

**SCENARIUSZ SZKOLENIA STACJONARNEGO – nr 14a**

Wersja 1.1

**MATERIAŁ WEWNĘTRZNY DLA TRENERÓW LOKALNYCH**

## **TYTUŁ SZKOLENIA: Dbam o swoje bezpieczeństwo w internecie- unikam zagrożeń**

Autorka: Renata Maciejczyk, trenerka centralna w obszarze Relacje z bliskimi

### **I. INFORMACJE PODSTAWOWE**

Obszar tematyczny: Relacje z bliskimi

Poziom: podstawowy

E-usługi, programy, narzędzia, których dotyczy szkolenie:

E- usługa:

- zarządzanie historią przeglądanych stron w przeglądarce internetowej
- trojany i wirusy
- zagrożenia w internecie
- instalacja nakładki blokującej niechciane treści
- usuwanie niechcianych wiadomości
- blokowanie niechcianego postu na portalu społecznościowym

Czas trwania: 120 minut

### **II. SZCZEGÓŁOWE CELE EDUKACYJNE**

W wyniku szkolenia uczestnik / uczestniczka:

a) Wiedza

- będzie wiedział/wiedziała, jakie są zagrożenia w internecie
- będzie znał/znała możliwości radzenia sobie z tymi zagrożeniami

- będzie wiedział/wiedziała, jak oddzielać chciane od niechcianych informacji

b) Umiejętności

- będzie potrafił/potrafiła zidentyfikować wirusy na Facebooku i Messengerze
- będzie potrafił/potrafiła ustawić, od kogo chce otrzymywać wiadomości na Facebooku
- będzie potrafił/potrafiła rozpoznać próbę oszustwa w wiadomości e-mail lub na portalu aukcyjnym
- będzie potrafił/potrafiła zainstalować nakładkę blokującą niechciane treści w przeglądarce

c) Postawa

- będzie miał/miała większą świadomość zagrożeń dla siebie i swojego dziecka, na jakie może natrafić w internecie
- będzie świadomy/świadoma, w jaki sposób radzić sobie z tymi zagrożeniami
- będzie miał/miała większą gotowość do używania dodatkowych narzędzi instalowanych w przeglądarce

Lista kompetencji uczestnika / uczestniczki z „Podstawowego katalogu kompetencji cyfrowych” rozwijanych podczas szkolenia:

(2.4.1) potrafię dbać o wizerunek i prywatność w internecie (własne oraz innych osób)

(2.4.2) potrafię śledzić informacje, które pozostawiam w internecie

(4.1.1) potrafię chronić mój komputer lub smartfon lub tablet przed zagrożeniami np. przy pomocy haseł, programów antywirusowych

Lista kompetencji uczestnika / uczestniczki z „Ramowego katalogu kompetencji cyfrowych” rozwijanych podczas szkolenia:

(2.3.1) potrafię zadbać o swoje bezpieczeństwo w internecie poprzez korzystanie z haseł, zapór sieciowych (Firewall), programów antywirusowych (4.1.1)

(2.3.2) potrafię zadbać o swoje bezpieczeństwo w internecie poprzez rozpoznawanie i unikanie różnych zagrożeń (np. phishing, niezabezpieczone połączenia, odbieranie wiadomości od nieznanych adresatów) (4.1.1)

(2.4.3) umiem rozpoznać zagrożenia związane z obiegiem informacji w internecie (reagować na niepożądane treści, ograniczać ryzyko związane z publikacjami naruszającymi dobre imię innych osób) (2.4.1, 2.4.2)

Krótki opis zakładanych korzyści, jakie osoba uczestnicząca odniesie dzięki posługiwaniu się e-usługami omawianymi na szkoleniu:

Po zakończeniu szkolenia osoba uczestnicząca będzie: znała zagrożenia, czyhające na nią w internecie, pozna najpopularniejsze wirusy, dowie się, na czym polegają internetowe oszustwa, a także w jaki sposób je rozpoznawać, czym grozi wejście w zainfekowany link na Facebooku lub Messengerze. Będzie potrafiła stosować dodatkowe narzędzia ograniczające niechciane treści w przeglądarce.

