DATEN-KLAU
DIE NEUGIERIGEN DATENSAMMLER

Viele Heranwachsende nutzen mobile Medien wir Smartphones oder Tablets ganz alltäglich, zum Lernen, zur Kommunikation, zum Spielen, zum Fotografieren. Die Geräte sind mobile Alleskönner und sie speichern nicht nur Kontaktdaten, Fotos, persönliche Nachrichten sondern geben auch Informationen über die Nutzungsweisen an z.B. Appanbieter weiter. Hier gilt es kritisch und wachsam zu sein und bewusst zu überlegen, welche Daten preisgegeben werden sollen und welche nicht..

Dieser Baustein passt sehr gut als Ergänzung zum Baustein 5 "Datencheck"

Gruppengröße: 3 bis 30 Schüler/innen

Dauer: 30 min

Material: Karten „Daten-Karten", verdunkelte Schwimmbrille oder Tuch zum Augen verdecken

HINTERGRUND

Viele Schülerinnen und Schüler (SuS) denken, dass die Nutzung kostenloser Apps auch wirklich „kostenlos" sei. Tatsächlich kosten die Apps kein Geld, dafür wollen die Firmen, wie Google (Playstore) oder Apple (App Store), aber die Daten der Nutzenden nach dem Motto: „Du nutzt unsere kostenlose App, dafür erhalten wir Deine Daten". Für Kinder ist es nicht ganz leicht zu verstehen wieso Internet und App-Anbieter so ein großes Interesse daran haben, alles zu sammeln, was die Menschen am Computer oder am Handy machen, was sie speichern, Welche Spiele sie nutzen, wo sie gerade sind (Standort), welche Musik gerne gehört wird.. Manches Mal benötigt natürlich eine App eine bestimmte Erlaubnis (Berechtigung) damit sie richtig funktioniert, doch mache App ist so neugierig und will auch Informationen haben, die völlig unwichtig sind für den ganzen Funktionsumfang. Spielerisch sollen die Kinder erfahren, wie Big-Data-Technologien funktionieren und wieso Datenschutz und die Auswahl der richtigen App wichtig ist. Natürlich „stehlen" die Firmen die Daten nicht sondern geben durchaus beim Download bekannt, welche Berechtigungen sie haben wollen, doch ist das Spiel für die SuS eine gute Erfahrung, wie unangenehme es sein kann, wenn private oder geheime Daten „einfach so" von anderen weggenommen werden.

Link- und Lesetipp: Persönliche Daten im Internet schützen. SCHAU HIN!-Tipps im Überblick: https://www.schau-hin.info/extrathemen/datenschutz.html

Linktipp*:* www.internet-abc.de/lm/luegner-und-betrueger-im-internet.html *https://www.internet-abc.de/lm/luegner-und-betrueger-im-internet/die-abzocker-apps-abos-onlinespiele-2.html*

VORBEREITUNG

Drucken und schneiden Sie die Vorlage „Daten-Karten“ (siehe Baustein 5 „Datencheck“) aus. Stellen Sie einen Stuhlhalbkreis auf, am offenen Ende steht ein Stuhl, vor diesem Stuhl liegen in Reichweite von 2 Metern die Datenkarten auf dem Fußboden aus.

DURCHFÜHRUNG

Alle Schüler/innen (SuS) sitzen im Stuhlhalbkreis. Die Lehrkraft erläutert kurz die Spielregeln bzw. die Szenerie und den Spielverlauf (s. Infokasten rechts).

Ein Kind setzt sich freiwillig auf dem Einzelstuhl, vor dem die Datenkarten, auf einer ca. 2 qm großen Fläche, ausliegen. Der Platz stellt den heimischen Computer/das eigene Smartphone/ Tablet dar, mit allen Daten (vom Foto über Notizen, bis hin zu Passwörtern). Der/die SuS sitzt Zuhause uns surft im Netz. Die eigenen Daten hat er/sie mehr oder weniger gut oder gar nicht geschützt. Manches Mal sind kluge oder eben nachlässige Privacy-Einstellungen zu sehen oder es werden neugierige Apps genutzt.

All das ist nicht sichtbar und wird (hin und wieder) von der Lehrkraft inszeniert: *„Wir sehen hier Fotos vom Geburtstag, ob die gut geschützt sind? Die Taschengeldhöhe, oho, die interessiert bestimmt die Bank, die Dir ein Konto andrehen wollen. Und da, die Kleidergröße, das interessiert bestimmt den schicken Klamottenladen.“* Die SuS im Stuhlhalbkreis stellen eben diese „Firmen“ dar (von bekannten Hamburger-Restaurants über Banken, Sportfirmen, Klamottenläden, Spielzeugfirmen usw.), vereinzelt können auch „Privatpersonen“ im Kreis sitzen. Allen ist gemein, dass sie an die Daten des einen/der einen SuS heranwollen.

