



STACJA 5

Wypuszczony balonik czyli pułapki wizerunku



KARTA PRACY DLA DUŻYNY

Tematyka: ochrona wizerunku, ryzyko kradzieży tożsamości cyfrowej, zjawisko sharentingu i cyberprzemocy, nieodwracalności publikacji w internecie „w sieci nic nie ginie”.

Weszliście do cyfrowej galerii zdjęć, zupełnie jak w internecie. Wasz wizerunek to nie tylko twarz, to Wasze dobro osobiste i dane osobowe chronione przez ogólne rozporządzenie o ochronie danych (RODO). Kiedy udostępniasz swoje zdjęcie podejmujesz ryzyko. Oczywiście, masz prawo do usunięcia swoich danych, ale co się stanie, jak Twoje zdjęcie błyskawicznie zostało podane dalej, przez kolejnych użytkowników internetu? Kiedy udostępnisz czyjeś zdjęcie, tylko za zgodą tej osoby, może być podobnie. Zatem już wiecie, że publikując zdjęcia, tracicie nad nim kontrolę – to jak wypuszczenie balonu w powietrze. Gdy wypuścisz z dłoni balon, tracisz nad nim kontrolę. Tak samo jest ze zdjęciem w internecie. Posłuchajcie historii Zosi i odpowiedzcie na pytania.

Zadanie 1

Poznajcie historię Zosi, a następnie udzielcie odpowiedzi na pytania.

Zosia zrobiła po lekcjach śmieszne zdjęcie swojemu koledze z ławki Tomkowi. Tomek jest na nim sam i wyraźnie widać jego twarz. Zosia chce wrzucić to zdjęcie na otwartą grupę na portalu społecznościowym, żeby zdobyć dużo „lajków”. Zanim jednak to zrobi, przypomina sobie historię swojej koleżanki Asi.

Asia wrzuciła do sieci zdjęcie z wakacji swojego młodszego brata. Po kilku miesiącach ktoś pobrał to zdjęcie i założył w internecie fałszywą zbiórkę pieniędzy na „chore dziecko” bezprawnie używając twarzy brata Asi. Zosia zaczyna mieć wątpliwości...

1. Jak nazywa się to przestępstwo, którego ofiarą padł brat Asi i dlaczego dziewczyna nie może po prostu skasować ukradzionego zdjęcia z internetu?

Odpowiedź:

.....

.....

.....



2. Mając na uwadze prawo i ogólne rozporządzenie o ochronie danych osobowych tzw. RODO, co musi zrobić Zosia przed publikacją zdjęcia Tomka?
Dlaczego to jest takie ważne?

Odpowiedź:

.....

.....

.....

3. Z uwagi na to, że Tomek jest niepełnoletni, kto jeszcze musi wyrazić zgodę na publikację?

Odpowiedź:

.....

.....

.....

Zadanie 2

Połączcie definicje z właściwymi hasłami (fiszki):

POJĘCIE

DEFINICJA

A. Phishing

1. Informacje pozostawiane w internecie świadomie (np. posty, zdjęcia) i nieświadomie (np. lokalizacja GPS, historia wyszukiwania). Informacje te pomagają stworzyć cyfrowy profil osoby.

B. Cyfrowy ślad

2. Zamieszczanie przez rodziców (często nadmierne i bezrefleksyjny) wizerunku i innych danych osobowych swoich dzieci w internecie np. świadectwa szkolnego, zdjęć z wakacji, zawodów sportowych i innych aktywności.

C. Dane osobowe

3. Informacje, które pozwalają na rozpoznanie osoby np. imię i nazwisko, adres, numer telefonu, e-mail, głos, odcisk palca czy wizerunek, kolor włosów. Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby.

D. Cyberprzemoc
(cyberbullying)

4. Próba oszustwa i podszywania się pod zaufaną osobę lub instytucję w celu wyłudzenia danych osobowych np. haseł lub danych kart płatniczych, aby komuś zaszkodzić.

E. Sharenting

5. Celowe krzywdzenie i nękanie kogoś przy użyciu sztucznej inteligencji i technologii deepfake np. udostępnianie ośmieszających przeróbek zdjęć czy filmów.



Zadanie 3

Wyobraźcie sobie, że niżej zamieszczony rysunek, to zdjęcie prawdziwego chłopca ze świadectwem ukończenia klasy 3, na którym są widoczne dane osobowe.



Zakreśl, jakie dane osobowe i informacje o chłopcu, zostały udostępnione na zdjęciu:

- ☐ imię
- ☐ nazwisko
- ☐ odcisk palca
- ☐ nazwa ulicy
- ☐ kolor włosów
- ☐ nazwa szkoły
- ☐ miejscowość
- ☐ wizerunek
- ☐ lokalizacja
- ☐ data urodzenia
- ☐ pesel
- ☐ numer buta
- ☐ kolor oczu

Publikując zdjęcia w internecie, zawsze warto zwrócić uwagę, czy w tle nie widać prywatnych informacji oraz wizerunków innych osób. Zwracajcie uwagę, jakie szczegóły widać na zdjęciu, które mogą zdradzić więcej informacji i danych niż zamierzacie.