W szczególności będzie:

- wiedziała, jakie są zagrożenia w internecie?
- dlaczego warto ustawiać silne hasła?
- znała fachowe słownictwo dotyczące oszustw internetowych
- umiała odróżnić fałszywe od prawdziwych wiadomości e-mailowe oraz domeny
- umiała zainstalować wtyczkę AdBlock do przeglądarki Google Chrome

### III. WARUNKI UDZIAŁU UCZESTNIKA / UCZESTNICZKI W SZKOLENIU

Szkolenie jest skierowane do osób, które mają podstawowe umiejętności komputerowe – na poziomie szkolenia „Pierwsze kroki z komputerem” oraz chcą pogłębić swoją wiedzę na temat bezpieczeństwa w Internecie.

### IV. POTRZEBNE ZASOBY

Sprzęt komputerowy – minimalne wymagania:

- a) przeglądarka internetowa: Google Chrome/Mozilla Firefox
- b) telefon/smartfon lub tablet
- c) Rzutnik, komputer i ekran dla trenera/trenerki

Oprogramowanie – minimalne wymagania:

- d) Open Office lub Microsoft Office

Internet - minimalne wymagania:

- e) Szkolenie nie wymaga szczególnego transferu danych czy szybkości, minimalna prędkość danych 2 Mb/s

Materiały papiernicze:

- f) Materiały do pisania (notowania) dla osób uczestniczących, post-ity i mazaki do wykorzystania przez trenera/trenerkę (dwa post-ity na osobę, jeden mazak na osobę)

Inne materiały:

- g) Prezentacja multimedialna

### V. RAMOWY SCENARIUSZ SZKOLENIA

Scenariusz – jest pomyślany jako wskazówka przy prowadzeniu szkolenia; opis początku i zakończenia szkolenia należy każdorazowo dostosować do sytuacji danej grupy. W scenariuszach są one opisane w sposób, który pozwala przeprowadzić szkolenie dla grupy, której uczestnicy nie brali dotychczas udziału w innych szkoleniach w ramach projektu, nie znają się. W grupach, dla których to szkolenie jest kolejnym a tym bardziej, gdy uczestniczą w tym samym dniu w więcej niż 2-godzinny szkoleniu – obie części, a przynajmniej rozpoczęcie należy odpowiednio skrócić / uprościć.

Rekomendujemy jednakże, aby nie eliminować zawierania tzw. kontraktu (zasad pracy na szkoleniu), przedstawienia celów szkolenia, a także elementu ewaluacji – choć mogą być bardzo skrócone. W części głównej szkolenia we wszystkich scenariuszach zostało zaproponowanych na tyle dużo ćwiczeń, aby wypełniły one dodatkowy czas. Można także posłużyć się materiałami z części X, aby dopełnić treści szkolenia w przypadku grup, które dobrze sobie radzą z komputerem i wykonują zadania szybciej niż inni.

Czas trwania modułu	Moduł	Czas trwania poszczególnych zagadnień / ćwiczeń	Potrzebne materiały

