SCENARIUSZ SZKOLENIA STACJONARNEGO – nr 7a
Wersja 1.1

MATERIAŁ DLA TRENERÓW LOKALNYCH

TYTUŁ SZKOLENIA: Bezpieczeństwo w sieci - realne zagrożenia i rola oprogramowania.

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:

Budowanie swojego bezpieczeństwa w sieci

- Strona producenta programu antywirusowego Avast https://www.avast.com/pl-pl/free-antivirus-download-
- Poradnik instalowania programu Avast https://support.avast.com/pl-pl/article/Install-Free-Antivirus
- Poradnik online programu antywirusowego Avast https://www.youtube.com/watch?v=7tqlTP26gvE

Czas trwania: 120 minut

II. SZCZEGÓŁOWE CELE EDUKACYJNE

W wyniku szkolenia uczestnik/uczestniczka:

a) Wiedza

- będzie wiedział/wiedziała, co to jest antywirus i do czego jest potrzebny
- będzie znał/znała potencjalne zagrożenia jakie wynikają z korzystania z usług dostępnych w Internecie i konsekwencje braku lub nieodpowiedniego zabezpieczenia urządzeń wykorzystywanych do dostępu do tych usług
- będzie znał/znała podstawowe strategie reagowania na potencjalnie ryzykowne sytuacje w internecie

- będzie wiedział/wiedziała, że nie należy instalować na komputerze oprogramowania którego pochodzenia nie zna

b) Umiejętności

- będzie potrafił/potrafiła zidentyfikować sytuacje stanowiące zagrożenie dla nich komputerów
- będzie potrafił/potrafiła zainstalować przykładowe bezpłatne oprogramowanie antywirusowe
- będzie potrafił/potrafiła rozpoznać próby wyłudzenia informacji lub próby włamania do komputera
- będzie mógł/mogła zminimalizować niebezpieczeństwa, które mogą spotkać go w Internecie

c) Postawa

- będzie miał/miała większą świadomość zagrożeń płynących z instalowania nieznanego oprogramowania
- będzie potrafił/potrafiła wykorzystać popularne sposoby zabezpieczania urządzeń i programów
- będzie miał/miała większa gotowość do korzystania z e-narzędzi związanych z bezpieczeństwem w sieci

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

(1.1.1) potrafię korzystać z co najmniej jednej przeglądarki internetowej

(1.1.2) umiem wyszukiwać informacje online za pomocą co najmniej jednej wyszukiwarki internetowej

(1.2.1) potrafię sprawdzać i oceniać wiarygodność informacji w internecie

(2.2.2) umiem pobierać z internetu różne informacje i treści

(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)

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

Po zakończeniu szkolenia osoba uczestnicząca będzie: wiedziała co to jest program antywirusowy i do czego jest potrzebny?, potrafiła zainstalować przykładowy bezpłatny program antywirusowy oraz będzie umiała zidentyfikować sytuacje stanowiące zagrożenie dla ich komputerów.

Ponadto będzie znała potencjalne zagrożenia jakie wynikają z korzystania z usług dostępnych

w Internecie i konsekwencje braku zabezpieczenia lub nieodpowiedniego zabezpieczenia urządzeń wykorzystywanych do dostępu do tych usług.

III. WARUNKI UDZIAŁU UCZESTNIKA / UCZESTNICZKI W SZKOLENIU

Szkolenie jest skierowane do osób, które mają podstawowe umiejętności komputerowe – na poziomie szkolenia „Pierwsze kroki z komputerem".

IV. POTRZEBNE ZASOBY

Sprzęt komputerowy – minimalne wymagania:

- Komputer z dostępem do Internetu
- przeglądarka internetowa: Google Chrome/Mozilla Firefox
- Rzutnik, komputer i ekran dla trenera/trenerki

Oprogramowanie – minimalne wymagania:

- Windows10
- 2GB wolnego miejsca na dysku

Internet - minimalne wymagania:

- Szkolenie nie wymaga szczególnego transferu danych czy szybkości, minimalna prędkość danych 2Mbp/s

Materiały papiernicze:

- 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:

- Prezentacja multimedialna

V. RAMOWY SCENARIUSZ 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-godzinnym 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**
20 min	**Początek szkolenia** 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	**Przebieg szkolenia** 1. **Zagrożenia w sieci. Popularne i skuteczne sposoby zapewnienia bezpieczeństwa w cyberprzestrzeni** a) (burza mózgów) jakie państwo znacie zagrożenia w sieci? Jakie państwo znacie sposoby zabezpieczenia przed zagrożeniami w Internecie? Pogadanka. b) prowadzący podsumowuje dyskusje i podaje najbardziej popularne i skuteczne sposoby zapewnia bezpieczeństwa w cyberprzestrzeni c) Kto posiada oprogramowanie antywirusowe, aktualizuje oprogramowanie czy konfiguruje aplikacje? Co wiecie na ten temat? <u>Mini-wykład</u> 2. **Zapoznanie z oprogramowaniem zwiększającym bezpieczeństwo w sieci** a) czym jest antywirus? I po co jest potrzebny? b) darmowe programy antywirusowe- ranking programów	20 minut 20 minut	komputer, rzutnik, ekran

	c) o czym należy pamiętać przy korzystaniu z programów antywirusowych? **3. Instalacja bezpłatnego programu antywirusowego Avast Free Antivirus** a) pobranie i instalacja programu Avast i zapisanie jej w znanej lokalizacji na komputerze b) zapoznanie się z Polityką prywatności Avast c) rejestracja programu Avast **4**. **Włączanie lub wyłączanie Zapory systemu Windows** a) co to jest zapora Windows i czemu służy? b) włączanie Zapory Windows c) Wyłączanie Zapory Windows	30 minut 20 minut	
10-15 min	**Zakończenie szkolenia** Mini-ewaluacja. Krótka rundka wśród OU z pytaniem: „Wy już znacie sposoby zabezpieczenia przed zagrożeniami w Internecie? Jakim program antywirusowy możecie polecić znajomym? Post-test (wypełnienie) Rozdanie zaświadczeń i pożegnanie	Cała część – 15 minut 5 minut 5 minut 5 minut	

VI. OPIS ĆWICZEŃ DO PRZEPROWADZENIA I WSKAZÓWKI METODOLOGICZNE

Głównym celem tego szkolenia jest zapoznanie osób uczestniczących w nim z potencjalnymi zagrożeniami jakie wynikają z korzystania z usług dostępnych w Internecie oraz z konsekwencjami braku lub nieodpowiedniego zabezpieczenia urządzeń wykorzystywanych do dostępu do tych usług.

W czasie szkolenia uczestnik dowie się, że nie należy instalować na komputerze oprogramowania którego pochodzenia nie zna. Pozna programy antywirusowe i będzie umiał zainstalować przykładowy bezpłatny program antywirusowy.

Podczas szkolenia proponowane jest wykorzystanie następujących metod: burza mózgu, mini wykład, praca indywidualna, prezentacja.

Prezentacja ma znaczenie typowo pomocnicze dla trenerek / trenerów lokalnych (TL), zawiera treści dotyczące wprowadzenia do szkolenia, informacje o projekcie, celach szkolenia, kolejnych krokach w ćwiczeniach. Można ją też wykorzystać jako drukowany materiał dla osób uczestniczących, dzięki któremu będą mogli samodzielnie przypomnieć sobie treści ze szkolenia, co jest ważne szczególnie w przypadku osób stawiających pierwsze kroki z e-usługami.

Warto, by trener/trenerka przed szkoleniem zapoznali się z programami antywirusowymi i przetestowali poszczególne zadania proponowane uczestnikom na sobie tak, aby podczas wykonywania zadań mogli podzielić się swoją wiedzą i doświadczeniem.

Podczas wykonywania ćwiczeń można pokazać uczestnikom pobieranie i instalację dowolnego bezpłatnego programu antywirusowego.

Ćwiczenie nr 1

Cel ćwiczenia:

Programy antywirusowe- czym jest antywirus? i po co jest potrzebny? (mini wykład)

Celem ćwiczenia jest zapoznanie uczestników z podstawowa wiedzą na temat programów antywirusowych.

Przebieg ćwiczenia:

a) Oprogramowanie antywirusowe, w dużym uproszczeniu, wykrywa, a następnie uniemożliwia złośliwym programom (określanym jako „wirusy") dostanie się do systemu komputera, a także rozbraja je i usuwa, gdy wykryje, że dany system jest zainfekowany.

Antywirus stanowi pierwszy krok do zabezpieczenia komputera czy laptopa. Głównym zadaniem oprogramowania antywirusowego jest uniemożliwienie złośliwemu oprogramowaniu zainstalowania się na komputerze użytkownika lub zaatakowanie systemu operacyjnego.

Aby zapobiec zainfekowaniu urządzenia, należy zainstalować odpowiedni program antywirusowy, a następnie regularnie go aktualizować. Antywirusy rozpoznają podejrzane zachowania i ostrzegają użytkownika.

b) Darmowe programy antywirusowe- przykłady

- Avira Free Security Suite 2017
- Panda Free Antivirus 2017
- Avast Free Antivirus 2017
- AVG AntiVirus FREE 2017, Microsoft Security Essentials, Agnitum, BitDefender, ClamAV.

