DIGITALISIERUNG
REALITÄT

DIGITALITÄT
&
KRIMINALITÄT

Cybersecurity | Cybercrime | Hacking

Datenschutz | Phishing

UNTERRICHTSENTWURF

2 UE á 45 Minuten

Digitale Lernwerkstatt

DIGITALE LERNWERKSTATT

JUGENDLICHE FIT MACHEN FÜR DEN DIGITALEN ARBEITSMARKT!

Mit der Digitalen Lernwerkstatt wollen wir Digitalisierung verständlich machen und digitale Kompetenzen vermitteln. Auf unserer Webseite www.digitale-lernwerkstatt.com bieten wir kostenlose Online-Module zum Selbstlernen für Jugendliche und Unterrichtsmaterial für Lehrer/innen.

Weitere Informationen zu unserem gesellschaftlichen Engagement finden Sie unter www.accenture.de/corporate.citizenship oder schreiben Sie uns unter: cc.asgr@accenture.com. Wir freuen uns auf Ihre Nachricht!

INHALTSVERZEICHNIS

1 EINLEITUNG

Dieses Themenheft eignet sich dazu, Schüler/innen mit unterschiedlichem Vorwissen mit dem Thema Digitale Kriminalität vertraut zu machen. Es werden wichtige Begriffe erklärt, Formen von Cyberkriminalität behandelt und Folgen für Betroffene verdeutlicht. Die Schüler/innen lernen, wie sie sich selbst vor Angriffen schützen können. In einem nächsten Schritt setzen sich die Schüler/innen mit den Motiven der Kriminellen auseinander und beleuchten die Möglichkeiten von Unternehmen im Schutz gegen Cyberattacken.

NUTZUNGSHINWEISE

Dieses Arbeitsbuch beinhaltet einen flexiblen Vorschlag zur Unterrichtsgestaltung. Sie können Ihren Unterricht ohne Hilfe von digitalen Medien gestalten oder mit verschiedenen Online-Materialien anreichern.

In diesem Themenheft werden Ihnen verschiedene Lernformate angeboten. Diese sind mit den hier dargestellten Symbolen gekennzeichnet und lassen sich durch das Anklicken öffnen.

Arbeitsblatt	*Kopiervorlage (auch im Anhang zu finden)*
PowerPoint Präsentation	*Computer und Beamer werden benötigt*
Video	*Computer und Beamer werden benötigt*
Online Training	*Computer/Smartphone für jede/n Schüler/in (Bearbeitung auch in Kleingruppen von 2-3 Personen möglich)*

Bitte beachten Sie, dass Sie für das Aufrufen dieser zusätzlichen Materialien zum Teil einen Internetzugang benötigen. Dieser wird im Folgenden mit dem nebenstehenden Symbol ergänzend hervorgehoben. Sie finden das Zeichen jeweils am Seitenrand der betreffenden Lernmedien.

2 DIGITALITÄT UND KRIMINALITÄT FÜR EINSTEIGER

2.1 INHALT

Diese Unterrichtseinheit sensibilisiert Ihre Schüler/innen für das Thema Cyberkriminalität. Sie lernen grundlegende Begriffe kennen und erfahren, welche Konsequenzen ein Angriff für Betroffene haben kann. Abschließend setzen Sie sich damit auseinander, welches Verhalten sie vor Cyberkriminalität schützen kann.

Dauer Offline:

45 Minuten

Im Anhang bieten wir Ihnen einen Zeitplan zur Strukturierung dieser Unterrichtseinheit.

2.2 LERNZIELE

1. *Wissen, was Cyberkriminalität bedeutet.*
2. *Verstehen, welche Folgen Cyberkriminalität haben kann.*
3. *Erkennen, wie man sich vor Angriffen schützen kann.*

Zusätzlich zu diesem Unterrichtsvorschlag, finden Sie im Anhang eine Auflistung aller Unterrichtsmaterialien, welche von der Digitalen Lernwerkstatt zu diesem Thema zur Verfügung gestellt werden.

2.3 BEDEUTUNG VON CYBERKRIMINALIÄT

2.3.1 Begriffsklärung

Cyberkriminalität begegnet heute fast Jedem. Bei einer Umfrage der Bitkom Research in Deutschland aus dem Jahr 2017 gaben ca. die Hälfte der Befragten an, in den letzten zwölf Monaten Erfahrungen mit Cyberkriminalität gemacht zu haben. Dies verdeutlicht, dass auch Ihre Schüler/innen sich der Gefahren im Netz bewusst werden müssen. Doch was ist eigentlich Cyberkriminalität?

DEFINITION

*Straftaten, bei denen die Täter moderne Informationstechnik nutzen, werden zunächst ganz allgemein als **Cyberkriminalität** (engl. cybercrime) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potentielle Opfer via E-Mail statt per Post erreicht.*

https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html

Wenn Cyberkriminalität so allgegenwärtig ist, hat vielleicht auch eine/r Ihrer Schüler/innen bereits persönliche Erfahrungen mit dem Thema gemacht? Sollte es niemanden in Ihrer Klasse getroffen haben, können Sie auf ein lebensnahes Beispiel im Anhang zurückgreifen, um Ihre Schüler/innen eingangs für das Thema zu sensibilisieren.

