insbesondere jüngeren Kindern helfen, sicher im Internet zu navigieren
- immer die Validität von Online-Informationen überprüfen
- nur Webseiten besuchen, die dem eigenen Alter entsprechen
- Alle Altersbeschränkungen respektieren und die „Bedingungen" und „Richtlinien" der Webseiten lesen



THEMA 1 Risiken Online

ZUSAMMENFASSUNG

- Passwörter und sensible Daten können durch viele Hardware- und Software-Schwachstellen in modernen Computern durchsickern.
- Es ist wichtig, dass man alles Mögliche tut, um den eigenen Computer und Daten zu schützen.
- Die wichtigsten Bedrohungen für Daten und Informationen sind Cyberkriminalität, Malware (MALicious softWARE), finanzieller Verlust und Identitätsdiebstahl.
- Es gibt viele Möglichkeiten, Internet-Betrug zu melden und es liegt in unserer Verantwortung, dies zu tun.
- Wir sind als Internet-Nutzer*innen verpflichtet, unsere Online-Rechte zu schützen und einzufordern, aber auch unsere Online-Verantwortung zu übernehmen.

THEMA 1 Risiken Online

MeLDE

QUELLEN UND REFERENZEN

- Biryukov, V. (2015, April 1). Deep Dive: 5 Threats Affecting Hardware. Retrieved from https://www.kaspersky.com/blog/hardware-malware/8169/
- Lindros, K. (2016, October 12). 12 hardware and software vulnerabilities you should address now. Retrieved from https://www.computerworld.com/article/3130119/12-hardware-and-software-vulnerabilities-you-should-address-now.html
- Lucian, C. (2015, March 19). At least 700,000 routers given to customers by ISPs are vulnerable to hacking. Retrieved from https://www.cio.com/article/2899734/at-least-700000-routers-given-to-customers-by-isps-are-vulnerable-to-hacking.html
- The security risks of outdated software. Retrieved from https://www.parkersoftware.com/blog/the-security-risks-of-outdated-software/
- SecurityTrails Team. (2018, October 16). Top 10 Common Network Security Threats Explained. Retrieved from https://securitytrails.com/blog/top-10-common-network-security-threats-explained
- Sanchez, M. (2010, December 9). The 10 most common security threats explained. Retrieved from https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained
- Maina, A. (2017, February 16). What is Spamming? Hint: It Involves More Than Just Email. Retrieved from https://smallbiztrends.com/2017/02/what-is-spamming.html
- Rouse, M. pharming. Retrieved from https://searchsecurity.techtarget.com/definition/pharming
- On the Internet. Retrieved from https://www.fbi.gov/scams-and-safety/on-the-internet

THEMA 1 Risiken Online

QUELLEN UND REFERENZEN

- Internet Fraud. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud
- Rouse, M. identity theft. Retrieved from https://searchsecurity.techtarget.com/definition/identity-theft
- Trend Micro Team. (2018, October 31). Information security: How Hackers Leverage Stolen Data for Profit. Retrieved from https://blog.trendmicro.com/information-security-how-hackers-leverage-stolen-data-for-profit/
- Oglethorpe, M. (2013, February 5). Rights and Responsibilities Online: Safer Internet Day 2013. Retrieved from https://themodernparent.net/rights-and-responsibilities-online-safer-internet-day-2013/

MODUL 4 - E-SICHERHEIT

GLOSSAR

Begriff	Definition
ADWARE	Unter Adware versteht man sämtliche Software, die dazu dient, Daten über die Surfgewohnheiten von Nutzer*innwn zu verfolgen, um ihnen Werbung und Pop-ups anzuzeigen.
COMPUTER VIRUS	Ein Computervirus ist eine Art von bösartigem Code oder Programm, das geschrieben wurde, um die Funktionsweise eines Computers zu verändern und das so konzipiert ist, dass es sich von Wirt zu Wirt verbreitet und die Fähigkeit besitzt, sich selbst zu replizieren.
COMPUTER WURM	Ein Computerwurm ist ein Malware-Programm, das sich schnell repliziert und von einem Computer zum anderen verbreitet.
HACKING	Hacking liegt vor, wenn unbefugte Nutzer*innen in Computersysteme einbrechen, um Informationen zu stehlen, zu verändern oder zu zerstören, oft durch die Installation gefährlicher Malware ohne Wissen oder Zustimmung der Nutzer*innen.
KEYLOGGING	Keylogging ist die Verwendung von Soft- oder Hardware zur Aufzeichnung von Tasteneingaben, während diese in den Computer eingetippt werden.
PHARMING	Pharming ist eine Betrugsmethode, bei der ein bösartiger Code auf einem PC installiert wird und Nutzer*innen ohne ihr Wissen oder Zustimmung auf betrügerische Webseiten umleitet.
PHISHING	Phishing ist eine Methode des Social Engineering mit dem Ziel, an sensible Daten wie Passwörter, Benutzernamen und Kreditkartennummern zu gelangen.

MODUL 4 - E-SICHERHEIT

GLOSSAR

Begriff	Definition
ROOTKIT	Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf Fernkontroll- und Verwaltungsebenen über einen Computer oder Computernetzwerke ermöglicht.
SPAMMING	Spamming ist die Informationsflut im Internet mit unerwünschten oder irreführenden Meldungen.
SPYWARE	Spyware ist jede Software, die dazu dient, Daten über die Surfgewohnheiten der Nutzer*innen zu verfolgen, um ihnen Werbung und Pop-ups anzuzeigen und die ohne deren Wissen auf dem Computer installiert wird.
SOCIAL ENGINEERING	Unter Social Engineering versteht man Täuschung, um Personen so zu manipulieren, dass sie vertrauliche oder persönliche Informationen preisgeben, die für betrügerische Zwecke verwendet werden können.
TROJANISCHES PFERD	Ein Trojanisches Pferd ist ein bösartiger Angriffscode oder eine Software, die Nutzer*innen dazu verleitet, sie freiwillig auszuführen, indem sie sich hinter einem seriösen Programm verstecken.