(Przykłady programów antywirusowych oraz znajdująca się powyżej porada dotycząca wersji demonstracyjnych i testowych, pochodzą z publikacji: „Bezpieczeństwo informatyczne szkół i instytucji publicznych – poradnik" - https://ipsec.pl/files/ipsec/bezpieczenstwo_informatyczne_szkol_i_instytucji_publicznych_-_poradnik.pdf

c) Płatne program antywirusowe - przykłady

- Bitdefender Total Security 2018
- Norton Security Deluxe 2017
- Kaspersky Total Security 2017
- G Data Internet Security 2017

d) dodatkowo przy korzystaniu z programu antywirusowego należy pamiętać o :

- ciągłej aktualizacji bazy wirusów komputerowych, można ustawić funkcje automatycznej aktualizacji
- korzystanie tylko z jednego programu antywirusowego, gdyż korzystanie więcej niż jednego programu na jednym komputerze może spowodować zakłócenia.

- instalacja oprogramowania tylko ze sprawdzonych źródeł.
- warto mieć taki program antywirusowy, który potrafi również skanować dołączane do Twojego komputera zewnętrzne nośniki pamięci, np.: na pendrivach.
- Nie używaj na stałe wersji demonstracyjnych i testowych. Testowe (evaluation, trial) wersje nawet najlepszych antywirusów po okresie testowym często wyłączają funkcje aktualizacji. Antywirus bez aktualizacji jest bezużyteczny. Jeśli nie możesz kupić pełnej wersji, wybierz produkt, który z założenia jest darmowy. Jeśli podejmujesz decyzję o zakupie, kieruj się wynikami niezależnych testów skuteczności, np. AV Comparatives, AV-Test, Virus Bulletin

Czas ćwiczenia: około 15 minut,

Ćwiczenie nr 2

Instalacja bezpłatnego programu antywirusowego np. Avast Free Antivirus

Cel ćwiczenia jest pobranie i zainstalowanie bezpłatnego programu antywirusowego np. Avast

Przebieg ćwiczenia:

Aby zainstalować program Avast na komputerze wykonaj następujące czynności:

a) Przejdź na stronę https://www.avast.com/pl-pl/free-antivirus-download- i wciśnij enter

b) Pobierz program ze strony producenta **Pobierz program**

c) Gdy plik zostanie pobrany kliknij na niego i rozpocznij instalacje.

d) Kolejne kroki potwierdzamy poleceniem **Dalej**

e) Kliknij przycisk **gotowe,** by zakończyć instalacje i zapisz go w znanej lokalizacji na komputerze (np. na pulpicie)

f) Kliknij prawym przyciskiem myszy pobrany plik instalacyjny avast_free_antivirus_setup_offline.exe i z menu kontekstowego wybierz polecenie **Uruchom jako administrator**.

g) Jeśli pojawi się okno dialogowe **Kontrola konta użytkownika** z pytaniem o pozwolenie, kliknij przycisk **Tak** (lub przycisk **Kontynuuj**).

h) Kliknij przycisk **Zainstaluj**, aby przeprowadzić instalację domyślną.

i) Kliknij przycisk **Kontynuuj**.

j) zapoznaj się z Polityką prywatności Avast i kliknij opcję **Kontynuuj**.

k) Program **Avast Free Antivirus** zostanie zainstalowany na komputerze i będzie gotowy do użycia. Interfejs użytkownika programu Avast można otworzyć, klikając ikonę Avast na pasku zadań lub na pulpicie systemu Windows.

Warto wiedzieć: Aby zarejestrować swój program Avast Free Antivirus, przejdź do opcji **Ustawienia** ▸ **Subskrypcja** i kliknij opcję **Zarejestruj się teraz**. W najnowszej wersji programu Avast podczas rejestracji nie jest wymagane podawanie danych kontaktowych.

Czas ćwiczenia: około 25 minut.

