DATEN-KLAU-SPIEL
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 uvm., sondern geben auch Informationen über die Nutzungsweisen z.B. an 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 Verbinden der Augen

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), Apple (App Store) oder Facebook viele Daten der Nutzenden (Standort, Fotos, Kontakte etc.) nach dem Motto: „Du nutzt unsere App kostenlos, dafür erhalten wir Deine Daten". Firmen setzen auf den „Rohstoff Daten", weil er es ihnen z.B. ermöglicht, die Wünsche der Kundschaft noch exakter zu analysieren und so passgenauere Produkte und Werbestrategien zu entwickeln. In einer vernetzten Welt ist es nicht einfach, die Kontrolle über die eigenen Daten zu behalten. Die Haltung „Wieso? Ich habe doch nichts zu verbergen!" greift dennoch zu kurz und lässt völlig außer Acht, dass Daten, die erfasst werden, natürlich auch immer missbraucht oder gehackt werden können – auch die von Kindern, die diese Gefahren noch überhaupt nicht abschätzen können. Deshalb ist es wichtig, eine kompetente, kritische Haltung zu entwickeln, ein Bewusstsein über den Wert von Daten und die Problematik der Sammlung und Weiterverwertung! Spielerisch sollen die Kinder erfahren, wieso Datenschutz und die Auswahl der richtigen App wichtig ist.

VORBEREITUNG

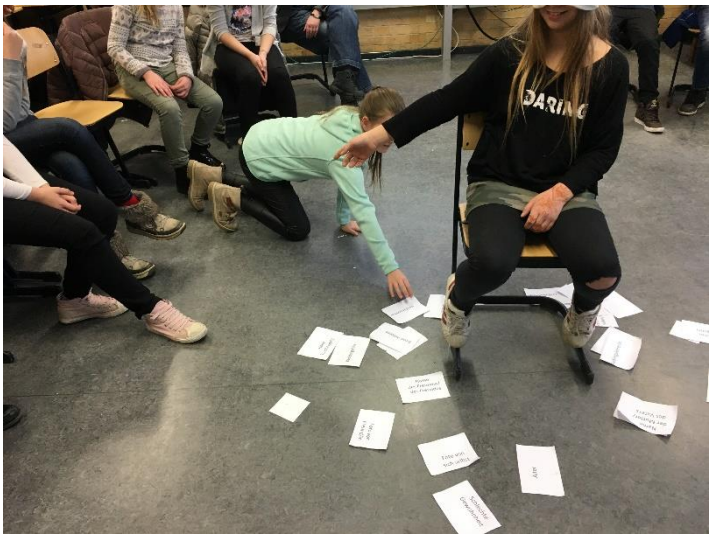
Drucken und schneiden Sie die Vorlage „Daten-Karten" aus Baustein 5 „Datencheck" aus. Stellen Sie einen Stuhlhalbkreis auf, am offenen Ende steht ein einzelner Stuhl, vor diesem Stuhl liegen in Reichweite von 1-2 Metern die Daten-Karten auf dem Fußboden aus.

DURCHFÜHRUNG

Alle (SuS) sitzen im Stuhlhalbkreis. Die Lehrkraft erläutert kurz die Spielregeln bzw. die Szenerie und den Spielverlauf (s. Infokasten nächste Seite oben rechts).

Ein Kind nimmt auf dem Einzelstuhl Platz. Vor seinem Stuhl liegen die Daten-Karten aus. Der Platz symbolisiert den heimischen Computer bzw. das eigene Smartphone/Tablet, mit allen Daten (Fotos, Notizen, Passwörter etc.). Diese eigenen Daten sind bei den meisten mehr oder weniger gut oder gar nicht geschützt. Manches Mal sind kluge oder eben nachlässige Privacy-Einstellungen zu sehen oder es werden kostenlose und entsprechend „neugierige“ Apps genutzt.