Im Internet oder auf dem Smartphone wird nicht immer bemerkt, wenn Daten „abgegriffen“ werden. Um die Situation daran anzupassen, werden dem/der „surfenden Schüler/-in“ die Augen mit einem Tuch oder einer verdunkelten Schwimmbrille verdeckt. Ab dem Zeitpunkt muss der/die Spielerin sich auf ihren Hörsinn verlassen, mit deren Hilfe die „Angreifer/innen“ abwehrt werden können.

Sind die Augen abgedeckt und ist sichergestellt, dass der/die SuS wirklich nicht sehen kann, deutet die Lehrkraft mit dem Finger zuerst auf eine/n Firmen-SuS im Halbkreis und zeigt dann auf die Datenkarte, die abgegriffen werden soll. Mit dem Hinweis: *„Der Angriff auf „ein Foto Deiner Eltern erfolgt!“* schleicht der/die „Firmen-SuS los und versucht unbemerkt die Karte zu ergattern. Deutet nun der/die Surfer/-in genau in die Richtung des Angriffs, muss sich die Firma zurückziehen. Dieser Rückzug muss verstanden werden, als gut genutze „Privatspähren-Einstellung“ und als gut eingestellte „App-Berechtigung“. Manches Mal hilft vielleicht auch eine gute Firewall oder ein tolles Antivirenprogramm.

Nach 4-5 Angriffen wird getauscht, dann darf sich ein/e andere/r Spieler/in verteidigen. Vorher wird aber erst besprochen, welcher „Datenklau“ besonders unangenehm ist.

SPIELREGELN

Die SuS die im Stuhlkreis sitzen übernehmen die Rolle von Firmen (Angreifer/-innen) die versuchen, unbemerkt die Datenkarten abzugreifen.

Auf dem Einzelplatz sitzt „der/die Surfer/-in“ und versucht der/die SuS seine Daten zu schützen, in dem bei einem bemerkten Angriff ein Handzeichen gegeben wird,

Die Spielleitung (Lehrkraft) erteilt den Firmen wortlos ein Angriffsziel und gibt dann Auskunft über den Erfolg oder Misserfolg der Mission.

ABSCHLUSS

Die SuS lieben es, wenn die Lehrkraft sich ebenfalls als Surfer/-in, den Angriffen der neugierigen Datensammler aussetzt. Hier wäre es gut, wenn eine zweite Lehrkraft moderiert. Am Ende können Sie auch den Server abstürzen lassen. Dann liegen bedauerlicherweise alle Daten frei, also ungeschützt im Netz und können von allen eingesammelt werden.
Besprechen Sie, wie sich das für die „bestohlene“ Lehrkraft anfühlt. „Es ist, als wäre in mein Haus eingebrochen worden, nur noch schlimmer“.
Besprechen Sie auch, welche Maßnahmen ergriffen werden müssen, wenn z.B, die Emailadresse oder das Passwort gestohlen wurde, müssen neue Adressen und Passwörter eingerichtet werden!

Die Kinder sollen verstehen: Jeder Mensch hat ein Recht auf Datenschutz und daher müssen die Anbieter von Apps einfach verständlich darlegen, was die App auf dem Smartphone „tut“. Zudem ist es wichtig, das die SuS selbst handeln und „neugierige“ Apps vom Handy (von den Eltern) löschen (lassen) oder erst gar nicht installieren.

VERTIEFUNG

Schließen Sie ein Smartphone oder Tablet an den Beamer und schauen Sie sich die App-Berechtigungen einzelner Apps an. Alternativ können die SuS eigene Smartphones mitbringen, um die Berechtigungen praktisch zu überprüfen. Bei diesem Einblick erkennen sie den wahren Preis des „Tauschgeschäftes“. So greift z.B. die Spiele-App „Angry Birds“ die Standortdaten ab. Für den Spielverlauf sind diese Daten allerdings gar nicht notwendig. Was genau mit den Daten passiert, geben die Firmen nur selten preis.

Filmclip: Apps – Neugierige Datensammler (2:16 Minuten) der Verbraucherzentrale Bundesverband. Veröffentlicht am 12.03.2014**.** Apps gehören für viele Smartphone-Nutzer/-innen einfach dazu. Die digitalen Helfer sind oft praktisch, aber auch sehr wissbegierig. Was das Datensammeln der App-Anbieter für jede/n Einzelne/n bedeutet und was sich ändern muss. https://www.youtube.com/watch?v=8YhxxrtOXCU

Filmclip: „Was sind eigentlich App- Berechtigungen?“
https://www.handysektor.de/mediathek/videos/erklaervideo-app-berechtigungen.html
"Was sind eigentlich App-Berechtigungen?". Das fragt sich auch Tom, der Apps total klasse findet und sehr viele auf seinem Smartphone installiert hat. Im Erklärvideo erklären wird gezeigt, was App-Berechtigungen sind, warum diese so wichtig sind und welche Berechtigungen die weit verbreitete App WhatsApp verlangt.