ARBEITSBLATT

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

DIDAKTISCHER TIPP

Fragen Sie Ihre Schüler/innen, wer bereits persönlich oder im Bekanntenkreis Erfahrungen mit Internetkriminalität gemacht hat. Dazu zählen z.B. folgende Bereiche:

- *Phishing E-Mail bekommen*
- *Virus auf dem Computer*
- *Chat mit einer Person, welche vorgibt jemand anderes zu sein*
- *Datendiebstahl*

Um sich tiefergehend mit dem Thema Kriminalität im Netz auseinanderzusetzen, ist es zunächst wichtig, grundlegende Schlagwörter kennenzulernen. Führen Sie dazu das folgende Online Training durch, welches einen umfassenden Einstieg in das Thema bietet. Zunächst werden einleitende Informationen zu Methoden und Gründen von Cyberkriminalität vermittelt. Anschließend wird erklärt, was unter Cyberkriminalität und Cybersecurity zu verstehen ist.

ONLINE TRAINING

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

DEFINITION CYBERSECURITY

*Unter **Cybersecurity** versteht man diejenigen Maßnahmen, die ergriffen werden, um einen Computer oder ein Computersystem vor Hackerangriffen oder unbefugtem Zugriff zu schützen.*

https://www.merriam-webster.com/dictionary/cybersecurity

2.3.2 Angriffspunkte und Konsequenzen

Nachdem Ihre Schüler/innen nun gelernt haben, wie präsent Cyberkriminalität im Alltag ist und welche wichtigen Begriffe damit in Verbindung stehen, geht es nun darum zu verstehen, wie wichtig der Schutz der eigenen Daten ist. Zeigen Sie dazu dieses Video, in dem erklärt wird, wie Hacker an Nutzerdaten und Passwörter gelangen und welche Konsequenzen dadurch für die Betroffenen entstehen können.

VIDEO

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

Angriffspunkte entstehen beispielsweise durch das Verwenden eines sehr einfachen Passworts bei der Anmeldung für Apps, Soziale Netzwerke, Online Shopping oder auch Online Banking. Die Folgen für die Betroffenen sind vielfältig: Hacker stehlen Bankdaten, um diese beim Online Shopping einzusetzen, Zugangsdaten zum Online Banking, um Gelder zu entwenden oder sie spezialisieren sich auf Datendiebstahl. Geklaute Datensätze können leicht weiter veräußert werden oder sie werden

eingesetzt, um mit der geklauten Identität Internetbetrug zu begehen. Betroffene haben also nicht nur Ärger, beispielsweise mit Ihrer Bank oder mit Freunden, deren Daten geklaut wurden, es kann sogar zu juristischen Konsequenzen kommen.

2.4 SCHUTZ VOR CYBERKRIMINALITÄT

2.4.1 Cyberattacken identifizieren

Doch wie erkennt man eine Cyberattacke? Welchen weiteren Angriffspunkten müssen Ihre Schüler/innen im Alltag entgehen? Nutzen Sie dieses Arbeitsblatt, um Ihre Schüler/innen in Einzel- oder Gruppenarbeit für verschiedene Formen von Angriffen zu sensibilisieren. Die Aufgabe besteht darin, in unterschiedlichen alltagsnahen Situationen einzuschätzen, welches Verhalten geeignet ist, um einem Angriff durch Viren oder Phishing-Mails zu entgehen.

ARBEITSBLATT

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

DIDAKTISCHER TIPP

Lassen Sie die Aufgabe in Kleingruppen ausführen und küren Sie die Gruppe mit den meisten richtigen Antworten im Anschluss zum „Held der Cybersecurity“.
Sollten auffallend viele falsche Antworten gegeben worden sein, verdeutlichen Sie Ihren Schüler/innen noch einmal die Konsequenzen für sich und Andere.

WUSSTEN SIE SCHON?

Die durch Cyberkriminalität entstandenen finanziellen Schäden lagen im Jahr 2016 bei ca 52 Mio. Euro.

Quelle: Bundeskriminalamt

2.4.2 Schutz vor Cyberattacken

Ihre Schüler/innen sollten nun Cyberattacken ohne größere Schwierigkeiten identifizieren können. Doch wie können Sie sich vor zukünftigen Angriffen schützen? Die folgende Liste gibt einen kurzen Überblick über wichtige Tipps zum Schutz der eigenen Daten:

- **E-Mails**
  - Keine vertraulichen Informationen per E-Mail versenden
  - Vorsichtig sein im Umgang mit E-Mail Anhängen
- **Handy**
  - Sicherheitssoftware installieren
  - Kein Jailbreak/Rooting vornehmen
  - GPS, Bluetooth und WLAN nur wenn benötigt einschalten
- **Passwörter**
  - Alle Geräte über Passwörter schützen
  - Passwörter niemandem mitteilen
- **Online Banking**
  - Nur private Geräte für den Zugang nutzen
  - Abrechnungen und Kontoauszüge regelmäßig prüfen
- **Daten**
  - Regelmäßige Back-Ups erstellen
- **Verhalten im Netz**
  - Vorsichtig mit neuen Bekannten im Netz sein
  - Vorsichtiger Umgang mit persönlichen Daten im Netz
  - Ausloggen vor dem Verlassen einer Website
- **Software**
  - Software nur aus vertrauenswürdigen Quellen nutzen
  - Virenschutz-Software nutzen

ONLINE TRAINING

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

Lassen Sie die Schüler/innen dieses Online Training durchführen, um tiefergehende Informationen zu den dargestellten Schutzmaßnahmen zu erlangen. Weiterhin erfahren sie, wie sie sich im Falle einer Cyberattacke am besten verhalten.

2.5 CHECKPOINT

CHECKPOINT

Überprüfen Sie den Lehrstoff mit Ihren Schüler/innen.
Diskutieren und reflektieren Sie anhand der folgenden Anregungen:

Welche Konsequenzen kann Cyberkriminalität für Betroffene haben

- ➔ *Finanzielle Konsequenzen*
- ➔ *Datendiebstahl*
- ➔ *Rufschädigung*
- ➔ *Juristische Konsequenzen*

Wie kann man sich vor Cyberattacken schützen?

- ➔ *Vorsichtiger Umgang mit Daten*
- ➔ *Software immer auf dem aktuellen Stand halten*
- ➔ *Komplexe Passwörter anlegen und geheim halten*
- ➔ *Keine vertraulichen Informationen im Netz teilen*
- ➔ *Skeptischer Umgang mit E-Mail Anhängen und neuen Bekannten im Netz*

3 DIGITALITÄT UND KRIMINALITÄT FÜR FORTGESCHRITTENE

3.1 INHALT

Diese Unterrichtseinheit vertieft das Thema Cyberkriminalität und sensibilisiert Ihre Schüler/innen dafür. Sie lernen, was sich hinter dem Begriff verbirgt, welche Akteure es gibt und welche Maßnahmen vor einer Cyberattacke ergriffen worden sein sollten. Abschließend setzen Sie sich damit auseinander, wie im Falle einer Cyberattacke zu agieren ist.

Dauer Offline:

45 Minuten

Im Anhang bieten wir Ihnen einen Zeitplan zur Strukturierung dieser Unterrichtseinheit.

3.2 LERNZIELE

1. *Verstehen, was Kriminalität im digitalen Kontext bedeutet.*
2. *Wissen, welche Schutzmaßnahmen getroffen werden können.*
3. *Reflektieren, wie verantwortungsbewusstes Verhalten im Netz aussieht.*

Zusätzlich zu diesem Unterrichtsvorschlag, finden Sie im Anhang eine Auflistung aller Unterrichtsmaterialien, welche von der Digitalen Lernwerkstatt zu diesem Thema zur Verfügung gestellt werden.

3.3 GRUNDLAGEN CYBERKRIMINALITÄT

3.3.1 Begriffsklärung

Cyberkriminalität ist inzwischen alltäglich: in Form von Phishing-Mails, dem Hacken von Facebook- und Instagram-Konten, oder gezielten Cyberattacken auf Unternehmen. Bevor wir uns vertiefter mit dem Thema **Cyberkriminalität** beschäftigen, muss zuerst einmal geklärt werden, was man darunter versteht.

DEFINITION CYBERKRIMINALITÄT

*Straftaten, bei denen die Täter moderne Informationstechnik nutzen, werden zunächst ganz allgemein als **Cyberkriminalität** (engl. cybercrime) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potentielle Opfer via E-Mail statt per Post erreicht.*

https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html

DIDAKTISCHER TIPP

Fragen Sie Ihre Schüler/innen, wer bereits persönlich oder im Bekanntenkreis Erfahrungen mit Internetkriminalität gemacht hat. Dazu zählen z.B. folgende Bereiche:

- *Phishing E-Mail bekommen*
- *Virus auf dem Computer*
- *Chat mit einer Person, welche vorgibt jemand anderes zu sein (Fake-Profil)*
- *Datendiebstahl*
- *Gehackte Social-Media-Accounts, z.B. Facebook- oder Instagramkonten*

Im Zusammenhang mit Cyberkriminalität ist immer wieder die Rede von „gehackt werden“ und „Hackern“. Aber wer oder was ist darunter zu verstehen?

DEFINITION HACKER

Hacker sind technisch versierte Personen im Hard- und Softwareumfeld. Sie finden Schwachstellen von Systemen, um auf sie aufmerksam zu machen oder sie für bestimmte Zwecke wie unbefugtes Eindringen oder zur Veränderung von Funktionen zu nutzen.

https://www.security-insider.de/was-ist-ein-hacker-a-596399/

3.3.2 Akteure und deren Motive

Nachdem Ihre Schüler/innen nun wissen, was unter Cyberkriminalität zu verstehen ist, soll es nun um die verschiedenen Akteure gehen. Diese haben unterschiedliche „Zielgruppen“ bzw. Opfer, gehen anders vor und werden von diversen Motiven angetrieben. In der folgenden Tabelle wird ein Überblick über die populärsten Akteure und deren Motive geboten.