STACJA 5

Wypuszczony balonik czyli pułapki wizerunku



KARTA MENTORA – OPIEKUNA STACJI

Rola mentora – jesteś przewodnikiem, który zadaje pytania, aby pomóc drużynie rozwiązać zadanie. Nie przekazujesz wiedzy, nie podajesz rozwiązań, ale naprowadzasz tylko pytaniami. Mentor nie krytykuje odpowiedzi drużyny, lecz zadaje jedno z pytań. Możesz wybrać je z zaproponowanej listy pytań pomocniczych. Zaliczenie stacji następuje, gdy uczeń własnymi słowami sformułuje prawidłową odpowiedź związaną z ochroną prywatności.

Instrukcja dla mentora

1. Daj drużynie 1 minutę na przeczytanie „Pigułki wiedzy”.
2. Przekaż drużynie „Kartę pracy” i włącz stoper, czas wykonania zadań to 8 minut.
3. Jeśli drużyna nie zna odpowiedzi, NIE podawaj rozwiązania. Zadawaj pytania naprowadzające oraz pytanie finałowe.
4. Po prawidłowym rozwiązaniu wręczasz drużynie fragment „Kodu odporności cyfrowej”.
5. Jeśli drużyna podjęła złą decyzję – zabierz odpowiedni „Żeton decyzji”.

Żetony decyzji: Wizerunek / Dane osobowe, które drużyna oddaje, jeśli udzieli złych odpowiedzi.

Fragment „Kodu odporności cyfrowej”, który drużyna otrzymuje po wykonaniu zadania: „Decyduję”.

Cel mentora: Uświadomienie nieodwracalności publikacji w sieci („w internecie nic nie ginie”), faktu, że wizerunek to dana osobowa oraz konieczności uzyskania zgody na jego publikację.

Główne zagadnienia: Nieodwracalność publikacji („w sieci nic nie ginie”), ochrona wizerunku, zgoda na publikację, sharenting, kradzież tożsamości cyfrowej.

Pytania naprowadzające

Dlaczego opublikowanie zdjęcia w internecie porównujemy do wypuszczenia z dłoni balonika? Zosia zrobiła śmieszne zdjęcie Tomkowi i chce je wrzucić na otwartą grupę dla „lajków”. Z kim bezwzględnie musi porozmawiać i czyje zgody uzyskać przed kliknięciem „Opublikuj”?

Pytania pogłębiające

Kiedy robicie zdjęcie ze świadectwem szkolnym na tle budynku szkoły, jakich prywatnych danych w tle nie powinny widzieć inne osoby?



Nawet jeśli Zosia usunie zdjęcie ze swojego profilu po 10 minutach, dlaczego nie ma pewności, że zdjęcie zniknęło z internetu?

Co to jest kradzież tożsamości cyfrowej i jak czyjeś zdjęcie z wakacji może zostać wykorzystane przez oszustów?

Pytanie finałowe (klucz zaliczenia stacji i otrzymania fragmentu „Kodu odporności cyfrowej”)

Dlaczego opublikowanie zdjęcia w internecie porównujemy do wypuszczenia z dłoni balonika?

Jaką złotą zasadą powinniśmy się kierować przed udostępnieniem zdjęć w sieci?

Pytanie na wniosek końcowy

O czym zawsze należy pomyśleć zanim udostępnimy czyjś wizerunek w sieci?

Oczekiwana odpowiedź: Przemyślenie skutków na przyszłość oraz bezwzględne zapytanie o zgodę osoby na zdjęciu i jej rodziców (jeśli osoba nie ukończyła 18 lat).

Uwaga: do wykonania zadania używamy wyłącznie gotowej, wydrukowanej karty rysunkowej a nie analizujemy realnych zdjęć uczniów. Analiza prywatnych zdjęć dzieci na forum grupy, mogłaby prowadzić do poczucia wstydu, hejtu lub stygmatyzacji.





STACJA 5

Wypuszczony balonik czyli pułapki wizerunku



KLUCZ ODPOWIEDZI DLA MENTORA – OPIEKUNA STACJI

Tematyka: ochrona wizerunku, ryzyko kradzieży tożsamości cyfrowej, zjawisko sharentingu i cyberprzemocy, nieodwracalności publikacji w internecie „w sieci nic nie ginie”.