15-20 min	<b>Początek szkolenia</b> 1. Przywitanie się trenera/trenerki, 2. Informacja trenera/trenerki o tym, że szkolenie jest realizowane w ramach projektu e-Mocni i współfinansowane ze środków UE 3. Przedstawienie się uczestników i zebranie oczekiwań wobec szkolenia podczas przedstawiania się (krótko o tym czego oczekują, co jest dla nich priorytetem na dziś) 4. Przedstawienie celów szkolenia oraz kontraktu pracy (można poinformować uczestników o zasadach pracy w grupie np.: pamiętaniu o wyciszeniu telefonu)? 5. Pre-test (wypełnienie)	20 minut	komputer, rzutnik, ekran  flipchart flamastry  małe karteczki
90 min	<b>Przebieg szkolenia</b> 1. <b>Budowanie świadomości na temat portali dla rodziców dostępnych w internecie</b> a) (burza mózgów) Jakiego znaczenia zagrożenia czyhające na Was lub Wasze dzieci w internecie? 2. <b>Jak wybrać odpowiedni portal?</b> a) (pogadanka) Trojany, wirusy, ataki hakerskie, phishing, pharming, czynnik ludzki, ochrona dzieci i młodzieży 3. <b>Dekalog bezpiecznego internetu</b> a) ćwiczenie – Flipchart – wypisanie zasad przez uczestników b) podanie dekalogu bezpiecznego internetu 4. <b>Oszustwa w serwisach aukcyjnych i wiadomości nieznanego pochodzenia</b> a) omówienie oszustw w serwisach aukcyjnych b) podszywanie pod bank c) oznaki podejrzanych wiadomości d) ćwiczenie – czym charakteryzuje się podejrzana strona internetowa? e) ćwiczenie – czym charakteryzuje się fałszywa reklama? f) ćwiczenie – czym charakteryzuje się podejrzana aplikacja? 5. <b>Wirusy na Facebooku i w Messengerze</b> a) omówienie rodzajów wirusów na Facebooku i Messengerze b) omówienie, jak reagować c) objawy zainfekowania konta d) blokowanie niechcianych wiadomości na Facebooku	5 minut          10 minut          25 minut          35 minut          25 minut	komputer, rzutnik, ekran
10-15 min	<b>Zakończenie szkolenia</b> Mini-ewaluacja.	Cała część – 15 minut	

	Krótką rundka wśród OU z pytaniem: „Wy już znacie zasady jak dbać o swoje bezpieczeństwo w Internecie. A jak zachęcicie swoich bliskich i rodzinę, by też korzystali niego bezpiecznie i unikali zagrożeń?	5 minut	
		5 minut	
	Post-test (wypełnienie)	5 minut	
	Rozdanie zaświadczeń i pożegnanie		

## VI. OPIS ĆWICZEŃ DO PRZEPROWADZENIA I WSKAZÓWKI METODOLOGICZNE

Głównym celem tego szkolenia jest przekazanie uczestnikom, na jakie zagrożenia są narażeni w internecie, jak minimalizować ryzyko, jak reagować na szkodliwe treści, w jaki sposób filtrować wiadomości na Facebooku oraz jak dostosować przeglądarkę do filtrowania niechcianych treści.

### Ćwiczenie nr 1

Cel ćwiczenia:

#### **Stworzenie dziesięciu zasad bezpiecznego internetu**

Przebieg ćwiczenia:

- Pytanie prowadzącego/ prowadzącej o zasady, dotyczące bezpiecznego internetu
- Utworzenie listy dziesięciu zasad bezpiecznego internetu przez uczestników (trener, może mieć przygotowaną listę lub skorzystać z gotowej listy (slajdy 22 – 31 w prezentacji) lub z materiału dodatkowego [http://domowykodeks.pl/kampania dla rodziców i dzieci Fundacji " dba o mój zasięg "](http://domowykodeks.pl/kampania_dla_rodzicow_i_dzieci_fundacji_dba_o_moj_zasieg). Wspólne tworzenie domowego kodeksu używania mediów cyfrowych. Tworzenie zasad korzystania ze smartfonów i innych urządzeń mobilnych
- Omówienie zasad

Czas ćwiczenia: około 25 minut

### Ćwiczenie nr 2

Cel ćwiczenia:

**Rozpoznawanie zagrożeń** – podejrzana strona internetowa, fałszywa reklama, podejrzana aplikacja (slajd 33- 42 w prezentacji )

Przebieg ćwiczenia:

- Próba ustalenia przez uczestników, czym jest podejrzana strona internetowa i jakie są jej cechy
- Odpowiedź np. „Adres jest niepoprawny lub niepełny; Strona ma słabej jakości tekst i obrazki; Adres nie zaczyna się od „https:/" (więcej odpowiedzi slajd 38)
- Próba ustalenia przez uczestników, czym jest fałszywa reklama i jakie są jej cechy
- Odpowiedź np. „Reklamowanie przypomina spam – ten sam link publikowany jest w wielu komentarzach; Nieprawdopodobnie zaniżona wartość sprzedawanego towaru” (więcej odpowiedzi slajd 40)
- Próba ustalenia przez uczestników, czym jest podejrzana aplikacja i jakie są jej cechy
- Odpowiedź np. „Źródło pochodzenia aplikacji; Data opublikowania aplikacji” (więcej odpowiedzi slajd 42)

Czas trwania: ok. 35 minut

### Ćwiczenie nr 3

Cel ćwiczenia:

**Rozpoznawanie wirusów na Facebooku i Messengerze** (slajd 44-52 w prezentacji)

Przebieg ćwiczenia:

- Omówienie, czym charakteryzują się podejrzane posty i wiadomości na Facebooku, np. posty rozpoczynające się od słów „Nie uwierzysz, co zrobiła...; lub inne tzw. „clickbaity”, czyli posty mające na celu zainteresowanie użytkownika, a następnie przekierowanie do innej strony (np. „Nigdy nie zgadniecie z kim spotyka się...” lub „Czy jedzenie chleba może Cię zabić?”
- Omówienie najlepszej reakcji na takie posty i wiadomości (np. nieklikanie w podejrzane posty, nieodpisywanie na podejrzane wiadomości, nieodpisywanie do ludzi, których nie mamy w znajomych na Facebooku)
- Ustawienie blokowania treści od danej osoby na Facebooku:
- Zalogowanie się na swojego Facebooka
- Przejście do strony Ustawień (ikona strzałki w prawym górnym rogu)
- Wybranie z menu bocznego „Blokowanie”, a następnie dodanie danych (imię, nazwisko lub adres e-mail) do blokowanych osób)
- Kliknięcie w niebieski przycisk „Zablokuj”

Czas ćwiczenia: około 25 minut,

## **VII. SPECYFIKA SZKOLENIA W ZALEŻNOŚCI OD RODZAJU GRUPY WIEKOWEJ LUB SPOŁECZNO-ZAWODOWEJ, DO KTÓREJ SZKOLENIE JEST SKIEROWANE**

	<b>Grupa / uczestnicy</b>	<b>Specyfika szkolenia (metodyka, język, ćwiczenia, oprogramowanie itp.) (jeśli dotyczy)</b>
1.	18-34 lat	W trakcie szkolenia można szerzej omówić interesujące zagrożenia uczestników lub skupić się na jednym wybranym.
2.	35-43 lat	Uczestnicy mogą tylko wybrać jakie funkcje komunikatora będą im przydatne - i tym poświęcić więcej czasu
3.	44-65 lat	Osoby mogą w potrzebować więcej czasu w poszczególnych ćwiczeniach.
4.	> 65 lat	Więcej czasu na poszczególne ćwiczenia, używanie obrazowego języka
5.	Osoby z niskim wykształceniem	Nie dotyczy
6.	Osoby o niskich dochodach	Nie dotyczy
7.	Osoby mieszkające na wsi	Nie dotyczy

## **VIII. PYTANIA DO ANKIETY BADAJĄCEJ PRZYROST KOMPETENCJI UCZESTNIKÓW SZKOLENIA**

1. Które z wymienionych nie stanowi zagrożenia dla Twojego komputera?

- a) tzw. "wirusy"
- b) tzw. "bakterie"
- c) tzw. "trojany"

2. Jak powinien rozpocząć się adres bezpiecznej strony?

- a) http:/
- b) https://
- c) www:/

3. Kiedy na pewno osoba, która przesyła w Messengerze i na Facebooku zainfekowane treści otrzyma Twoją wiadomość?

- a) napiszę do niego/niej przez Messenger
- b) napiszę na jego/jej tablicy
- c) zadzwonię lub powiem jej/jemu osobiście

Prawidłowa odpowiedź: 1b, 2b, 3c.