	HACKTIVISTEN	**CYBERTERRORISMUS/ STAATLICHE SPIONAGE**	**ORGANISIERTE KRIMINALITÄT**
OPFER	Firmen, größere Systeme, Medien und Politik	Einzelpersonen, Firmen und Institutionen	Privatpersonen und Firmen
METHODE	Überwindung von Sicherheitssystemen, Protest und Propaganda	Erpressung und Ausspionieren von Daten und Informationen	Datenklau durch die bewusste Täuschung von anderen Personen
MOTIV	Politische/ ideologische Ziele oder Anerkennung in Hackerkreisen	Politische bzw. wirtschaftliche Ziele, wie z.B. der Gefährdung der öffentlichen Sicherheit	Geld

ARBEITSBLATT

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

Aber nicht nur die Akteure variieren, sondern auch die Art der Cyberattacke, kann sehr unterschiedlich ausfallen. Um das Wissen Ihrer Schüler/innen zu überprüfen, bearbeiten Sie dieses Arbeitsblatt mit Ihnen.

3.4 MASSNAHMEN FÜR UNTERNEHMEN

Ihre Schüler/innen haben bisher gelernt, was unter Cyberkriminalität zu verstehen ist, welche Akteure mit welcher Motivation agieren und welche Arten von Cyberattacken es gibt. Es soll nun darum gehen, welche Maßnahmen vorsorglich getroffen werden können und welches Handeln im Falle einer Cyberattacke richtig ist.

Um bei einer Cyberattacke schnell und richtig handeln zu können, sollten zwei Sachen vorab geklärt werden:

- **BUSINESS CONTINUITY:** Welchen Einfluss hat der Ausfall von bestimmten Systemen auf das Tagesgeschäft? Um bei einem Angriff weiterhin dem Kundengeschäft nachgehen zu können, sollten Unternehmen für sehr wichtige Systeme über den ganzen Globus verteilte Datencenter mit den exakt gleichen Daten haben. So stehen diese Daten im Notfall weiterhin zur Verfügung.
- **INCIDENT RESPONSE:** Welchen Plan verfolgen wir, wenn eine Cyberattacke stattfindet? Dafür sollte man z.B. erfahrene und vertrauenswürdige Experten einbinden, die das Unternehmen dabei unterstützen, die richtigen Maßnahmen zu finden. Damit die Experten schlimmeres verhindern und unverzüglich mit der Arbeit beginnen können, müssen ihnen die technischen und finanziellen Ressourcen unverzüglich zur Verfügung gestellt werden.

ONLINE TRAINING

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

Gerade für Unternehmen stellen Cyberattacken eine Gefahr dar. Dabei sind kleine und mittelständische Unternehmen genauso betroffen, wie die großen. Es ist also unabhängig von der Unternehmensgröße wichtig, Vorsorgemaßnahmen zu ergreifen, um sich vor potentiellen Cyberattacken zu schützen. In diesem kurzen online Quiz können Ihre Schüler/innen herausfinden, ob sie wissen, welche Schutzmaßen ein Unternehmen ergreifen sollte.

Wenn alle Schutzmaßnahmen versagt haben und es im Unternehmen doch zu einer Cyberattacke gekommen ist, gibt es einige Dinge zu beachten. Genaueres wird Peter Stinner, Cyber Defense Spezialst, im folgenden Video erklären.

VIDEO

Klicken Sie hier, oder besuchen Sie www.digitale-lernwerkstatt.com

DIDAKTISCHER TIPP – GRUPPENDISKUSSION

Diskutieren Sie mit Ihren Schüler/innen, wie verantwortungsbewusstes Verhalten im Netz aussieht, z.B.

- ➔ *Sichere Passwörter*
- ➔ *Keine persönlichen Daten preisgeben*
- ➔ *Freundschaftsanfragen in sozialen Netzwerken nur von Personen annehmen, die man auch im realen Leben kennt*
- ➔ *Keine E-Mail-Anhänge von unbekannten Absendern öffnen oder runterladen*

3.5 CHECKPOINT

CHECKPOINT

Ihre Schüler/innen sollten nun wissen, was unter Cyberkriminalität zu verstehen ist, welche Akteure es gibt und mithilfe welcher Maßnahmen Sie sich schützen können.