➤ Opis stacji

Weszliście do cyfrowej galerii zdjęć, zupełnie jak w internecie. Wasz wizerunek to nie tylko twarz, to Wasze dobro osobiste i dane osobowe chronione przez ogólne rozporządzenie o ochronie danych (RODO). Kiedy udostępniasz swoje zdjęcie podejmujesz ryzyko. Oczywiście, masz prawo do usunięcia swoich danych, ale co się stanie, jak Twoje zdjęcie błyskawicznie zostało podane dalej, przez kolejnych użytkowników internetu? Kiedy udostępnisz czyjeś zdjęcie, tylko za zgodą tej osoby, może być podobnie. Zatem już wiecie, że publikując zdjęcia, tracicie nad nim kontrolę – to jak wypuszczenie balonu w powietrze. Gdy wypuścisz z dłoni balon, tracisz nad nim kontrolę. Tak samo jest ze zdjęciem w internecie. Posłuchajcie historii Zosi i odpowiedzcie na pytania.

Zadanie 1

Historia Zosi oraz klucz odpowiedzi

Zosia zrobiła po lekcjach śmieszne zdjęcie swojemu koledze z ławki Tomkowi. Tomek jest na nim sam i wyraźnie widać jego twarz. Zosia chce wrzucić to zdjęcie na otwartą grupę na portalu społecznościowym, żeby zdobyć dużo „lajków”. Zanim jednak to zrobi, przypomina sobie historię swojej koleżanki Asi.

Asia wrzuciła do sieci zdjęcie z wakacji swojego młodszego brata. Po kilku miesiącach ktoś pobrał to zdjęcie i założył w internecie fałszywą zbiórkę pieniędzy na „chore dziecko” bezprawnie używając twarzy brata Asi.

Zosia zaczyna mieć wątpliwości...

1. **Jak nazywa się to przestępstwo, którego ofiarą padł brat Asi i dlaczego dziewczyna nie może po prostu skasować ukradzionego zdjęcia z internetu?**

Odpowiedź: *Takie działanie może być uznane na przykład za oszustwo, kradzież tożsamości, bezprawne wykorzystanie wizerunku innej osoby. Ktoś może ukraść nasze zdjęcie lub dane i wykorzystać je żeby oszukać innych, albo zdobyć pieniądze (oszustwo finansowe). Kiedy wrzucimy zdjęcie do internetu, trudno je potem całkowicie usunąć. Ktoś może je zapisać, zrobić zrzut ekranu albo wysłać*



dalej. Dlatego tracimy kontrolę nad tym, gdzie nasze zdjęcie się pojawi i kto je zobaczy oraz jak je wykorzysta.

2. **Mając na uwadze prawo i ogólne rozporządzenie o ochronie danych osobowych tzw. RODO, co musi zrobić Zosia przed publikacją zdjęcia Tomka? Dlaczego to jest takie ważne?**

Odpowiedź: Zosia musi zapytać Tomka o zgodę na udostępnienie jego wizerunku. Wizerunek to dobro osobiste i dana osobowa, chronione prawem. Zdjęcie może zostać użyte do cyberprzemocy lub stworzenia złośliwego deepfake’a, czyli fałszywego obrazu, filmu lub nagrania dźwiękowego wykonanego za pomocą narzędzi sztucznej inteligencji.

3. **Z uwagi na to, że Tomek jest niepełnoletni, kto jeszcze musi wyrazić zgodę na publikację.**

Odpowiedź: Tomek nie ma 18 lat (nie jest pełnoletni), zgodę musi potwierdzić również jego rodzic lub opiekun prawny.

Zadanie 2

Klucz odpowiedzi zawiera pojęcia z prawidłowymi odpowiedziami i opisem definicji.

A – 4 / B – 1 / C – 3 / D – 5/ E – 2

POJĘCIE	DEFINICJA
A. Phishing Phishing to podstępne wyłudzenie danych.	4. Próba oszustwa i podszywania się pod zaufaną osobę lub instytucję w celu wyłudzenia danych osobowych np. haseł lub danych kart płatniczych, aby komuś zaszkodzić.
B. Cyfrowy ślad Cyfrowy ślad to ogół pozostawionych informacji w internecie	1. Informacje pozostawiane w internecie świadomie (np. posty, zdjęcia) i nieświadomie (np. lokalizacja GPS, historia wyszukiwania). Informacje te pomagają stworzyć cyfrowy profil osoby.
C. Dane osobowe Dane osobowe to informacje służące rozpoznaniu kogoś.	3. Informacje, które pozwalają na rozpoznanie osoby np. imię i nazwisko, adres, numer telefonu, e-mail, głos, odcisk palca czy wizerunek, kolor włosów. Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby.





D. Cyberprzemoc (cyberbullying) Cyberprzemoc to rodzaj przemocy w sieci, nękanie.	5. Celowe krzywdzenie i nękanie kogoś przy użyciu sztucznej inteligencji i technologii deepfake np. udostępnianie ośmieszających przeróbek zdjęć czy filmów.
E. Sharenting Sharenting to zjawisko, które może naruszać prywatność dziecka ze strony opiekunów.	2. Zamieszczanie przez rodziców (często nadmierne i bezrefleksyjny) wizerunku i innych danych osobowych swoich dzieci w internecie np. świadectwa szkolnego, zdjęć z wakacji, zawodów sportowych i innych aktywności.

Zadanie 3

Wyobraźcie sobie, że niżej zamieszczony rysunek, to zdjęcie prawdziwego chłopca ze świadectwem ukończenia klasy 3, na którym są widoczne dane osobowe.

Zakreśl, jakie dane osobowe i informacje o chłopcu, zostały udostępnione na zdjęciu:

- ☐ imie
- ☐ nazwisko
- ☐ odcisk palca
- ☐ nazwa ulicy
- ☐ kolor włosów
- ☐ nazwa szkoły
- ☐ miejscowość
- ☐ wizerunek
- ☐ lokalizacja
- ☐ data urodzenia
- ☐ pesel
- ☐ numer buta
- ☐ kolor oczu

**PUBLIKUJĄC ZDJĘCIA W INTERNECIE, ZAWSZE WARTO ZWRÓCIĆ UWAGĘ, CZY W TLE
NIE WIDAĆ PRYWATNYCH INFORMACJI.**



STACJA 5

Wypuszczony balonik czyli pułapki wizerunku



PIGUŁKA WIEDZY

Główne zagadnienia

Twój wizerunek, to nie tylko obraz twarzy – to także sylwetka, sposób chodzenia fryzura, ubiór, a nawet głos czy avatar w grze, które pomagają Ciebie rozpoznać. Wizerunek jest Twoim dobrem osobistym i stanowi dane osobowe chronione przez prawo.

Nikt bez zgody Twojej i Twoich rodziców nie powinien z niego korzystać.

- **Kradzież cyfrowej tożsamości**

Bezprawne pobranie nieswojego zdjęcia z sieci i wykorzystanie go np. do założenia fałszywego konta lub fałszywej zbiórki pieniędzy.

- **Phishing**

Phishing to podstępne wyłudzenie danych osobowych.

- **Cyfrowy ślad**

Wszystko, co robisz w sieci (posty, zdjęcia, lajki, lokalizacja GPS), tworzy Twój cyfrowy ślad. Buduje on Twoją reputację na całe życie oraz tworzy Twój profil cyfrowy w internecie.

- **Sharenting**

Nieprzemyślane i nadmierne publikowanie danych i zdjęć dzieci przez dorosłych.

ZROZUM, ŻE TWÓJ WIZERUNEK JEST PRAWNIE CHRONIONY, A PUBLIKACJA W INTERNECIE MA NIEODWRACALNE SKUTKI!

- **Obowiązek uzyskania zgody**

Zanim opublikujesz w sieci zdjęcie z kolegą lub koleżanką, bezwzględnie musisz zapytać ich o zgodę (w przypadku osób niepełnoletnich zgody muszą udzielić również rodzice).

- **Brak kontroli po publikacji**

Kiedy wrzucimy zdjęcie do internetu, trudno je potem całkowicie usunąć. Ktoś może je zapisać, zrobić zrzut ekranu albo wysłać dalej. Dlatego tracimy kontrolę nad tym, gdzie nasze zdjęcie się pojawi i kto je zobaczy oraz jak je wykorzysta.

- **Tło zdjęcia zdradza dane**

Publikując np. zdjęcie ze świadectwem szkolnym, nieświadomie ujawniasz imię, nazwisko, nazwę oraz adres szkoły (lokalizację).

- **Metafora wypuszczonego balonika**

Udostępnienie zdjęcia w sieci jest jak **wypuszczenie z dłoni balonika** – od razu tracisz nad nim kontrolę!



ZŁOTA ZASADA STACJI 5 SUPERMOC DETEKTYWA PRYWATNOŚCI

PAMIĘTAJ, ŻE „INTERNET NIE ZAPOMINA”. ZANIM UDOSTĘPNISZ CZYJEŚ ZDJĘCIE, ZAWSZE ZAPYTAJ O ZGODĘ. UDOSTĘPNIANIE ZDJĘCIA W INTERNECIE JEST JAK WYPUSZCZENIE BALONU Z DŁONI – OD RAZU TRACISZ NAD NIM KONTROLĘ, A Z SIECI NIEZWYKLE TRUDNO COKOLWIEK USUNĄĆ.



PRZEMYŚL DWA RAZY, ZANIM KLIKNIESZ „WYŚLIJ” I UDOSTĘPNISZ SVOJE DANE OSOBOWE.