## **IX. LISTA ZAGADNIEŃ OMÓWIONYCH NA SZKOLENIU**

1. Jakie są najpopularniejsze zagrożenia w internecie?
2. Jak ustawiać hasła i dlaczego często je zmieniać?
3. Charakterystyka podejrzanych stron internetowych
4. Charakterystyka fałszywych reklam
5. Charakterystyka podejrzanych aplikacji
6. Oszustwa na portalach aukcyjnych i poczcie elektronicznej
7. Blokowanie treści na Facebooku

## **X. MATERIAŁY DYDAKTYCZNE DLA UCZESTNIKÓW**

1. Prezentacja Power Point, którą trener / trenerka wyświetli uczestnikom podczas szkolenia:

2. Prezentacja Power Point z logo Unii Europejskiej i Funduszy Europejskich w wersji czarno-białej – do wydrukowania uczestnikom jako materiały (opcjonalnie).

3. Materiał typu „jeśli chcesz wiedzieć więcej”:

<https://www.shopalike.pl/nie-daj-sie-oszukac-w-sieci/> strona zawierająca informacje jak nie dać się oszukać w sieci( infografiki)

<https://www.cyfrowobezpiecni.pl/strefa-ucznia>. Informacje, filmy edukacyjne o cyfrowym bezpieczeństwie dziecka i ucznia

<https://panoptykon.org/wiadomosc/dzieci-w-cyfrowym-swiecie-> materiały edukacyjne dla dziecka, rodzica z zakresu bezpieczeństwa i zagrożeń cyfrowych

[https://fundacja.orange.pl/files/user\\_files/user\\_upload/materiały\\_edu\\_dla\\_nauczycieli/Poradnik Bezpieczne media/Bezpieczne media. Przewodnik dla rodzicow..pdf](https://fundacja.orange.pl/files/user_files/user_upload/materiały_edu_dla_nauczycieli/Poradnik_Bezpieczne_media/Bezpieczne_media._Przewodnik_dla_rodzicow..pdf)

[https://fdds.pl/baza\\_wiedzy/bezpieczenstwo-dziecka-sieci/](https://fdds.pl/baza_wiedzy/bezpieczenstwo-dziecka-sieci/) materiały edukacyjne o zagrożeniach w cyfrowym świecie

<http://domowykodeks.pl/> kampania dla rodziców i dzieci Fundacji " dba o mój zasięg ". Wspólne tworzenie domowego kodeksu używania mediów cyfrowych. Tworzenie zasad korzystania ze smartfonów i innych urządzeń mobilnych

<https://www.kaspersky.pl/kaspersky-free> - Kaspersky Free to darmowa wersja popularnego antywirusa firmy Kaspersky Lab oferująca skuteczny skaner plików, witryn internetowych oraz poczty. Względem płatnej edycji program pozbawiony został między innymi kontroli rodzicielskiej oraz zabezpieczenia płatności internetowych



Scenariusz dostępny na licencji Creative Commons: Uznanie autorstwa 3.0. Polska. Pewne prawa zastrzeżone na rzecz Fundacji Rozwoju Społeczeństwa Informacyjnego i autorów. Zezwala się na dowolne wykorzystanie materiałów w tym utworów, tworzenia i rozpowszechniania ich kopii w całości lub we fragmentach, wprowadzania zmian i rozpowszechniania utworów zależnych - pod warunkiem zachowania niniejszej informacji licencyjnej i wskazania autorów oraz FRIS jako właścicieli praw do tekstu. Tekst licencji dostępny na stronie: <https://creativecommons.org/licenses/by/3.0/pl/>.