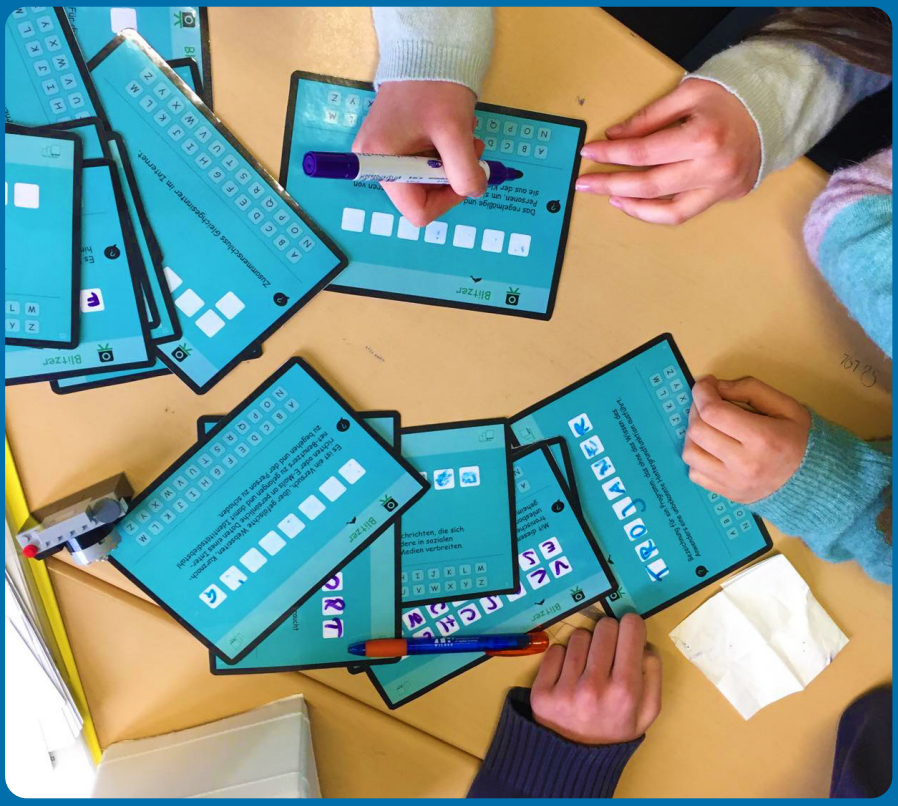


SecAware4school - Spielbasierte Sensibilisierung zum Thema Informationssicherheit im Schulunterricht

Im Projekt SecAware4school wurden insgesamt 36 analoge und digitale spielbasierte Lernszenarien in drei Schwierigkeitsgraden entwickelt und mit Pilotschulen erprobt. In Kreativworkshops wurden Ideen für Lernszenarien entwickelt, die zu verschiedenen Bereichen der Informationssicherheit sensibilisieren und im Schulunterricht eingesetzt werden.

Spielbasierte Lernszenarien

Erlebnisorientierte und interaktive Methoden wurden bei der Entwicklung der analogen und digitalen Lernszenarien eingesetzt.

Schülerinnen und Schülern sowie deren Bezugspersonen, den Lehrenden und Eltern, ist es möglich, sich spielerisch über Themen wie Verhalten in sozialen Netzwerken, Internet, Mobbing, Umgang mit Passwörtern, Bildrechten und Fake News zu sensibilisieren.

In ihrer Gesamtheit vermitteln die Lernszenarien den achtsamen und sicheren Umgang mit sensiblen Informationen und persönlichen Daten.

Drei Schwierigkeitsniveaus

Am Projekt waren Klassenstufen zwischen der 6. und 11. involviert. Um die Lernszenarien für alle Beteiligten gleichermaßen interessant zu gestalten, wurden 3 Schwierigkeitsgrade festgelegt: Der erste und somit leichteste Schwierigkeitsgrad eignet sich für die Klassenstufen 6 bis 7, der mittlere für die 8. und 9. Klassenstufen und der höchste Schwierigkeitsgrad ist den Klassenstufen 10 und 11 zuzuordnen.

Durch die Anpassung der Lernszenarien in jeweils drei Schwierigkeitsgrade wird neuer Input an den vorhandenen Wissensstand der Beteiligten angeknüpft.

Verhalten in sozialen Netzwerken

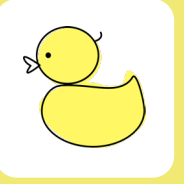
An dieser Lernstation geht es darum, Lösungen und Ansprechpartner in verschiedenen Situationen zu finden und sich einen adäquaten und freundlichen Umgang in sozialen Netzwerken anzueignen.

Fake or real?

Fake News ist der moderne Ausdruck für eine Information, die von allgemein bekannten Tatsachen ablenken und diese im Extremfall verfälschen soll. An diesem Lernszenario soll die Wahrnehmung für richtige oder falsche Nachrichten sensibilisiert werden.