Ćwiczenie nr 3

Włączanie lub wyłączanie Zapory systemu Windows (dotyczy Windows 10)
Celem ćwiczenia jest włączenie lub wyłączanie Zapory systemu Windows 10

Przebieg ćwiczenia:

Zapora Windows to moduł ochronny pełniący rolę systemowego firewalla, czyli zapory sieciowej. Jest on odpowiedzialny za filtrowanie całego ruchu sieciowego i ewentualne blokowanie ataków zdalnych na dany komputer. Zapora nie jest pojedynczym programem, lecz rozbudowanym podsystemem ochronnym, do którego dostęp możemy uzyskiwać poprzez Panel sterowania albo poprzez odrębną aplikację dającą dostęp do zaawansowanych funkcji systemowej zapory sieciowej

Zapora systemu Windows powinna być zawsze uruchomiona, nawet jeśli włączono również inną zaporę. Wyłączenie Zapory systemu Windows powoduje, że urządzenie (i ewentualna sieć lokalna) jest bardziej podatna na zagrożenia związane z nieautoryzowanym dostępem. Aby włączyć lub wyłączyć Zaporę systemu Windows:

a) Naciśnij przycisk **Start** i wybierz kolejno opcje **Windows Defender Security Center** > **Zapora i ochrona sieci**.

b) Wybierz profil sieciowy, a następnie w obszarze **Zapora systemu Windows** włącz lub wyłącz zaporę.
Czas ćwiczenia: około 20 minut,

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

	Grupa / uczestnicy	**Specyfika szkolenia (metodyka, język, ćwiczenia, oprogramowanie itp.)** (jeśli dotyczy)
1.	18-34 lat	W trakcie szkolenia należy podkreślić, że jest wiele programów antywirusowych i dostosować szkolenie do potrzeb uczestników.
2.	35-43 lat	Uczestnicy mogą tylko takie zabezpieczenia przed zagrożeniami jakie będą im przydatne, i tym poświęcić więcej czasu.
3.	44-65 lat	Osoby mogą potrzebować więcej czasu na wyjaśnienie słownictwa i porozmawiać o tym jakich zagrożeń sami doświadczyli.
4.	>65 lat	Więcej czasu na poszczególne ćwiczenia, używanie obrazowego języka
5.	Osoby z niskim wykształceniem	Bardzo obrazowe słownictwo, metaforyczne.
6.	Osoby o niskich dochodach	Nie dotyczy
7.	Osoby mieszkające na wsi	Nie dotyczy

VIII. PYTANIA DO ANKIETY BADAJĄCEJ PRZYROST KOMPETENCJI UCZESTNIKÓW SZKOLENIA

1. Jaki symbol w pasku adresu potwierdza, że połączenie jest bezpieczne?

a) czerwony wykrzyknik

b) zielona kłódka

c) zielony trójkąt

2. Który z poniższych programów jest programem antywirusowym?

a) Internet Explorer

b) Avast Free Antivirus

c) Adobe Reader

3. Z jakiej strony najlepiej pobrać i zainstalować program antywirusowy?

a) ze strony producenta

b) z dowolnej strony

c) ze strony podanej od znajomego

Prawidłowa odpowiedź: 1b, 2b, 3a,

IX. LISTA ZAGADNIEŃ OMÓWIONYCH NA SZKOLENIU

1. Zagrożenia w sieci. Popularne i skuteczne sposoby zapewnienia bezpieczeństwa w cyberprzestrzeni
2. Zapoznanie z oprogramowaniem zwiększającym bezpieczeństwo w sieci
3. Programy antywirusowe- czym jest antywirus? i po co jest potrzebny?
4. Instalacja bezpłatnego programu antywirusowego np. Avast Free Antivirus
5. Włączanie lub wyłączanie Zapory systemu Windows

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. Materiały edukacyjne - zrzuty ekranowe (printscreen) dot. danej e-usługi.

Ćwiczenie 2.

Instalacja bezpłatnego programu antywirusowego np. Avast Free Antivirus

4. Materiały typu „jeżeli chcesz wiedzieć więcej"

1. Opis 10 najlepszych programów antywirusowych do pobrania na komputery z Windowsem http://www.benchmark.pl/testy_i_recenzje/darmowe-programy-antywirusowe.html
2. Ranking najlepszych antywirusów 2018 - darmowych i płatnych programów antywirusowych na peceta, laptopa lub tablet https://www.pcworld.pl/ranking/Najlepszy-antywirus-2018-Oto-ranking-top-15-antywirusow-antywirusow-
4. Darmowe-i-platne-programy,406168.html
5. „Bezpieczeństwo informatyczne szkół i instytucji publicznych – poradnik" – https://ipsec.pl/files/ipsec/bezpieczenstwo_informatyczne_szkol_i_instytucji_publicznych_-_-

   _poradnik.pdf
6. Instrukcja aktywowania programu Avast Free https://support.avast.com/pl-pl/article/9

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 FRSI jako właścicieli praw do tekstu. Tekst licencji dostępny na stronie: https://creativecommons.org/licenses/by/3.0/pl/.