Um den Lehrstoff zu überprüfen, können Sie anhand folgender Anregungen mit Ihren Schüler/innen diskutieren und reflektieren:

Was versteht man unter Cyberkriminalität?
*Der Begriff **Cyberkriminalität** beschreibt kriminelle Aktivitäten, die mithilfe von digitalen Technologien ausgeführt werden.*

Welche Arten von Cyberattacken werden unterschieden?
- ➔ *Phishing-Mails zur Abfrage persönlicher Daten, wie z.B. Passwörtern*
- ➔ *Spam-Mails mit Viren, Trojanern oder Würmern*
- ➔ *Hoax-Mails, zum Teil mit verseuchten Anhängen*

Wie können sich Unternehmen schützen?
- ➔ *Umfassendes Sicherheitspaket*
- ➔ *Besonders sensible Bereiche identifizieren, um vermehrt schützen zu können*
- ➔ *Umfassende Sicherheitslösung inkl. Mobiltelefone*
- ➔ *Einhaltung aller Standards*
- ➔ *Schulung aller Mitarbeiter und Sensibilisierung für Online-Gefahren*
- ➔ *Sicherheitslösung mit Echtzeitüberwachung*

4 GLOSSAR

Cyberkriminalität	Straftaten, bei denen die Täter moderne Informationstechnik nutzen, werden zunächst ganz allgemein als Cyberkriminalität (engl. cybercrime) bezeichnet. Cyberkriminalität ist zum Beispiel ein Betrugsversuch, der das potentielle Opfer via E-Mail statt per Post erreicht.
Cybersecurity	Unter Cybersecurity versteht man diejenigen Maßnahmen, die ergriffen werden, um einen Computer oder ein Computersystem vor Hackerangriffen oder unbefugtem Zugriff zu schützen.
Datentracking	Tracking ist eine Basistechnologie des Netzes. Nahezu jeder Seitenaufruf wird von Werbedienstleistern mitgeschnitten und weiterverarbeitet. Aus diesen Informationen können individuelle Profile erstellt werden, die es ermöglichen, Nutzerinnen und Nutzern auf sie zugeschnittene Werbeangebote zu zeigen. Einige Anbieter werten auch die Inhalte von E-Mails aus und seit einiger Zeit auch die Nutzung von Smartphone-Apps. Hierbei spielt auch die Analyse des aktuellen Standorts eine zunehmend größere Rolle.
Hacker	Hacker sind technisch versierte Personen im Hard- und Softwareumfeld. Sie finden Schwachstellen von Systemen, um auf sie aufmerksam zu machen oder sie für bestimmte Zwecke wie unbefugtes Eindringen oder zur Veränderung von Funktionen zu nutzen.
Jailbreak	Unter Jailbreak versteht man den Zugriff auf das Betriebssystem (hier iOS), um dort grundlegende Veränderungen vornehmen zu können.
Rooting	Unter Rooting versteht man den Zugriff auf das Betriebssystem (Android), um dort grundlegende Veränderungen vornehmen zu können.

5 ANHANG

Anhang 1: Unterrichtsplan „Digitalität und Kriminalität für Einsteiger“

Anhang 2: Unterrichtsplan „Digitalität und Kriminalität für Fortgeschrittene“

Anhang 3: Medienliste

Anhang 4: „Cyberattacke – Ein Beispiel“ Arbeitsblatt

Anhang 5: „Was tust du? Quiz

Anhang 6: „Arten von Cyberattacken“ Arbeitsblatt

Digitalität und Kriminalität - Einsteiger

Lern-ziele

1. Wissen, was Cyberkriminalität bedeutet.
2. Verstehen, welche Folgen Cyberkriminalität haben kann.
3. Erkennen, wie man sich vor Angriffen schützen kann.

Dauer 45 Minuten

Zeit	Unterrichtsinhalt	Arbeits- und Sozialform	Format	Feinlernziele
5	Einführung ins Thema mit Sammlung von Erfahrungsberichten	Unterrichtsgespräch	Diskussion	Erkennen, wie gegenwärtig Cyberkriminalität ist.
8	Einführung zu Cybersecurity und Cyberkriminalität	Computergestütztes Lernen	Online Training	Wissen, was sich hinter den Begriffen Cybersecurity und Cyberkriminalität verbirgt.
4	Folgen von Cyberkriminalität	Videobasiertes Lernen	Video	Verstehen, welche Folgen Cyberkriminalität für den Einzelnen haben kann.
10	Arbeitsblatt zur Einschätzung von richtigem und falschem Verhalten bei der Abwehr von Cyberattacken	Einzelaufgabe	Arbeitsblatt	Reflektieren von sicherheitsbewusstem Verhalten im Netz.
8	Security im Alltag - Wie kannst du dich schützen?	Computergestütztes Lernen	Online Training	Erkennen, welche Möglichkeiten es gibt, sich besser vor Cyberangriffen zu schützen.
10	Abschluss mit Rückbezug auf eingangs geschilderte Erfahrungsberichte	Unterrichtsgespräch	Diskussion	Reflektieren, wie verantwortungsbewusster Umgang im Netz funktioniert.
45				

Digitalität und Kriminalität - Fortgeschrittene

Lern-ziele

1. Verstehen, was Kriminalität im digitalen Kontext bedeutet.
2. Erkennen, welche Schutzmaßnahmen getroffen werden können.
3. Reflektieren, wie verantwortungsbewusstes Verhalten im Netz aussieht.