All das ist nicht sichtbar und wird (hin und wieder) von der Lehrkraft kommentiert: *„Wir sehen hier Fotos vom Geburtstag, ob die gut geschützt sind? Die Taschengeldhöhe, oho, die interessiert bestimmt die Bank, die Dir ein Konto anbieten wollen. Da ein Foto Deines Lieblingsessens, das ist spannend für den Essens-Lieferdienst. Und da, die Kleidergröße, das interessiert bestimmt den schicken Klamottenladen.“*



SPIELREGELN

*Die SuS, die im Stuhlkreis sitzen, überlegen, welche **„Firma“** (Schnellrestaurant, Bank, Sportfirma, Klamottenladen, Spielzeugfirma usw.) sie sind und sollen im Spielverlauf versuchen, unbemerkt Daten (also die Daten-Karten) abzugreifen.*

*Auf dem Einzelplatz sitzt ein Kind als **„Surfer/-in“** und versucht, seine Daten zu schützen, in dem es bei einem bemerkten Angriff in die Richtung zeigt, aus der es den Angriff vermutet. Seine Augen sind verbunden, so dass der Daten-Klau nicht gesehen sondern nur gehört werden kann.*

*Die **Spielleitung** (Lehrkraft) erteilt einer „Firma“ wortlos einen **Angriffsauftrag**, damit unklar ist, aus welcher Richtung dieser Angriff erfolgt. Und nennt dann hörbar das Ziel des Auftrags, z.B.: „Es erfolgt ein Angriff auf deine Kontaktdaten.“*

Die beauftragte „Firma“ schleicht sich an und versucht, die Daten-Karten möglichst unbemerkt / ungehört in ihren Besitz zu bringen.

*Kann der / die „Surfer/-in“ den Angriff nicht hören, war der **Daten-Klau** erfolgreich. Andernfalls zeigt es in die Richtung, aus der es den Angriff vermutet.*

Die SuS im Stuhlhalbkreis stellen eben diese „Firmen“ dar (von bekannten Schnellrestaurants über Banken, Sportfirmen, Klamottenläden, Spielzeugfirmen usw.), vereinzelt können auch „Privatpersonen“ im Kreis sitzen. Allen ist gemein, dass sie an die Daten heranwollen.

Im Internet oder auf dem Smartphone wird nicht immer bemerkt, wenn Daten „abgegriffen“ werden. Um die Situation daran anzupassen, werden dem Kind auf dem Einzelstuhl die Augen mit einem Tuch oder einer verdunkelten Schwimmbrille verdeckt. Ab dem Zeitpunkt muss das Kind sich auf seinen Hörsinn verlassen, mit dessen Hilfe die „Angreifer/-innen“ bemerkt und so abgewehrt werden können.

Sind die Augen abgedeckt und ist sichergestellt, dass das Kind wirklich nicht sehen kann, deutet die Lehrkraft wortlos zuerst auf ein Kind im großen Stuhlkreis und zeigt dann auf die Daten-Karte, die abgegriffen werden soll. Mit dem Hinweis *„Ein Angriff auf ein Foto Deiner Eltern erfolgt!“* schleicht die „Firma“ los und versucht, unbemerkt die Karte zu ergattern.

Deutet nun das Kind auf dem Einzelplatz genau in die Richtung, aus der der Angriff kommt, muss sich die Firma zurückziehen. Dieser Rückzug symbolisiert eine gut genutzte „Privatsphären-Einstellung“ bzw. eine gut eingestellte „App-Berechtigung“. Manches Mal hilft vielleicht auch eine gute Firewall oder ein starkes Antivirenprogramm.

Nach 4-5 Angriffen wird getauscht, dann darf sich ein anderes Kind gegen Daten-Klau verteidigen. Vorher wird aber erst besprochen, welcher „Datenklau“ besonders unangenehm bzw. folgenreich ist.

ABSCHLUSS

Die SuS lieben es, wenn die Lehrkraft sich ebenfalls als Surfer/-in den Angriffen der neugierigen Datensammler/-innen aussetzt. Hier wäre es gut, wenn eine zweite Lehrkraft moderiert. Am Ende können Sie auch den Server abstürzen lassen. Dann liegen bedauerlicherweise alle Daten (Fotos, private Informationen usw.) frei, also ungeschützt, im Netz und können von allen eingesammelt werden.

Besprechen Sie, wie sich das für die „bestohlene“ Person anfühlt. „Es ist, als wäre in mein Haus eingebrochen worden, nur noch schlimmer: jeder kann meine Emails lesen, an mein Bankkonto heran und Überweisungen machen, sieht meine persönlichsten Fotos …!“ 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! Allerdings muss auch klar sein: die meisten Firmen stehlen die Daten nicht, wir geben sie ihnen freiwillig durch die Nutzung der App.

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

Tipp: Um zu sehen, welche App worauf zugreift, kann die App „MyPermissions - Privacy Cleaner“ auf dem Handy installiert werden.

PLATZ FÜR NOTIZEN: