6 Widoczność i bezpieczeństwo w Internecie dziś i jutro

Maria Bajak, Iryna Manczak, Katarzyna Sanak-Kosmowska

Wprowadzenie

Z jednej strony rozwój technologiczny wspiera kontakty społeczne, ułatwia pracę i zdobywanie wiedzy oraz podnosi komfort życia i implikuje dobrobyt. Z drugiej zaś postępująca cyfryzacja i powszechny dostęp do sieci internetowej prowadzą do powstania wielu nowych problemów i zagrożeń. Rzutują one na strukturę obowiązujących standardów, norm etycznych i przepisów prawnych, które mają chronić użytkowników sieci. By uczynić ich bardziej świadomymi niebezpieczeństw i umiejącymi sobie z nimi radzić, ważna jest edukacja od najmłodszych lat. Należy pamiętać, że zagrożenia płynące z sieci dotyczą zarówno osób prywatnych, jak i różnych instytucji (np.: szkół, przedsiębiorstw, urzędów), a nawet całych społeczności. Celem zajęć warsztatowych z zakresu widoczności i bezpieczeństwa w Internecie jest przedstawienie niebezpieczeństw czyhających na jego użytkowników oraz wskazanie sposobów odpowiedniego reagowania w takich sytuacjach.

Należy podkreślić, że problemy świata cyfrowego dotyczą różnych obszarów. Niebezpieczeństwa mogą generować nie tylko strony zawierające niestosowne i drastyczne treści, ale również portale zbierające wrażliwe dane czy nawet komunikatory internetowe i media społecznościowe. Każdy użytkownik cyberprzestrzeni powinien być ich świadomy i odporny na pojawiające się zagrożenia. Rosnące możliwości narzędzi cyfrowych zwiększają również pole działania cyberprzestępców, którzy wykorzystują różnorodne techniki manipulacji

w celu osiągnięcia korzyści osobistych lub finansowych. Ważnym obszarem prowadzonych zajęć jest przedstawienie konkretnych technik ataków hakerskich i uświadomienie uczestnikom zajęć zagrożeń płynących z cyberprzestępczości.

Warto wskazać, że najpowszechniejszą walutą w sieci internetowej są dane osobowe. Zbieranie informacji na temat użytkowników jest zjawiskiem powszechnym, a plastyczność cyberprzestrzeni sprawia, że zdobyta wiedza w łatwy sposób może zostać przekształcona w spersonalizowany przekaz marketingowy. Wprawdzie ułatwia to podejmowanie decyzji zakupowych oraz przyczynia się do budowania relacji marek z nabywcami, ale jednocześnie prywatność w sieci staje się narzędziem transakcyjnym i krytycznym problemem dla osób fizycznych. Uczestnicy zajęć dowiedzą się, jak cenne są ich dane osobowe i dlaczego warto je chronić.

Tabela 6.1. Efekty uczenia się – temat zajęć: „Widoczność i bezpieczeństwo w Internecie dziś i jutro”

Rodzaj efektu uczenia się	Wyszczególnienie
Wiedza	uczestnicy/uczestniczki zajęć: • znają zagrożenia czyhające na użytkowników sieci internetowej oraz konkretne techniki stosowane przez hakerów w celu dokonania przestępstw • potrafią zdefiniować najważniejsze pojęcia z zakresu cyberbezpieczeństwa i ochrony danych osobowych
Kompetencje	uczestnicy/uczestniczki zajęć: • potrafią ocenić stopień bezpieczeństwa w cyberprzestrzeni • potrafią zidentyfikować rodzaje danych gromadzonych przez strony internetowej oraz możliwości ich wykorzystania przez administratorów
Umiejętności	uczestnicy/uczestniczki zajęć: • potrafią stworzyć odpowiednie zabezpieczenia strony internetowej czy profilu w mediach społecznościowych • potrafią odpowiednio reagować na zagrożenia w sieci internetowej • potrafią krytycznie myśleć i pracować w grupie

Źródło: opracowanie własne.

Najważniejsze pojęcia i definicje

CZĘŚĆ 1. Dane osobowe

We współczesnym świecie ważną walutą stały się dane osobowe, którymi użytkownicy sieci płacą za możliwość dostępu do treści na stronach internetowych. Pozornie darmowe portale wymagają wyrażenia zgody na zbieranie informacji o odbiorcy, które następnie wykorzystywane są do personalizacji działań marketingowych w sieci internetowej. Przetwarzane dane dotyczą m.in. różnych informacji personalnych oraz zachowania internauty w przestrzeni wirtualnej (Tabela 6.2). Aby rozsądnie podejmować decyzje o udostępnieniu swoich danych w zamian za możliwość korzystania z treści na stronach internetowych, ważna jest świadomość, że nasze zachowanie w Internecie jest nieustannie analizowane.

Tabela 6.2. Dane zbierane o konsumencie w sieci internetowej

Rodzaj danych	Przykład
Demograficzne	zbieranie informacji na temat płci, wieku, stanu cywilnego i statusu związku, wykształcenia, roli w rodzinie
Geograficzne	określanie lokalizacji, w której znajduje się urządzenie, z którego korzysta dany użytkownik
Ekonomiczne	gromadzenie wiedzy na temat aktywności zawodowej, poziomu życia, wartości dokonywanych zakupów, marek i modeli posiadanych urządzeń elektronicznych oraz odwiedzanych sklepów online

Rodzaj danych	Przykład
Psychograficzne	wskazywanie zainteresowań i cech osobowościowych użytkownika oraz ocenianie jego stylu życia na podstawie aktywności w Internecie i specyficznych powiązań ze znajomymi w sieci
Behawioralne	badanie zachowania internauty, sposobu jego reagowania na komunikaty pojawiające się w sieci, lojalności wobec marek oraz wszelkich innych aktywności online
Intencje zakupowe	określanie planów zakupowych konsumenta na podstawie przeglądanych przez niego stron i oglądanych produktów
Użytkowanie produktu	zbieranie danych na temat sposobów korzystania z urządzeń podłączonych do sieci, dokonywanie pomiarów, ustalanie prawidłowości i analizowanie danych

Źródło: opracowanie własne.

Prawo do prywatności – prawo do samodzielnego decydowania o swoim życiu i ochrony przed ingerowaniem w nie innych.

Dane osobowe – wszelkie informacje dające możliwość zidentyfikowania konkretnej osoby, np.: imię, nazwisko, numer telefonu, e-mail, PESEL, adres zamieszkania itd.

Ochrona danych osobowych – aktywna ochrona informacji o personalnym charakterze, zabezpieczanie jednostki przed zagrożeniami związanymi z przetwarzaniem personalnych informacji na jej temat m.in. poprzez nadanie im względnie neutralnej formy, która umożliwia bezpieczne zarządzanie danymi przez administratorów.

Pliki cookie – pliki należące do administratora serwisu internetowego, które przesyłane są do przeglądarki internetowej użytkownika odwiedzającego daną witrynę. W efekcie dają jej możliwość zapisania informacji o preferencjach i zachowaniu użytkownika. Na tej podstawie tworzony jest profil użytkownika, który umożliwia dostosowywanie działań marketingowych do jego potrzeb i preferencji.

RODO (Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679) – dyrektywa wyznaczająca obecnie standardy sposobu gromadzenia informacji na temat użytkowników sieci internetowej obowiązująca w Polsce oraz innych krajach Unii Europejskiej.

Tryb incognito – funkcja pozwalająca na przeglądanie sieci internetowej z zachowaniem większej prywatności, bez zapisywania odwiedzanych stron w historii przeglądarki. Tryb incognito nie chroni przed atakami hakerskimi.

CZĘŚĆ 2. Cyberprzestępczość

Obecnie jednym z największych niebezpieczeństw jest cyberprzestępczość. Obserwujemy dynamiczny wzrost kompetencji użytkowników sprzętu komputerowego oraz sieci internetowej, kreującej anonimowe środowisko sprzyjające działalności kryminalnej. Przestępcy internetowi nieustannie doskonalą swoje techniki, co powoduje trudności w stworzeniu adekwatnych zabezpieczeń. Wiele z powszechnie stosowanych systemów informatycznych posiada luki w bezpieczeństwie, a jednocześnie możliwości ścigania cyberprzestępców są ograniczone. Część popełnianych wykroczeń jest niewykrywana z powodu zaawansowanych umiejętności hakerów. Wraz z rozwojem technologicznym, systematycznie dokształcają się oni i poszukują coraz bardziej niekonwencjonalnych rozwiązań, które często nie są jeszcze znane organom ścigania.

Cyberprzestępczość – wszelkie nielegalne działania dokonywane w przestrzeni cyfrowej.

Haker – użytkownik sieci posiadający dużą wiedzę na temat komputerów i Internetu, którą wykorzystuje w celu nielegalnego osiągnięcia korzyści osobistych lub finansowych.

Przestępstwo komputerowe – nielegalne działania dokonywane bezpośrednio za pośrednictwem systemów i sieci komputerowych, które zagrażają bezpieczeństwu ich oraz przetwarzanych przez nie danych.

Przestępstwa przy wykorzystaniu komputerów – wszelkie nielegalne działania, które są popełniane za pomocą systemów i sieci komputerowych. Odnoszą się nie tylko do bezpieczeństwa komputerów i zgromadzonych w nich danych, ale również do zdobywania, posiadania i rozpowszechniania treści i materiałów za ich pośrednictwem czy grożenia, znieważania, oszukiwania oraz dręczenia innych użytkowników sieci.

Atak hakerski – włamanie do systemów i sieci komputerowych, a wskutek tego naruszenie bezpieczeństwa ich oraz przetwarzanych przez nie danych. Może mieć charakter nieukierunkowany lub ukierunkowany (Tabela 6.3). Do najpopularniejszych technik dokonywania ataków hakerskich należą:

1. **Ataki nieukierunkowane:**
   a. wyłudzanie (*phishing*) – masowe rozsyłanie wiadomości (np. e-maile, SMS-y, wiadomości wysyłane za pośrednictwem komunikatorów internetowych) zawierających prośby o udostępnienie danych lub linki prowadzące do fałszywych stron internetowych, które zawierają szkodliwe oprogramowanie;
   b. atak przy wodopoju (*watering hole attack*) – udostępnienie fałszywej strony internetowej lub przejęcie istniejącej w celu zdobycia danych odwiedzających ją i logujących się na nią

użytkowników. Technika ta często jest łączona z wyłudzaniem (*phishingiem*);

c. wymuszanie (*ransomware*) – rozpowszechnianie złośliwego oprogramowania, które atakuje system komputerowy lub serwer i szyfruje wszystkie przechowywane na nim dane. Następnie przestępcy szantażują ofiarę, aby w zamian za odszyfrowanie tych danych uzyskać określone korzyści;
d. skanowanie (*scanning*) – wyrywkowe ataki nakierowane na losowe urządzenia podłączone do sieci internetowej.

2. Ataki ukierunkowane:

a. wyłudzanie profilowane (*spear-phishing*) – rozsyłanie spersonalizowanych komunikatów (np.: e-maile, SMS-y, wiadomości wysyłane za pomocą komunikatorów internetowych) zawierających załączniki ze szkodliwym oprogramowaniem lub link aktywujący jego pobranie;
b. sieć botów (botnet) – uzyskanie kontroli nad jednym z urządzeń podłączonych do lokalnej sieci komputerowej w celu wykonania ataków na inne urządzenia (np. uzyskanie dostępu do drukarki, aby przejąć kontrolę nad połączonym z nią komputerem);
c. przerwanie łańcucha dostaw (*subverting the supply chain*) – bezpośredni atak na konkretne urządzenie lub system, które mają duże znaczenie dla realizacji celu przestępstwa, a jednocześnie są słabo zabezpieczone. Efektem ma być przejęcie kontroli nad realizacją jakiegoś procesu (np. produkcji) lub jego całkowite wstrzymanie.

Tabela 6.3. Rodzaje ataków hakerskich

Rodzaje ataków	Charakterystyka	Przykład
Atak nieukierunkowany	• masowe uderzenie na jak największą liczbę urządzeń oraz użytkowników sieci • dla napastnika nie ma znaczenia tożsamość ofiar, a jedynie ich liczba • techniki włamania z reguły wykorzystują otwartość Internetu	• wyłudzanie • atak przy wodopoju • wymuszanie • skanowanie
Atak ukierunkowany	• działanie kryminalne wymierzone w konkretną osobę lub organizację • przestępca posiada precyzyjnie określone cele oraz plan na przeprowadzenie natarcia • przygotowanie zajmuje zazwyczaj długi czas i opiera się na poszukiwaniu najsłabszych punktów zabezpieczenia systemu	• wyłudzanie profilowane • sieć botów • przerwanie łańcucha dostaw

Znajomość niebezpieczeństw związanych z cyberprzestępczością skłania do refleksji nad metodami ich profilaktyki. Wiele ze sposobów prowadzenia ataków hakerskich nakierowanych jest na wykorzystanie nieświadomości i lekkomyślności użytkowników sieci. Dlatego też ważne jest podejmowanie działań zapobiegawczych, takich jak:

- wykorzystanie skomplikowanych kombinacji liter, numerów i znaków specjalnych przy ustawianiu haseł oraz ich regularne zmienianie;
- regularne aktualizowanie systemów bezpieczeństwa;
- właściwe zabezpieczenie lokalnej sieci komputerowej i podłączonych do niej urządzeń;
- zachowanie ostrożności w przypadku łączenia się z siecią internetową z niezaufanych źródeł (np. ogólnodostępne wi-fi);

- regularne skanowanie bezpieczeństwa posiadanych urządzeń;
- zachowanie szczególnej ostrożności przy otwieraniu wiadomości z nieznajomych źródeł, nieklikanie w podejrzane linki;
- zgłaszanie zauważonych niebezpieczeństw.

CZĘŚĆ 3. Fake newsy i hejt

Poszukiwanie sensacji, propaganda i manipulacja towarzyszą ludzkości od zarania dziejów. Jednak obecnie, w dobie technologii cyfrowych, rozpowszechnianie fałszywych informacji stało się prostsze niż kiedykolwiek. Narzędzia informatyczne umożliwiają nie tylko zmienianie treści wypowiedzi, ale także tworzenie przekonujących montaży zdjęć czy nawet podkładanie cudzych głosów i twarzy w materiałach wideo. Dodatkowo dają możliwość błyskawicznego rozprzestrzeniania się opublikowanych treści. Szczególnie szybko informacje rozpowszechniają się w mediach społecznościowych, gdzie użytkownicy mają możliwość polubienia, skomentowania lub udostępnienia informacji swoim znajomym za pomocą jednego kliknięcia. W efekcie internauci są zewsząd otaczani przez fałszywe lub podkoloryzowane treści, których głównych zadaniem jest wywołanie jak największej sensacji. Świadomy użytkownik Internetu powinien wiedzieć, że nie należy wierzyć we wszystkie podane w nim informacje.

Fake news – treść zawierająca nieprawdziwe lub przeinaczone informacje.

Hejt – zjawisko poniżania i agresji wobec innych użytkowników Internetu.

Manipulacja – wykorzystanie różnorodnych środków, metod i technik w celi wywierania wpływu na innych ludzi i przekonania ich do przyjęcia określonego zdania na dany temat lub założonych działań.

Propaganda – działania zmierzające do ukształtowania pożądanych poglądów wśród ludzi i sterowania ich zachowaniem poprzez wykorzystanie różnorodnych technik manipulacji.

Dezinformacja – celowe i konsekwentne szerzenie nieprawdziwych informacji w celu wprowadzenia odbiorców w błąd i przyjęcia przez nich określonych postaw i zachowań.

Bańka informacyjna – dopasowywanie informacji wyświetlanych w Internecie do preferencji i poglądów danego użytkownika, ograniczające mu dostęp do danych z alternatywnych źródeł.

Viral – treści, które są chętnie rozpowszechniane przez internautów, przez co szybko stają się popularne w sieci.

Rozpowszechnianie się fałszywych informacji może prowadzić do wywołania silnych emocji i paniki wśród ludzi, a co za tym idzie – agresywnych lub nieodpowiedzialnych zachowań. Dodatkowo stanowią one zagrożenie dla dobrego imienia osób, marek, przedsiębiorstw, miejsc itd. Mogą prowadzić do umacniania się stereotypów oraz pogłębiania podziałów społecznych, a w efekcie niechęci np. do konkretnych grup społecznych, mniejszości etnicznych czy po prostu posiadaczy innych poglądów. Jest to niebezpieczne zjawisko, któremu trzeba przeciwdziałać. Przede wszystkim należy weryfikować wszystkie informacje, z którymi mamy styczność, m.in. poprzez:

- zbadanie wiarygodności źródła,
- zapoznanie się z całością materiału, a nie tylko z jego nagłówkiem,
- sprawdzenie wiadomości w różnych źródłach,
- przemyślenie treści i jej sensu oraz emocji, jakie wzbudzają,
- zapytanie o opinię ekspertów.

W przypadku, gdy treść wydaje się podejrzana, nie należy jej dalej udostępniać w poszukiwaniu sensacji, ponieważ przyczynia się to do rozprzestrzenianie się fake newsów.

Przykładowy scenariusz lekcji

Przykładowy scenariusz zajęć obejmuje trzy moduły:

1. Dane osobowe.
2. Cyberprzestępczość.
3. Fake newsy i hejt.

Każdy z poszczególnych modułów powinien zająć dwie godziny lekcyjne. W razie potrzeby zajęcia mogą zostać skrócone poprzez rezygnację z wykonania niektórych ćwiczeń. W założeniu scenariusz kierowany jest do grupy osób w wieku około 12–14 lat. Jednakże odpowiednia moderacja zajęć pozwala na ich przeprowadzenie również z młodszymi i starszymi grupami.

TEMAT: Widoczność i bezpieczeństwo w Internecie dziś i jutro

Głównym celem zajęć jest nabycie świadomości zagrożeń w sieci internetowej oraz umiejętności reagowania na niebezpieczeństwa, a także zrozumienie wartości danych osobowych i konieczności rozsądnego nimi rozporządzania. Specyfikację zajęć, w tym cele szczegółowe i metody dydaktyczne, przedstawia tabela 6.4.

Tabela 6.4. Specyfikacja zajęć „Widoczność i bezpieczeństwo w Internecie dziś i jutro"

Cele ogólne	uczestnicy/uczestniczki zajęć: • są świadomi zagrożeń w sieci internetowej • potrafią odpowiednio reagować na niebezpieczeństwa w cyberprzestrzeni • rozumieją, jak wartościowe są ich dane osobowe, i potrafią je chronić oraz umiejętnie nimi rozporządzać

Cele szczegółowe	uczestnicy/uczestniczki zajęć: • potrafią wskazać techniki ataków hakerskich oraz sposoby ochrony przed nimi • mają świadomość, jak chronić swoje dane w sieci internetowej i rozwijać swoje kompetencje w tym zakresie • wiedzą, w jaki sposób zostawiają ślady w cyberprzestrzeni i w jaki sposób mogą one zostać wykorzystane • mają świadomość, że nie wszystkie wiadomości pojawiające się w sieci internetowej są prawdziwe • potrafią świadomie wybierać treści, z którymi się zapoznają, oraz ocenić swoje bezpieczeństwo w obrębie danej witryny • rozumieją specyfikę zagrożeń pojawiających się w Internecie i wiedzą jak sobie z nimi radzić • systematycznie dokształcają się w zakresie niebezpieczeństw w Internecie oraz pogłębiają umiejętności świadomego korzystania z jego zasobów
Metody i sposoby realizacji celów	wykład audytoryjny, dyskusja, studium przypadku, praca w grupie, metoda dramowa, analiza SWOT, mapa myśli, metoda puzzli, rozwiązywanie problemów
Praktyczne wskazówki	• ze względu na obszerność materiału, zajęcia powinny zostać podzielone na odrębne moduły, np. w sposób sugerowany w niniejszym podręczniku: 1. dane osobowe, 2. cyberprzestęp czość, 3. fake newsy i hejt • każdą część zajęciową warto rozpocząć od dyskusji, a dopiero później przejść do wykładu, po którym będą realizowane kolejne ćwiczenia aktywizujące • uczestnicy i uczestniczki zajęć są z pewnością aktywnymi użytkownikami Internetu, dlatego też cennym uzupełnieniem zajęć będzie zapytanie ich o ich własne doświadczenia dotyczące niebezpieczeństw w sieci

Praktyczne wskazówki	• w studium przypadku dotyczącym fake newsów (Zadanie 2 w Module 3) warto wykorzystać aktualne przykłady artykułów zawierających nieprawdziwe informacje, najlepiej dotyczące spraw, które w danym momencie wzbudzają wiele emocji

Źródło: opracowanie własne.

Przebieg zajęć

Trzy oddzielne moduły, na które zajęcia zostały podzielone, mogą być realizowane podczas jednej (z zachowaniem odpowiedniej kolejności) lub kilku lekcji. Każdy z modułów powinien być traktowany jako kompletna całość, dlatego też najlepiej zachować ich odrębną strukturę. Sugerowany przebieg zajęć dla każdego z modułów prezentuje się następująco:

1. Dyskusja wprowadzająca.
2. Wykład.
3. Ćwiczenia aktywizujące.

W ramach zaproponowanych poniżej ćwiczeń aktywizujących podano również propozycje tematów do wprowadzającej dyskusji grupowej.

Ćwiczenia aktywizujące

CZĘŚĆ 1. Dane osobowe

1.1. Dyskusja

Zajęcia powinny zostać rozpoczęte od dyskusji dotyczącej zbierania danych osobowych. Uczestnicy zajęć powinni przyjąć dwie perspektywy

w tracie rozważań. Z jednej strony jest to punkt widzenia przedsiębiorstw:

1. Co daje firmom możliwość zbierania danych o konsumentach?
2. Czy można udoskonalać produkty w oparciu o dane zbierane w sieci? Jak?
3. W jaki sposób dane o konsumentach pomagają w skutecznym promowaniu produktów?

Następnie uczestnicy i uczestniczki zajęć proszeni są o przyjęcie perspektywy konsumenta:

1. Czy zbieranie danych osobowych może być niebezpieczne? Dlaczego?
2. W jaki sposób strony internetowe zbierają o nas dane? Do czego mogą je wykorzystać?
3. Czego dotyczą dane zbierane o nas w sieci internetowej?
4. Czy warto chronić swoją prywatność w sieci internetowej? Dlaczego?

Moderator dyskusji powinien ją podsumować i uzupełnić najważniejsze wątki.

1.2. Analiza SWOT

Kwestie związane z przyszłością wzbudzają wiele emocji, które mają zarówno pozytywny, jak i negatywny wydźwięk. Dlatego też warto je uporządkować. W tym celu można zastosować analizę SWOT. Pozwala ona zidentyfikować mocne (S) i słabe (W) strony omawianego zagadnienia oraz wskazać wynikające z niego szanse (O) i zagrożenia (T).

Grupę ćwiczeniową należy podzielić na pary lub niewielkie zespoły, które będą analizować temat „Zbieranie danych o konsumencie w Internecie przez przedsiębiorstwa". W ramach zadania uczniowie zapisują swoje pomysły dotyczące śledzenia użytkowników w przestrzeni

online, wskazując na ich mocne i słabe strony oraz szanse i zagrożenia (Rysunek 6.1). Dodatkowo w celu urozmaicenia ćwiczenia do każdego ze wskazanych skojarzeń może zostać przyporządkowana odpowiednia waga w skali od 1 do 5 (gdzie 1 oznacza niewielkie, a 5 bardzo duże znaczenie danego zagadnienia).

NOWE TECHNOLOGIE W PRZYSZŁOŚCI

MOCNE STRONY	WAGA
mocna strona 1	5
mocna strona 2	2
mocna strona 3	4
mocna strona 4	1
…	…

SŁABE STRONY	WAGA
słaba strona 1	3
słaba strona 2	1
słaba strona 3	5
słaba strona 4	3
…	…

SZANSE	WAGA
szansa 1	4
szansa 2	5
szansa 3	1
szansa 4	3
…	…

ZAGROŻENIA	WAGA
zagrożenie 1	2
zagrożenie 2	3
zagrożenie 3	5
zagrożenie 4	3
…	…

Rysunek 6.1. Przykładowy arkusz do analizy SWOT

Źródło: opracowanie własne.

Na koniec uczestnicy zajęć powinni zaprezentować swoje analizy SWOT i omówić wspólnie z całą grupą ćwiczeniową.

1.3. Metoda dramowa

Uczestnicy zajęć dzieleni są na cztery zespoły, które będą reprezentować różne grupy osób związanych ze zbieraniem danych osobowych:

- pracownicy przedsiębiorstwa – ta grupa ma przyjąć rolę osób zbierających dane w celu optymalizacji produktów przedsiębiorstwa oraz sposobów ich promocji.
- konsumenci – ta grupa reprezentuje użytkowników sieci internetowej, którzy korzystają z jej zasobów w zamian za swoje dane osobowe.
- hakerzy – ta grupa przyjmuje rolę cyberprzestępców, których celem jest zdobycie danych osobowych użytkowników sieci internetowej.
- prawnicy – ta grupa to eksperci prawni specjalizujący się w ochronie danych osobowych.

Jeżeli grupa zajęciowa jest liczna, można podzielić ją na dwie części i dopiero je podzielić na cztery zespoły. Wtedy grupy będą po kolei wzajemnie obserwować swoje scenki.

Uczestnicy zajęć wcielają się w swoje role i prezentują sytuację, w której dane zbierane przez przedsiębiorstwo zostają wykradzione przez cyberprzestępców. Wcześniej otrzymują czas, aby się przygotować do odegrania swoich postaci. Można zasugerować następujący przebieg scenki:

1. pracownicy przedsiębiorstwa postanawiają ulepszyć swoje produkty i promocje, dlatego zaczynają zbierać dane o konsumentach;
2. konsumenci korzystają z Internetu i pozostawiają w nim swoje dane osobowe, nie czytają regulaminów ich przetwarzania, tylko od razu akceptują wszystkie warunki;
3. hakerzy postanawiają wykraść dane osobowe z przedsiębiorstwa i podejmują różne działania w tym celu;
4. pracownicy przedsiębiorstwa dowiadują się o wycieku danych osobowych i informują o tym konsumentów;
5. konsumenci dowiadują się o wycieku ich danych osobowych, są przerażeni i zgłaszają się do prawników, aby prosić ich o pomoc;

6. prawnicy omawiają niebezpieczeństwa związane z wyciekiem danych osobowych, radzą, co zrobić w takiej sytuacji i jak uniknąć jej w przyszłości.

Po pracy w grupach uczestnicy odgrywają przygotowane przez siebie scenki.

Po zakończeniu inscenizacji prowadzący zajęcia opowiada o konsekwencjach wykradzenia danych osobowych i konieczności ich ochrony, a następnie płynnie przechodzi do kolejnego modułu zajęć poświęconego cyberprzestępczości.

CZĘŚĆ 2. Cyberprzestępczość

2.1. Dyskusja

Moduł zajęciowy powinien zostać rozpoczęty od dyskusji uczestników o cyberprzestępczości. W ramach rozważań można poruszyć następujące kwestie:

- Jakie zagrożenia pojawiają się w sieci internetowej?
- Czy uczestnicy zajęć spotkali się kiedyś z hejtem w sieci? Na czym polega to zjawisko?
- Na czym polega cyberprzestępczość?
- W jaki sposób hakerzy dokonują ataków?
- Na co trzeba uważać w sieci internetowej?
- Jak można się bronić przed niebezpieczeństwami w sieci internetowej?

W tej dyskusji warto poprosić uczestników zajęć o podzielenie się własnymi doświadczeniami dotyczącymi poruszanych tematów.

2.2. Mapa myśli

Uczestnicy łączeni są w kilkuosobowe grupy. Następnie w ramach zadania otrzymują duże arkusze papieru oraz kolorowe flamastry i przygotowują mapę myśli dotyczącą zagrożeń w sieci internetowej. Na środku powinien zostać zapisany główny temat rozważań. Następnie rysowane są od niego gałęzie, które prowadzą do różnych zagadnień powiązanych z zagrożeniami w sieci internetowej (np.: hejt, cyberprzestępczość, zbieranie danych osobowych). Kolejnym etapem jest dopisywanie do poszczególnych zagadnień konkretnych przemyśleń, które mogą się okazać punktem wyjścia do generowania dalszych pomysłów.

Zadanie może zostać dodatkowo urozmaicone wykorzystaniem różnych kolorów do oznaczenia poszczególnych rodzajów zagrożeń w sieci internetowej.

2.3. Metoda puzzli

Uczestnicy zajęć dzieleni są na kilkuosobowe grupy. Potrzebna jest taka ilość grup, by opracowane zostały wszystkie tematy. Liczebność grup zależna jest od ogólnej liczby uczestników zajęć. Każda z grup losuje technikę ataku cybernetycznego stosowaną przez hakerów (wyłudzanie, wymuszanie, atak przy wodopoju, skanowanie, wyłudzanie profilowane, sieć botów, przerwanie łańcucha dostaw). W przypadku małych grup zajęciowych można wybrać do puli wyłącznie tylko ataki nieukierunkowane lub tylko ukierunkowane. Następnie grupy wspólnie opracowują dane zagadnienia, uwzględniając m.in. sposób prowadzenia ataku, jego skutki oraz sposoby ochrony przed tego typu działaniami. Swoje przemyślenia mogą opracować w formie pisemnej lub multimedialnej, przygotowując w ten sposób materiały dla każdego członka grupy. Następnie uczestnicy są mieszani ze sobą tak, aby utworzyć nowe grupy, w których znajdzie się dokładnie po jednej osobie z pierwotnych. Przedstawiają swój temat reszcie nowej grupy, omawiając wszystkie zagadnienia przygotowane z wcześniejszą.

Na koniec zadania uczestnicy zajęć mogą wrócić do swoich pierwotnych grup i wspólnie zaprezentować na forum przygotowany temat. Prowadzący zajęcia powinien dodatkowo uzupełnić przedstawiane zagadnienia.

część 3. Fake newsy i hejt

3.1. Dyskusja

Moduł zajęciowy warto rozpocząć od dyskusji grupowej dotyczącej fake newsów pojawiających się w sieci internetowej. Przede wszystkim należy zacząć od tego, jak uczestnicy zajęć rozumieją pojęcie fake newsa i czy w przeszłości zdarzyło im się spotkać z takim zjawiskiem. W ramach dyskusji powinny zostać poruszone kwestie dotyczące tego, gdzie pojawiają się nierzetelne informacje, czego dotyczą, a także jak się przed nimi chronić.

Można również zapytać osoby biorące udział w dyskusji o to, czy uważają fake newsy za niebezpieczne i dlaczego tak lub nie. Można odnieść się do kwestii pandemii COVID-19 i pojawiającej się w sieci internetowej dezinformacji na jej temat lub innych aktualnych przykładów.

3.2. Studium przypadku

Uczestnicy zajęć dzieleni są na cztero- i pięcioosobowe grupy. Każdy z zespołów otrzymuje do przeczytania trzy fragmenty artykułów, postów lub innych publikacji, z których co najmniej jeden jest fake newsem. Wszystkie grupy powinny otrzymać te same fragmenty. Zadaniem każdej z grup jest dokonanie oceny, które z materiałów zawierają nieprawdziwe treści. Następnie członkowie zespołu powinni zastanowić się nad tym, jakie emocje, myśli i postawy wzbudzają w nich analizowane publikacje. Każda grupa zapisuje je na oddzielnych arkuszach papieru (są trzy arkusze – każdy przydzielony do danego fragmentu) kolorowymi flamastrami (do różnych typów emocji warto przyporządkować

odpowiednie kolory flamastrów, np.: zielony – emocje pozytywne, czerwony – emocje negatywne, niebieski – emocje neutralne). Następnie członkowie grup prezentują po kolei na forum swoje przemyślenia dotyczące publikacji.

Prowadzący ćwiczenia wskazuje, które publikacje zawierają nieprawdziwe informacje, i podejmuje dyskusję z uczestnikami zajęć. Dopytuje się, które elementy publikacji sprawiły, że komunikaty zostały uznane za wiarygodne lub nie. Pytania pomocnicze, które mogą zostać zadane w trakcie rozmowy z grupą:

- Jakie macie wrażenia odnośnie poszczególnych publikacji?
- Czy mieliście trudności z rozpoznaniem informacji nieprawdziwych?
- Co sprawia, że komunikaty nieprawdziwe wyglądają niewiarygodnie?
- Czy zawsze wierzycie w to, co przeczytacie lub usłyszycie?
- Jak się bronić przed fake newsami?

Na zakończenie ćwiczenia prowadzący powinien podsumować przemyślenia uczestników i zapisać na tablicy najważniejsze sposoby chronienia się przed fake newsami.

3.3. Rozwiązywanie problemów

Uczestnicy zajęć otrzymują kartki papieru oraz kolorowe flamastry. Na kartce rysują oś czasu i zaznaczają na niej czynności, które zazwyczaj wykonują w ciągu dnia. Powinni umieścić co najmniej 30 czynności. Następnie zaznaczają kolorami swoje aktywności, przyjmując, że np.:

- kolor zielony odpowiada czynnościom, którymi mogliby się podzielić publicznie na swoim profilu w mediach społecznościowych;
- kolor żółty odpowiada czynnościom, które mogliby przedstawić w mediach społecznościowych swoim najbliższym znajomym;

- kolor czerwony odpowiada czynnościom, którymi nie chcieliby się dzielić w mediach społecznościowych.

Dodatkowo osoby biorące udział w ćwiczeniu proszone są o zaznaczenie gwiazdką czynności, których upublicznianie w mediach społecznościowych mogłoby spowodować hejt.

Następnie uczestnicy zajęć łączą się w pary i wspólnie omawiają swoje osie czasu.

Kolejna część zadania polega na dyskusji podsumowującej, moderowanej przez prowadzącego, podczas której powinny zostać poruszone następujące kwestie:

- Dlaczego pokazujemy tylko niektóre elementy swojego życia w sieci internetowej?
- Co może spowodować hejt?
- Czy uczestnicy zajęć doświadczyli kiedyś hejtu?
- Jak bronić się przed hejtem?
- Czy uczestnikom zajęć zdarza się hejtować innych?
- Dlaczego wizerunek w mediach społecznościowych jest ważny?

Na koniec ćwiczenia prowadzący zajęcia powinien podkreślić, że nasze zachowanie w Internecie kształtuje nasz wizerunek w oczach innych użytkowników. Należy zaznaczyć, że wszelkie treści, które umieszczamy w mediach społecznościowych (włączając w to posty, komentarze, udostępnienia czy polubienia) wymagają wcześniejszej refleksji.

Bibliografia

Adamski, A. (2000). *Prawo karne komputerowe*. Warszawa: C.H. Beck.

Bakalarczyk-Burakowska, K., Ciekanowski, Z. (2019). Cyberprzestępczość jako współczesne zagrożenie. *Edukacja dla Bezpieczeństwa 42*(1), 159–168.

Borecka, J. (2006). Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych. *Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie 4*, 5–14.

Cho, H., Rivera-Sánchez, M., Lim, S.S. (2009). A Multinational Study on Online Privacy: Global Concerns and Local Responses. *New Media & Society 11*(3), 395–416.

FBI. *Common Internet of Things Devices May Expose Consumers to Cyber Exploitation*. Pobrane z: https://www.ic3.gov/media/2017/171017-1.aspx (01.12.2021).

FBI. *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*. Pobrane z: https://www.ic3.gov/media/2019/191002.aspx (30.11.2021).

Interpol. *Global Cybercrime Strategy. Summary.* Pobrane z: https://www.interpol. int/content/download/5586/fi le/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB (2.12.2021).

Ministerstwo Cyfryzacji. *RODO Informator*. Pobrane z: https://www.gov.pl/documents/31305/436699/RODO.pdf/9b7e519b-0d5c-1ef8-4caf--02f8d247aa1d (01.12.2021).

Suchorzewska, A. (2010). *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*. Warszawa: Wolters Kluwer Polska.

Niniejszy dokument stanowi fragment podręcznika „Uniwersytet Odpowiedzialny. Edukacja w zakresie przedsiębiorczości cyfrowej. Podręcznik dla nauczycieli i rodziców” pod redakcją naukową dra Norberta Laurisza oraz dr Katarzyny Sanak-Kosmowskiej, Kraków 2021. Podręcznik został wydany przez Uniwersytet Ekonomiczny w Krakowie oraz Fundację Gospodarki i Administracji Publicznej.

Publikacja została opracowana w ramach projektu pt. Program Pilotażowy „Uniwersytet Odpowiedzialny” realizowanego przy wsparciu finansowym Województwa Małopolskiego.