Dauer 45 Minuten

Zeit	Unterrichtsinhalt	Arbeits- und Sozialform	Format	Feinlernziele
5	Begriffsklärung - Einleitung - digitale Kriminalität	Unterrichtsgespräch	Diskussion	Verstehen, was unter Kriminalität im digitalen Kontext zu verstehen ist.
3	Wer und welche Motive stecken hinter Cyberattacken?	Computerbasiertes Lernen	Online-Training	Wissen, wer die Akteure von Cyberkriminalität sind und welche Motive sie antreiben.
5	Arbeitsblatt: Arten Cyberattacke	Einzelaufgabe	Arbeitsblatt	Verstehen, welche verschiedenen Arten von Cyberattacken es gibt.
10	Was sollte vor einer Cyberattacke geklärt werden?	Unterrichtsgespräch	Diskussion	Wissen, welche Vorsichtsmaßnahmen getroffen werden sollten.
7	Was tun im Fall einer Cyberattacke?	Videobasiertes Lernen	Video	Erkennen, welche Maßnahmen im Falle einer Cyberattacke hilfreich und sinnvoll sind.
7	Wie können sich Unternehmen schützen?	Computerbasiertes Lernen	Online Training (Quiz)	Wissen, wie sich Unternehmen vor Cyberattacken schützen können.
8	Gruppendiskussion: Wie sieht verantwortungsbewusstes Verhalten aus?	Unterrichtsgespräch	Diskussion	Reflektieren, wie verantwortungsbewusstes Verhalten im Netz aussieht.
45				

MEDIENLISTE

Name	Beschreibung	Format
Was sind Fake-Profile?	Definition und Hintergrund von Fake-Profilen sowie Hinweise zum Selbstschutz.	Video
Quiz: Fake-Profile erkennen und sich schützen	Wissensabfrage zum Thema Fake-Profile und Selbstschutz vor unechten Profilen.	Online Training
Darknet, Download, Streaming: Was ist (il)legal?	Wissensabfrage zum Thema Fake-Profile und Selbstschutz vor unechten Profilen.	Online Training
Cyber Mobbing, Hate Speech & Trolling	Erklärung der Unterschiede zwischen Download und Streaming, sowie ein Exkurs zum Thema Darknet.	Online Training
Was ist Cyber Kriminalität - Definition	Spiel mit dem Ziel das Thema Cyber Kriminalität kennenzulernen.	Online Training
Advanced: Cyber Security im Unternehmen	Überblick über die Sicherheitsmaßnahmen, die Unternehmen ergreifen, um sich vor Cyber Kriminalität zu schützen.	Online Training
Warum Cyber Kriminalität? Was ist Cyber Kriminalität - Beispiele	Erkennen von Hintergründen und Motiven von Cyberkriminalität.	Online Training
Advanced: Was können Unternehmen in einem Fall eines Cyber-Attacks machen?	Peter Stinner gibt einen Überblick über Handlungsmöglichkeiten von Unternehmen im Falle eines Hacker Angriffs.	Video
Folgen von Cyberkriminalität	Methoden und Motive der Hacker sowie Tipps zum Schutz der eigenen Daten im Netz.	Video
Wie wird Cyber Kriminalität durchgeführt?	Erklärung wichtiger Begriffe, wie zum Beispiel Social Engineering, Spam und Hardware Keylogger.	360° Video
Cyber Security im Alltag	Tipps, wie man sich im Alltag vor Cyber Kriminalität schützen kann.	Online-Training
Cyberattacke – Ein Beispiel		Arbeitsblatt für das Themenheft entwickelt. Nach Abnahme ins Curriculum sowie den DLW Katalog aufnehmen und verlinken
Was tust du?		Arbeitsblatt für das Themenheft entwickelt. Nach Abnahme ins Curriculum sowie den DLW Katalog aufnehmen und verlinken
Arten von Cyberattacken		Arbeitsblatt für das Themenheft entwickelt. Nach Abnahme ins Curriculum sowie den DLW Katalog aufnehmen und verlinken
Risiken: Tools zur Datensicherheit im Netz	Vorstellung hilfreicher Instrumente zur Erhöhung der Datensicherheit.	PowerPoint
Cybersicherheit	Überblick über das Thema Cyberkriminalität sowie Vorstellung präventiver Maßnahmen.	PowerPoint
Mein sicheres Passwort	Anleitung zur Erstellung von sicheren Passwörtern und deren Aufbewahrung	PowerPoint
Gruppenarbeit zu Cyberkriminalität	Heranführung an das Thema Cyberkriminalität mit integrierter Gruppenarbeit zur Verbesserung von Cybersecurity.	PowerPoint

CYBERATTACKE

EIN BEISPIEL

Digitale Lernwerkstatt

Max ist bislang recht sorglos mit seinen persönlichen Informationen umgegangen. Er kann sich seine Passwörter nur schwer merken und hat daher ein Passwort für alle Plattformen die er nutzt. Auf seinem Tablet hat er die Passwörter für die sozialen Netzwerke und sein E-Mailpasswort sogar gespeichert. Das ist ganz praktisch – so muss er einfach nur die Seite aufrufen und ist direkt eingeloggt.

Momentan hat er jedoch ein Problem. Er bekommt viele Nachrichten von Freunden und Bekannten mit der immer gleichen Frage: „Warum schickst du mir so seltsame Videos?“ Dabei hat Max doch gar nichts verschickt!?

Kann es sein, dass Max Opfer eines Hackers geworden ist?

Aufgabe 1:

Welche Schwachstellen im Umgang mit Daten findest du bei Max?

Aufgabe 2:

Wie sollte Max vorgehen, um sich in Zukunft zu schützen?

CYBERATTACKE

EIN BEISPIEL – MUSTERLÖSUNG

Digitale Lernwerkstatt

Max ist bislang recht sorglos mit seinen persönlichen Informationen umgegangen. Er kann sich seine Passwörter nur schwer merken und hat daher ein Passwort für alle Plattformen die er nutzt. Auf seinem Tablet hat er die Passwörter für die sozialen Netzwerke und sein E-Mailpasswort sogar gespeichert. Das ist ganz praktisch – so muss er einfach nur die Seite aufrufen und ist direkt eingeloggt.

Und da ist ja auch schon wieder eine neue Nachricht in seinem Lieblings-Netzwerk. Jemand bittet ihn um Hilfe bei der Suche nach einer vermissten Person. Zwar kennt Max den Absender nicht, aber helfen möchte er natürlich trotzdem und klickt auf den Link, der in der Nachricht angegeben ist.

Wenige Tage später ist Max ratlos: Er bekommt viele Nachrichten von Freunden und Bekannten mit der immer gleichen Frage: „Warum schickst du mir so seltsame Videos?“ Dabei hat Max doch gar nichts verschickt!?

Kann es sein, dass Max Opfer eines Hackers geworden ist?

Aufgabe 1:

Welche Schwachstellen im Umgang mit Daten findest du bei Max?

- Ein Passwort für alle Plattformen
- Passwort auf Website gespeichert
- Auf Link in einer Nachricht von einem unbekannten Absender geklickt

Aufgabe 2:

Wie sollte Max vorgehen, um sich in Zukunft zu schützen?

- Passwörter komplexer anlegen
- Skeptischer im Umgang mit Nachrichten von unbekannten Absendern sein

WAS TUST DU?

QUIZ

Digitale Lernwerkstatt

Cyberattacken können jeden treffen. Doch manchmal bekommen wir eine scheinbar ganz harmlose E-Mail und werden durch einen Klick zum Opfer. Versuche in den folgenden Situationen zu entscheiden, wie du dich am besten verhältst, um Angriffen zu entgehen.

Situation 1 – Gewinnspiel
Du bekommst eine E-Mail mit einer Gewinnbenachrichtigung: „Herzlichen Glückwunsch zum neuen Smartphone!“ Zwar kannst du dich nicht an deine Teilnahme erinnern, aber ein neues Handy wünschst du dir schon lange.
Was tust du?

- ☐ Ich folge dem Link in der E-Mail. So eine Gelegenheit lasse ich mir nicht entgehen!
- ☐ Da bin ich lieber vorsichtig. Wer weiß, was sich hinter dem Link verbirgt?

Situation 2 – Social Media
Du erhältst eine Freundschaftsanfrage über ein soziales Netzwerk von einer dir fremden Person. Dazu bekommst du eine nette Nachricht mit einem Video, das du dir unbedingt ansehen sollst.
Was tust du?

- ☐ Spannend! Das sehe ich mir direkt an. Und neue Kontakte sind doch auch super.
- ☐ Ich bleibe skeptisch. Da ich die Person nicht kenne, prüfe ich erst, wer sich dahinter verbirgt.

Situation 3 – App
Du prüfst die neuen Abfahrtszeiten deines Schulbusses auf der Website des Anbieters. Dabei siehst du, dass es dort jetzt auch eine App für das Smartphone gibt. Wie praktisch!
Was tust du?

- ☐ Mit einem Download mache ich mich nur angreifbar. Ich nutze weiterhin die Website.
- ☐ Die App stammt vom Eigentümer der Website, daher kann ich sie problemlos runterladen.

Situation 4 – Software
Du hast im Netz ein Programm gefunden, dass dir den kostenlosen und einfachen Download aktueller Musik verspricht. Die Website kennst du zwar nicht, aber das Angebot ist verlockend.
Was tust du?

- ☐ Kostenlose Musikdownloads sind vermutlich illegal. Wer weiß, was sich hinter dem Programm in Wahrheit verbirgt. Ich lade es lieber nicht herunter.
- ☐ Klingt toll! Nach sowas habe ich schon länger gesucht. Ich schaue mich noch kurz auf der Website um und lade es dann herunter.

Situation 5 – E-Mail
Ein Freund hat dir eine E-Mail geschickt. Die E-Mail beinhaltet die neuste Version eures Referats für nächste Woche.
Was tust du?

- ☐ Bei E-Mail Anhängen sollte man grundsätzlich vorsichtig sein. Ich rufe ihn lieber an.
- ☐ Wir haben besprochen, dass er mir das Referat per Mail schickt. Ich öffne also den Anhang.

WAS TUST DU?

QUIZ – MUSTERLÖSUNG

Digitale Lernwerkstatt

Cyberattacken können jeden treffen. Doch manchmal bekommen wir eine scheinbar ganz harmlose E-Mail und werden durch einen Klick zum Opfer. Versuche in den folgenden Situationen zu entscheiden, wie du dich am besten verhältst, um Angriffen zu entgehen.

Situation 1 – Gewinnspiel
Du bekommst eine E-Mail mit einer Gewinnbenachrichtigung: „Herzlichen Glückwunsch zum neuen Smartphone!“ Zwar kannst du dich nicht an deine Teilnahme erinnern, aber ein neues Handy wünschst du dir schon lange.
Was tust du?

- ☐ Ich folge dem Link in der E-Mail. So eine Gelegenheit lasse ich mir nicht entgehen!
- ☑ Da bin ich lieber vorsichtig. Wer weiß, was sich hinter dem Link verbirgt?

Situation 2 – Social Media
Du erhältst eine Freundschaftsanfrage über ein soziales Netzwerk von einer dir fremden Person. Dazu bekommst du eine nette Nachricht mit einem Video, das du dir unbedingt ansehen sollst.
Was tust du?

- ☐ Spannend! Das sehe ich mir direkt an. Und neue Kontakte sind doch auch super.
- ☑ Ich bleibe skeptisch. Da ich die Person nicht kenne, prüfe ich erst, wer sich dahinter verbirgt.

Situation 3 – App
Du prüfst die neuen Abfahrtszeiten deines Schulbusses auf der Website des Anbieters. Dabei siehst du, dass es dort jetzt auch eine App für das Smartphone gibt. Wie praktisch!
Was tust du?

- ☐ Mit einem Download mache ich mich nur angreifbar. Ich nutze weiterhin die Website.
- ☑ Die App stammt vom Eigentümer der Website, daher kann ich sie problemlos runterladen.

Situation 4 – Software
Du hast im Netz ein Programm gefunden, dass dir den kostenlosen und einfachen Download aktueller Musik verspricht. Die Website kennst du zwar nicht, aber das Angebot ist verlockend.
Was tust du?

- ☑ Kostenlose Musikdownloads sind vermutlich illegal. Wer weiß, was sich hinter dem Programm in Wahrheit verbirgt. Ich lade es lieber nicht herunter.
- ☐ Klingt toll! Nach sowas habe ich schon länger gesucht. Ich schaue mich noch kurz auf der Website um und lade es dann herunter.

Situation 5 – E-Mail
Ein Freund hat dir eine E-Mail geschickt. Die E-Mail beinhaltet die neuste Version eures Referats für nächste Woche.
Was tust du?

- ☐ Bei E-Mail Anhängen sollte man grundsätzlich vorsichtig sein. Ich rufe ihn lieber an.
- ☑ Wir haben besprochen, dass er mir das Referat per Mail schickt. Ich öffne also den Anhang.

ARTEN VON CYBERATTACKEN

ARBEITSBLATT

Digitale Lernwerkstatt

Von Cyberattacken oder -angriffen hört man immer wieder. Weißt du auch, was sich hinter den verschiedenen Arten verbirgt?

Was ist eine Phishing-Mail?

Was sind Spam-Mails und welche Probleme verbergen sich dahinter?

Was ist ein Hoax?

ARTEN VON CYBERATTACKEN

ARBEITSBLATT – MUSTERLÖSUNG

Von Cyberattacken oder -angriffen hört man immer wieder. Weißt du auch, was sich hinter den verschiedenen Arten verbirgt?

Was ist eine Phishing-Mail?

Phishing-Mails sind eine Form von Spam-Mails, die zum Ziel haben, dem Empfänger private Daten, wie z.B. Passwörter oder Kontoinformationen zu entlocken.

Was sind Spam-Mails und welche Probleme verbergen sich dahinter?

Spam ist ein Überbegriff für jegliche Form unerwünschter E-Mails. Diese lassen sich je nach Inhalt in verschiedene Begreife gliedern:

- *Hoax: Ein Schwindel oder schlechter Scherz; häufig mit „verseuchtem“ Anhang*
- *Phising: Versucht, private Daten zu entlocken*
- *Scam: Verspricht, dass Empfänger schnell und mit einfachen Mitteln reich wird. Häufig muss vorab Geld überwiesen werden, was der ganze Sinn „des Scams“*

Was ist ein Hoax?

- *Schlechter Scherz oder Falschmeldung*
- *Z.B. falsche Warnungen vor bösartigen Computerprogrammen, Petitionen, Geheimtipps zum schnellen Geld verdienen*