Fake News

Das Ziel des Lernszenarios ist das Finden und Herstellen der Zusammenhänge zwischen den Fake News-Fällen, die ein konkretes Ereignis beschreiben. In Gruppendiskussionen muss eine Übereinstimmung gefunden werden, die die logische Zusammengehörigkeit von angewandtem Werkzeug, den Begriffen und der Strategie zum betrachteten Fall sinnvoll erscheinen lässt.



Storytelling

Das Lernszenario „Storytelling“ fördert gleichzeitig Kreativität und die Verknüpfung erlernter Begriffe, indem eine kurze Geschichte zu einem bestimmten Thema der Informationssicherheit erfunden und die gewürfelten Symbole darin eingebaut werden sollen.

Security Sketch

In der Rolle einer/s Büromitarbeitenden sollen die richtigen Entscheidungen in Bezug auf die Passwortsicherheit getroffen werden. Beispielsweise soll entschieden werden, wie mit einem neu erhaltenen Passwort umgegangen werden soll und ob/ wo dieses notiert wird. Dieses digitale Lernszenario dient dazu, für den richtigen Umgang mit Passwörtern zu sensibilisieren. Neben der deutschen Version wurde dieses Lernszenario auch in englischer Sprache umgesetzt, um der Internationalisierung an den Schulen gerecht zu werden.

Bildrechte

Dieses digitale Lernszenario hilft bei der Auseinandersetzung rund mit dem Thema Bildrechte. Der allgemein sorglose Umgang mit Multimediainhalten wirft zahlreiche Fragen auf. Ein Leitfaden für das rechtskonforme Verhalten sensibilisiert die Teilnehmenden.

Hacker Terminal

In diesem digitalen Lernszenario werden grundlegende Begriffe der Informationssicherheit wiederholt und vertieft. In der Rolle der Retro-Hacker sollen anhand von Hinweisen „verschlüsselte“ Kennwörter erraten werden, um an Zugänge und ins System zu gelangen.

Datenspionage

Das digitale Lernszenario dient der Bewusstmachung möglicher Sicherheitsobjekte am Arbeitsplatz, die einer besonderen Aufbewahrung bedürfen. Objekte mit sensiblen Informationen sollen erkannt und auf sichere Weise am Arbeitsplatz aufbewahrt werden.

Security Surfer

In diesem analogen Lernszenario wird das globale Thema Internet aufgegriffen und die Möglichkeiten, die das Internet bietet, näher beleuchtet. Beim Surfen im weiten Meer des Internets sollen die Gefahren erkannt und die passenden Schutzmaßnahmen gefunden werden.

Schnelles Begrifferaten

Dieses Lernszenario trainiert den sicheren Gebrauch von Fachbegriffen im Bereich der Informationssicherheit. Aufgrund der zunehmenden Menge an online verfügbaren Informationen und Diensten ist es von Bedeutung, sich mit Fachbegriffen der Informationssicherheit vertraut zu machen.

Zur Benutzung der spielbasierten Lernszenarien im Unterricht finden Sie eine Anleitung zum Selbsterstellen der Lernszenarien auf der Website des Projektes:
https://secaware4school.wildau.biz

Digital sozial

Bei diesem analogen Lernszenario geht es um das Verhalten im und mit dem Internet sowie den Umgang mit dem Smartphone in der eigenen Umwelt. Es soll zur Diskussion bezüglich des Verhaltens gegenüber anderen Personen anregen und für den kritischen Umgang mit den „neuen“ Medien sensibilisieren.

Security Duell

Dieses Lernszenario bietet die Möglichkeit, potenzielle Angriffspunkte in einem Unternehmen zu erkennen und passende Schutzmaßnahmen zu fnden.

Veranstaltungsblock im Projekt

1. Informationsveranstaltungen
2. Awareness Trainings
3. Kreativworkshops
4. Ausbildung zur/zum Sicherheitsbeauftragten

Materialien und mehr Informationen unter
https://secaware4school.wildau.biz

Das Forschungsprojekt SecAware4school ist ein Projekt unter partizipatorischer Beteiligung von fünf Pilotschulen aus Berlin und Brandenburg. Es wurde an der Technischen Hochschule Wildau mit dem folgenden Forschungsteam von Frau Prof. Dr. Margit Scholl durchgeführt: Regina Schuktomow (operative Projektleitung), Peter Koppatz (technische Leitung), Denis Edich, Stefanie Gube und Josephine Gerlach. Wir danken zudem Peter Ehrlich als Labor-Ingenieur für wichtige Impulse und Clara Paetow als zeitweilige studentische Mitarbeiterin. Wir danken vor allem der Horst Görtz Stiftung (HGS) für die Förderung.

Kontakt
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

Prof. Dr. Margit Scholl (Hrsg.)
margit.scholl@th-wildau.de

Projektlaufzeit: 01.09.2018 – 31.12.2020
Das Projekt „Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)“ wird aus Mitteln der Horst Görtz Stiftung gefördert.

ISBN: 978-3-9819225-1-6

SecAware 4school

GEFÖRDERT VON HGS Horst Görtz Stiftung

Technische Hochschule Wildau Technical University of Applied Sciences WILDAU