1.
Rodzic w internecie

Rodzic w internecie

Grupa docelowa uczestników Rodzice w wieku 25+, znający podstawy obsługi komputera.

Liczebność grupy szkoleniowej Maksymalnie 12 osób.

Cele szkolenia Przygotowanie rodziców:

1. do roli przewodnika dziecka w bezpiecznym i mądrym korzystaniu z internetu dzięki poznaniu bazy legalnych materiałów kulturalnych, rozrywkowych i edukacyjnych dostępnych w sieci oraz znajomości źródeł wiedzy dostępnych na otwartych licencjach, by jak najlepiej wykorzystywać internet w edukacji i rozwoju dziecka,
2. do reagowania na sytuacje zagrożenia dzięki umiejętnościom zabezpieczania dziecka przez niepożądaną aktywnością w internecie oraz poznaniu metod nadzorowania aktywności za pomocą odpowiedniego oprogramowania,
3. do korzystanie z e-usług publicznych dostępnych dla rodziców, dzięki założeniu profil zaufanego i korzystaniu z usług platformy ePUAP.

Warianty realizacji szkolenia

Szkolenie trwa 12h i podzielone jest na moduły. Szkolenie może być realizowane w kilku wariantach: w trybie dwóch pełnych dni lub w podziale na moduły.

Wariant 1: Dwa pełne dni (każdy 6h), realizowane łącznie lub w rozbiciu 2 x 1 dzień. Dzień I: moduły 1-3 | dzień II: moduły 4-6.

Wariant 2: Trzy spotkania x 4 godziny. Spotkanie I: moduły 1-2 | spotkanie II: moduły 3-4 | spotkanie III: moduły 5-6.

Założenia

- Osoby uczestniczące (OU) potrafią obsłużyć komputer w stopniu podstawowym.
- Grupa szkoleniowa liczy maksymalnie 12 osób i może być prowadzona przez jednego instruktora (osobę prowadzącą – OP).
- Szkolenie powinno odbywać się w sali wyposażonej w liczbę stanowisk komputerowych odpowiadającą liczbie osób uczestniczących, z dostępem do szerokopasmowego internetu, rzutnik z ekranem lub tablicę multimedialną.

Materiały i przygotowanie (się) do szkolenia

1. Poznanie prezentacji szkoleniowej z najważniejszymi zagadnieniami i zasobami omawianymi przez całe szkolenie.
2. Przeczytanie kompendium „Bezpieczeństwo dzieci online".
3. Obejrzenie filmu dla instruktorów dot. scenariusza „Rodzic w internecie".
4. Obejrzenie filmu instruktażowego dla osób uczestniczących „Bezpieczne korzystanie z komputera i smartfona".
5. Założenie konta na mentimeter.com i skopiowanie ankiety „Rodzic w internecie" – link do ankiety.
6. Założenie konta e-PUAP i profilu zaufanego.
7. Wszystkie materiały szkoleniowe – prezentacje i filmy instruktażowe – dla osób prowadzących i osób uczestniczących znajdują się na stronie programu *Ja w internecie*: jawinternecie.edu.pl/strefaedukacji.

Przebieg szkolenia w podziale na moduły

1. Wprowadzenie do szkolenia

45 min. | 1-8

Krok 1. Przedstawienie się osoby prowadzącej i osób uczestniczących

Krok 2. Omówienie programu, przebiegu i zasad

Krok 3. Wypełnienie kwestionariusza osobowego

Krok 4. Wypełnienie pre-testu

2. Wyszukiwanie informacji i pomysłów na działania

3 godz. 15 min. | 9-26

Krok 1. Dzieci i młodzież w sieci – wprowadzenie (60 min.)

Krok 2. Wyszukiwanie wartościowych zasobów edukacyjnych, kultury i rozrywki (135 min.)

3. Bezpieczne korzystanie z komputerów i smartfonów

2 godz. | 27-47

Krok 1. Podstawy bezpieczeństwa komputera i korzystania z sieci (90 min.)

Krok 2. Bezpieczne korzystanie ze smartfonów (30 min.)

4. Reagowanie na zagrożenia i kontrola rodzicielska

2 godz. | 48-65

Krok 1. Korzystanie z sieci i smartfonów przez dzieci i młodzież (40 min.)

Krok 2. Rozpoznawanie i reagowanie na zagrożenia oraz dobre praktyki kontroli rodzicielskiej (80 min.)

5. E-usługi dla rodziców

3,5 godz. | 66-87

Krok 1. Informacje i programy dot. bezpieczeństwa dzieci w sieci, które powinni znać rodzice – wprowadzenie (60 min.)

Krok 2. Zakładania konta w ePUAP i profilu zaufanego (60 min.)

Krok 3. E-usługi dla rodziny (90 min.)

6. Zakończenie szkolenia

30 min. | 88-91

Krok 1. Podsumowanie szkolenia przez osobę prowadzącą i osoby uczestniczące

Krok 2. Wypełnienie ankiety ewaluacyjnej

Moduł 1.

45 min. 1-8

Wprowadzenie do szkolenia

Cele modułu

1. Poznanie się wzajemne osoby prowadzącej (dalej OP) i osób uczestniczących (dalej OU).
2. Zebranie danych osobowych od OU.
3. Określenie doświadczenia i poziomu kompetencji cyfrowych OU (pre-test).
4. Prezentacja programu i przebiegu szkolenia oraz zasad współpracy.

Przebieg

1. Przedstaw się i poproś OU o przedstawienie się oraz krótkie opowiedzenie o swojej motywacji i oczekiwaniach dotyczących szkolenia: dlaczego zdecydowałem/am się na udział w szkoleniu? Co jest dla mnie interesujące, na co liczę?
2. Odnieś się do oczekiwań OU omawiając plan szkolenia.
3. Przedstaw zasady współpracy prezentując slajdy.
4. Pokaż, gdzie OU znajdą wszystkie materiały omawiane podczas szkolenia, prezentując zakładkę „strefa edukacji" na stronie programu *Ja w internecie*. Link do materiałów: jawinternecie.edu.pl/strefaedukacji.
5. Przedstaw informacje dotyczące danych osobowych i poproś o wypełnienie kwestionariusza danych osobowych online. Link do kwestionariusza: jawinternecie.edu.pl/rejestracja.
6. Krótko omów sprzęt i oprogramowanie używane podczas szkoleń.
7. Na zakończenie pierwszego modułu poproś o wypełnienie pre-testu kompetencji (uruchomionego przed warsztatem na wszystkich komputerach osób uczestniczących). Link do strony, na której znajduje się pre-test: badania.koduj.gov.pl.

Uwagi

1. Możemy prosić o wypełnienie kwestionariusza jeszcze przed szkoleniem, w czasie, kiedy oczekujemy na zebranie się grupy. Zgoda na podanie danych i wypełnienie kwestionariusza jest **warunkiem koniecznym** uczestnictwa w szkoleniu. Jednocześnie wypełnianie kwestionariusza pozwoli zorientować się OP w umiejętnościach i kompetencjach OU w zakresie obsługi komputera i korzystania z przeglądarki.
2. Niezależnie od wariantu, w którym realizowane jest szkolenie (2 x 6 godz. lub 3 x 4 godz.), osoby uczestniczące wypełniają dane tylko na początku pierwszego spotkania.

Moduł 2.

3 godz. 15 min | 9-26

Wyszukiwanie informacji i zasobów w sieci

Cele modułu

1. Poznanie zaawansowanych opcji wyszukiwania informacji, zasobów i aktywności w sieci, które można polecać dzieciom.
2. Poznanie serwisów oferujących sprawdzone treści dla dzieci.
3. Użycie filtrów wyszukiwania.

Krok 1. Dzieci i młodzież w sieci – wprowadzenie

60 min. | 9-11

Instrukcja dla OP

Przed szkoleniem przygotuj cztery plakaty z pytaniami do zadania grupowego. Każdemu plakatowi nadaj tytuł – na górze plakatu zapisz jedno pytanie:

1. *Jakie szanse związane z internetem widzicie dla swoich dzieci?*
2. *Jakie zagrożenia związane z internetem widzicie dla swoich dzieci?*
3. *Czego potrzeba dzieciom, by lepiej zrozumiały rzeczywistość internetu?*
4. *Jakie tematy warto podejmować z dziećmi/młodzieżą w przyszłości?*

Po zakończeniu ćwiczenia zachowaj plakaty z odpowiedziami OU, przydadzą się jeszcze w Module 4.

Doświadczenie

1. Podziel uczestników na cztery 3-osobowe grupy i omów co będzie się działo. Każda grupa będzie miała pięć minut, żeby odpowiedzieć na pytanie na plakacie. Po upływie tego czasu, grupy wymieniają się plakatami i będą mieć kolejne pięć minut na następne pytanie i tak kolejno z każdym plakatem.
2. Każdej grupie rozdaj jeden plakat z zapisanym pytaniem. Poproś, by w ciągu pięciu minut uczestnicy wypisali na plakacie swoje odpowiedzi, refleksje, pomysły dotyczące tytułowego pytania. Zachęć do zapisywania zarówno ogólnych, jak i konkretnych pomysłów, np. nazw świetnego zasobu czy aktywności w sieci sprawdzonego dla dzieci.
3. Pilnuj czasu – kiedy minie pięć minut, poproś OU o zakończenie pisania i przekazanie plakatu sąsiedniej grupie.
4. Po zakończeniu procedury zaproś grupy, by przedstawiły krótko wyniki swojej pracy na forum, np. każda grupa prezentuje ten plakat, od którego zaczynała.

Refleksja

5. Nawiązując do wcześniejszej pracy, zapytaj OU, skąd wiedzą w jaki sposób ich dzieci korzystają z sieci i jak to kontrolują? Czy rozmawiają z dziećmi i wspólnie korzystają razem z nimi z sieci? Czy ustalają wspólnie zasady korzystania z komputera, smartfonu?
6. Na zakończenie tej części, wspólnie z OU podsumuj i zapisz na plakacie lub we wcześniej przygotowanym dokumencie Google Docs, propozycję kilku aktywności, o których chcą się dowiedzieć więcej i których podejmą się po szkoleniu, np. rozmowa z dzieckiem o bezpieczeństwie w sieci, wspólne spędzenie czasu na wyszukiwaniu i oglądaniu edukacyjnych filmów, zagranie z dziećmi w grę, którą lubią i porozmawianie o niej.

135 min. 12-26

Krok 2.
Wyszukiwanie zasobów i treści odpowiednich dla dzieci

Instrukcja dla OP

Zrób kopię dokumentu Google i przygotuj go do udostępnienia, z prawem do edycji dla OU [przykładowy dokument]. Do tej części warsztatu przygotuj również tablet, smartfon lub upewnij się, że OU mają przynajmniej jedno urządzenie na cztery osoby do wykorzystania w trakcie spotkania.

Doświadczenie

1. Zapytaj OU w jakim wieku są ich dzieci oraz pod jakim kątem wybierają strony i treści w sieci dla swoich dzieci? Na co zwracają uwagę? Zbierz odpowiedzi i podkreśl, że w tej części będą mieli okazję poznać kilka serwisów, które przydatne są dla dzieci w różnym wieku.
2. Poproś OU o otworzenie w przeglądarce internetowej adresu dokumentu Google Docs, na którym będą pracować. Wyjaśnij podstawowe funkcje edytora zwracając uwagę na możliwość jednoczesnej współpracy i edycji przez wiele osób.
3. Pokaż, gdzie w przygotowanym dokumencie Google Docs jest gotowe miejsce na treści dla różnych kategorii wiekowych.
4. Następnie poproś o odnalezienie we wskazanych serwisach ciekawych i wartościowych treści dla dzieci. OU szukają w serwisach:
   - lekcji wideo z matematyki na kanale Khan Academy na YouTube (w polskiej wersji językowej) na poziomie szkolnym adekwatnym do wieku dzieci OU,
   - materiałów dot. bezpieczeństwa w sieci odpowiedniego dla wieku dzieci, który można będzie polecić nauczycielom w szkole,
   - gry, która pomaga dzieciom w uczeniu się podstaw nauki liczenia,
   - w aplikacji mobilnej YouTube Kids wideo dla dzieci OU z grupy,
   - lektur szkolnych dla klas, w których są dzieci w grupie, w serwisie Wolne Lektury.

Refleksja

5. Omów i podsumuj doświadczenie OU. Dopytaj co budziło szczególne trudności, wyjaśnij wątpliwości dotyczące korzystania ze stron.

Prezentacja OP

6. Omów najważniejsze cechy i różnice działania wyszukiwarek w stronach, których dotyczyło zadanie.
7. Zaprezentuj możliwości włączania filtrów rodzinnych (*safe search*) w popularnych wyszukiwarkach:
   - Google, opcja wyszukiwania z włączonym filtrem *safe search*,
   - YouTube, opcja wyszukiwania z filtrem *safe search* oraz aplikacja YouTube Kids,
   - zwróć też uwagę na ograniczenia stosowania takich automatycznych filtrów, które bywają nieskuteczne wobec niektórych treści, a czasem są zbyt restrykcyjne i blokują treści odpowiednie dla dzieci np. edukacyjne.
8. Przedstaw porady dot. sprawdzania stron i aplikacji dla dzieci:
   - korzystanie z systemów oceny gier pod kątem wieku PEGI,
   - sprawdzanie recenzji w zaufanych miejscach, takich jak strona saferinternet.pl (po polsku) i commonsensemedia.org (po angielsku),
   - wyszukiwanie opinii na blogach i forach dla rodziców.

9. Przedstaw krótko ryzyka związane z wykorzystywaniem treści naruszających prawa autorskie:
   - naruszenie praw autorskich jest naruszeniem przepisów prawa cywilnego,
   - może wiązać się z usunięciem treści w sposób automatyczny np. na YouTube.
10. Podpowiedz jak i gdzie sprawdzać legalność źródeł:
   - baza legalnych źródeł na stronach Legalnej Kultury,
   - baza otwartych zasobów.

Zagadnienia i podstawowe umiejętności cyfrowe realizowane w Module 2.

1.1. Wyszukiwanie wartościowych treści dla dzieci i rodziców wraz z oceną wiarygodności źródeł informacji związanych z rozwojem zainteresowań, treści edukacyjne, zasoby kultury, gry komputerowe i gry online, strony instytucji publicznych, związanych ze zdrowiem, w tym na portalach, gdzie informacjami dzielą się inni użytkownicy.

1.2. Rozpoznawanie treści szkodliwych i niebezpiecznych dla dzieci i młodzieży oraz sposoby reagowania na nie, w tym znajomość oznaczeń wieku i treści w odniesieniu do stron internetowych, gier i aplikacji (w tym system PEGI).

1.3. Umiejętność odróżnienia źródeł treści legalnych od nielegalnych (film, muzyka, książki etc.) streaming, VOD, itp., pobieranie plików, aplikacje.

3.5. Nauka samodzielna i wspólna z dzieckiem z wykorzystaniem cyfrowych zasobów kultury i archiwów oraz źródeł internetowych (np. Wikipedia, TED, Khan Academy, Ninateka, POLONA).

Moduł 3.

2 godz. 27-47

Bezpieczne korzystanie z komputerów i smartfonów

Cele modułu

1. Poznanie podstawowych zasad bezpieczeństwa w sieci.
2. Umiejętność tworzenia mocnego hasła i zastosowania podstawowych zasad bezpieczeństwa w sieci.
3. Rozpoznawanie podstawowych zagrożeń typu atak phishingowy, połączenie z niebezpieczną lub nieszyfrowaną stroną.
4. Rozwój umiejętności oceny jakości i bezpieczeństwa aplikacji mobilnych.

90 min. 27-41

Krok 1.
Podstawy bezpieczeństwa komputera i korzystania z sieci

Doświadczenie

1. Poproś OU o sprawdzenie samodzielnie w serwisie Haveibeenpwned.com czy ich adresy mailowe i związane z nimi hasła padły ofiarą wycieków.
2. Zapytaj OU co należy zrobić w takiej sytuacji? W jaki inny sposób, niż hasło, można chronić dostęp do swoich danych w sieci?
3. Na koniec poproś OU, by jeśli posiadają konto w bankowości elektronicznej, poczcie Gmail lub Facebooku odnalazły informację o tym czy i w jaki sposób mogą uruchomić tzw. dwuetapową weryfikację, czyli dodatkowe, oprócz hasła, zabezpieczenie logowania się.

Prezentacja OP

4. Przedstaw OU na czym polega atak phishingowy i wyciek danych oraz omów konsekwencje tych ataków.
5. Następnie OU na podstawie prezentacji OP oceniają poziom zabezpieczeń w sieci jakie stosują. Zapytaj OU o następujące informacje:
   - Ile znaków ma ich hasło do poczty mailowej?
   - Czy zawiera wielkie i małe litery oraz cyfry i znaki specjalne?
   - Jak często zmieniają hasła?
   - Czy zdarzyło im się kiedyś stracić kontrolę nad dostępem do jakiejś usługi lub serwisu WWW?
   - Czy wiedzą co oznacza kłódka w pasku adresu przeglądarki?
   - Czy zdarza im się zainstalować program lub aplikację bez sprawdzenia dokładnie jak działa i czy jest bezpieczna?
   - Jak zabezpieczają swój komputer, a jakie zabezpieczenia stosują na smartfonach przed tym, aby nikt nie zyskał dostępu do danych na nich trzymanych?
6. Odpowiedzi na każde z pytań komentuj omawiając odpowiednie slajdy z sugestiami lepszego zabezpieczenia w danym zagadnieniu.

30 min. 42-47

Krok 2.
Bezpieczne korzystanie ze smartfonów

Prezentacja OP

1. Poproś OU o podanie przykładów informacji i danych, które przechowują na swoich telefonach, np. dostęp do poczty, zdjęcia dzieci, prywatne konwersacje w smsach itp.
2. Następnie poproś OU o podanie przykładów, w jaki sposób te informacje mogłyby wpaść w niepowołane ręce. Jeżeli OU mają kłopot z odpowiedzią przedstaw sposoby opisane na slajdzie nr 45:
   - utrata telefonu bez zabezpieczeń typu PIN,
   - wyciek danych z aplikacji (jak zaprezentowane na przykładzie haveibeenpwned i adresów mailowych),
   - podszycie się pod kogoś w celu uzyskania informacji (jak w przypadku ataków phishingowych),
   - awaria/błąd w oprogramowaniu lub urządzeniu (jak w przypadku niedawnej awarii telefonów Samsung, które samodzielnie wysyłały zdjęcia do osób z list kontaktów).

3. Po podsumowaniu sposobów utraty danych, zapytaj OU czy wiedzą, jakie treści znajdują się w smartfonach ich dzieci i czy, oprócz omówionych wcześniej zagrożeń, dotyczą ich jeszcze inne zagrożenia? Jeśli tak to jakie? Zaprezentuj slajd nr 46.
4. Przedstaw podstawowe aspekty działania współczesnego smartfonu. Możesz wykorzystać do tego jako pomoc infografikę „Co wie o mnie mój telefon" (slajd 47).
5. Przedstaw funkcje działania sklepów z aplikacjami na systemach iOS i Android oraz zasady dot. wybierania bezpiecznych aplikacji, oznaki ewentualnych zagrożeń, takich jak phishing, płatne połączenia.

Zagadnienia i podstawowe umiejętności cyfrowe realizowane w Module 3.

1.2. Rozpoznawanie treści szkodliwych i niebezpiecznych dla dzieci i młodzieży oraz sposoby reagowania na nie, w tym znajomość oznaczeń wieku i treści w odniesieniu do stron internetowych, gier i aplikacji (w tym system PEGI).

3.1. Umiejętność nadzorowania aktywności dziecka w sieci.

3.2. Wiedza na temat ogólnych zasad bezpieczeństwa, których powinno przestrzegać dziecko w internecie, w tym: sposoby reagowania na zagrożenia w sieci (hate, trolling, kradzież treści) i znajomość instytucji świadczących pomoc w zakresie przeciwdziałania zagrożeniom (np. telefon dla rodziców 800 100 100), tworzenie bezpiecznych haseł, logowanie się przez sprawdzone sieci WiFi etc., bezpieczne zarządzanie prywatnością w sieci, w tym publikowanie różnych treści przez rodziców i dzieci, dbałość o wizerunek dziecka w internecie.

3.3. Symptomy nadużywania internetu przez dziecko i reakcja na nie.

3.4. Uświadomienie dziecku sposobu i konsekwencji działania transakcji w internecie (zakupy, sprzedaż, zawieranie umów, płatności elektroniczne) oraz płatności wewnątrz aplikacji mobilnych. Odpowiedzialność prawna rodziców za postępowanie dziecka w internecie, prawa i obowiązki wynikające z regulaminów wybranych serwisów internetowych.

Moduł 4.

2 godz. 48-65

Reagowanie na zagrożenia i kontrola rodzicielska

Cele modułu

1. Zrozumienie różnic w sposobach komunikacji w sieci między dziećmi a dorosłymi.
2. Rozpoznawanie zagrożeń i sytuacji ryzykownych u dzieci w związku z korzystaniem z sieci.
3. Umiejętność poszukiwania pomocy w sytuacjach zagrożenia lub ryzyka.

40 min. 48-51

Krok 1.
Korzystanie z sieci i smartfonów przez dzieci i młodzież

Instrukcja dla OP

Zrób kopię ankiety na menti.com i uzupełnij aktualny kod dla OP na swojej prezentacji. Link do ankiety. Pytania do ankiety opracowano na podstawie raportu badawczego nt. wykorzystania sieci przez dzieci i młodzież.

Doświadczenie

1. Poproś OU o wypełnienie ankiety na menti.com na temat doświadczeń korzystania z sieci zarówno własnych, jak i swoich dzieci (znanych stron, wykorzystywanych komunikatorów, aplikacji).

Refleksja

2. Po zakończeniu ankiety zapytaj OU czy znają wszystkie serwisy i narzędzia wymienione w ankiecie?
3. Omów wyniki ankiety, prezentując zapytaj OU, czy coś ich zaskakuje w wynikach, jeżeli tak, to co?

Prezentacja OP

4. Przedstaw OU najważniejsze wyniki z raportu „Nastolatki w sieci 3.0" oraz badań Urzędu Komunikacji Elektronicznej na Dzień Bezpiecznego Internetu 2018:
   - zwróć uwagę na najważniejsze zjawiska i zmiany jakie występują w praktykach dzieci, młodzieży i rodziców,
   - podkreśl jak różnią się oceny rodziców odnośnie tego co dzieci faktycznie robią w sieci od deklaracji dzieci,
   - zwróć uwagę jak szybko wiele praktyk dzieci i dorosłych w sieci się zmienia i od czego to zależy, np. pojawienie się nowej aplikacji o specyficznych funkcjach jak Snapchat, Instagram, mody, czy nagłaśnianie w mediach marginalnych zachowań.

80 min. 52-65

Krok 2.
Rozpoznawanie i reagowanie na zagrożenia oraz dobre praktyki kontroli rodzicielskiej

Instrukcja dla OP

Wróć z OU do doświadczenia z pierwszego modułu, kiedy na plakatach OU analizowały szanse i zagrożenia związane z korzystaniem przez dzieci z internetu. Przypomnij zagrożenia, które OU wówczas wymieniły. Spośród wymienionych zagrożeń, jeśli się pojawiły, wybierz i doprecyzuj podane poniżej, te które dotyczą bezpośrednio korzystania z technologii. Do dalszej pracy podziel OU na trzy mniejsze grupy i przydziel każdej grupie jedno zagrożenie.

Doświadczenie

1. Podziel OU na trzy grupy, przydziel każdej grupie jedno zagrożenie:
   - nadużywanie internetu i gier komputerowych,
   - dostęp i korzystanie ze szkodliwych treści (np. pornografii),
   - udostępnianie danych osobowych i wizerunku.
2. Poproś, by w małej grupie wspólnie przedyskutowali i odpowiedzieli na pytania:
   - Jak rozpoznawać zagrożenie?
   - Jak rozmawiać o zagrożeniu z dzieckiem?
   - Jak reagować z pozycji rodzica, kiedy zagrożenie wystąpi?
3. Poproś o zaprezentowanie i podsumowanie wyników dyskusji na forum.

Refleksja

4. Omów odpowiedzi OU zwracając uwagę na różnorodne rozwiązania i granice dla różnych zachowań, które OU wskazały. W przypadku zagrożeń związanych z nadmiernym korzystaniem z sieci lub graniem w gry komputerowe dopytaj o to gdzie/kiedy stawiają dzieciom granice lub co uważają za „nadmierne" lub „uzależniające"?

Prezentacja OP

5. Omów slajdy klasyfikujące zagrożenia związane z nowymi technologiami, porady dotyczące ich rozpoznawania oraz przeciwdziałania im. Zwróć szczególną uwagę na te zagrożenia i zachowania, które mogą wymagać specjalistycznej pomocy. Zagrożenia do omówienia:
   - nieodpowiednie do wieku treści – filtry treści, kontrola rodzicielska,
   - materiały przedstawiające przemoc i wykorzystywanie dzieci – zgłaszanie treści, pomoc psychologiczna,
   - cyberprzemoc – gdzie szukać wsparcia, dyzurnet.pl,
   - seksting i wizerunek dziecka – gdzie szukać wsparcia, dyzurnet.pl,
   - mowa nienawiści (ang. *hate speach*) – dyzurnet.pl, zgłaszanie naruszeń do portali,
   - zagrożenia związane z grami – system PEGI, zasady dot. czasu, gry edukacyjne,
   - szkodliwe oprogramowanie – zabezpieczenia aplikacji i komputera,
   - ukryte koszty w aplikacjach – zabezpieczenia aplikacji i kontrola rodzicielska,
6. Przedstaw OU metody włączenia kontroli rodzicielskiej dla najmłodszych dzieci w urządzeniach mobilnych (Android i iOS) oraz na komputerach stacjonarnych (konta użytkowników z ograniczonymi uprawnieniami). Omów również rolę ustalania wspólnie zasad ze starszymi dziećmi jako ważnego sposobu zastępowania kontroli rodzicielskiej.

UWAGA!

Istnieje duże prawdopodobieństwo, że dyskusja o zagrożeniach wywoła wśród rodziców wiele emocji i burzliwą dyskusję. Rodzice mogą mieć różne poglądy na temat zagrożeń oraz sposobów radzenia sobie z nimi. Różnice te mogą wynikać z wielu różnych czynników, innych światopoglądów czy modeli rodzicielstwa. Potencjalnie może to być trudna sytuacja dla osoby prowadzącej. Dlatego warto od początku jasno określić swoją rolę. Pamiętaj, żeby stawiać się w roli przewodnika po świecie internetu, a nie doradcy ds. wychowywania dzieci. Unikaj oceniających komentarzy, prywatnych opinii jak „należy" postępować z dziećmi, kto jest dobrym rodzicem itp. Tam gdzie jest to możliwe powołuj się na wyniki badań lub wskazuj na specjalistyczne publikacje i instytucje, które zajmują się danym zagadnieniem. Podkreślaj, że żadne z omawianych zagrożeń nie istnieje w próżni, może mieć różne podłoże, jego zrozumienie może wymagać rozmowy z dzieckiem, a jeśli to potrzebne, zaangażowania specjalisty.

Zagadnienia i podstawowe umiejętności cyfrowe realizowane w Module 4.

4.1. Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem.

4.2. Korzystanie z narzędzi kontroli rodzicielskiej na komputerach i urządzeniach mobilnych.

Moduł 5.

3,5 godz. 66-87

E-usługi dla rodziców

Cele modułu

1. Poznanie e-usług dla rodziców.
2. Poznanie wartościowych i sprawdzonych programów dot. bezpieczeństwa w sieci.
3. Rozwój umiejętności nawigacji po serwisach z e-usługami dla rodziców.
4. Poznanie sposobów składania elektronicznych wniosków do e-usług dla rodziców.

Krok 1. Informacje i programy informacyjne dla rodziców

60 min. 66-69

Instrukcja dla OP

Przed szkoleniem przygotuj kopię dokumentu Google Docs i przygotuj go do udostępnienia, z prawem do edycji dla OU.

Doświadczenie

1. Podziel OU na cztery grupy i poproś, by każda grupa wyszukała w sieci praktyczne informacje dot. programu na jeden z podanych tematów. Co dany program oferuje? W jakich sytuacjach i komu może być pomocny? Jak się skontaktować z organizatorami? – przydziel losowo po jednym z tematów dla każdej z grup:
   - cyfrowobezpieczni.pl i cybernauci.edu.pl
   - cyfrowa-wyprawka.org
   - uodo.gov.pl/pl/p/edukacja
   - dyzurnet.pl
   - rodzicpoludzku.pl
2. Poproś OU o wyszukanie również możliwości nawiązania kontaktu elektronicznego z wybranymi przez nich programami.
3. Poproś OU o umieszczenie ich odpowiedzi i informacji we wcześniej przygotowanym dokumencie online Google Docs.

Refleksja

4. Zapytaj OU ile serwisów z ćwiczenia znali, ile jest dla nich nowych? Jakimi kryteriami kierowali się oceniając czy dane serwisy podają rzetelne informacje?
5. Podsumowując, zwróć uwagę np. na kwestię domen z rozszerzeniem .gov, aktualność informacji, certyfikat bezpieczeństwa, zalety korzystania ze sprawdzonych źródeł w porównaniu z informacją z forów internetowych.

Prezentacja OP

6. Przedstaw krótko cele i zastosowanie portali dla rodziców podanych w ćwiczeniu oraz pozostałych, opisanych w prezentacji.

Krok 2.
Zakładanie konta w ePUAP i profilu zaufanego

60 min. 70-74

Instrukcja dla OP

Przed szkoleniem załóż konto (jeśli nie posiadasz) w systemie ePUAP. Szczegółowa instrukcja zakładania dostępna jest tutaj: pz.gov.pl.

Doświadczenie

1. Chętne OU mogą podczas szkolenia założyć konto w systemie ePUAP, wówczas składają wniosek o założenie profilu i wysyłają wniosek. Jeżeli nikt nie chce zrobić tego podczas szkolenia, omów kolejne kroki, jakie należy wykonać, by móc zrobić to w domu. Podkreśl, że w materiałach szkoleniowych OU znajdą film instruktażowy, jak to zrobić krok po kroku.

Prezentacja OP

2. Przedstaw korzyści z posiadania z kont zaufanych takich jak ePUAP, np. ułatwienie składania wniosków 500+.
3. Przedstaw opcje założenia profilu zaufanego przez internet z potwierdzeniem w punkcie potwierdzającym, lub za pośrednictwem bankowości elektrycznej.
4. Przedstaw krok po kroku sposób zakładania konta w serwisie ePUAP.

Krok 3.
E-usługi dla rodziny

90 min. 75-87

Prezentacja OP

1. Przedstaw OU funkcje i informacje jakie znajdą w portalu rodzina.gov.pl.

Doświadczenie

2. Po krótkiej prezentacji portalu, poproś OU o wyszukanie wybranych informacji na temat:
   - telefonu dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci,
   - korzystania z dokumentów za pomocą smartfonu,
   - wyrabiania paszportu dla dziecka,
   - zapisu dziecka do przedszkola lub żłobka.

Refleksja

3. Omów i podsumuj doświadczenie OU. Dopytaj co budziło szczególne trudności, wyjaśnij wątpliwości dotyczące korzystania ze strony rodzina.gov.pl.

Prezentacja OP

4. Przedstaw inne portale rządowe istotne dla rodziców, m.in.:
   - dot. bezpieczeństwa transportu dzieci na wakacje lub wycieczki: bezpiecznyautobus.gov.pl,
   - dot. informacji praktycznych na temat urlopu rodzicielskiego: rodzicielski.gov.pl,
   - dot. jednostek pomocy społecznej, oferty rehabilitacyjnej, partnerów Karty Dużej Rodziny: empatia.mpips.gov.pl.
5. Przedstaw kroki do złożenia wniosków o wybrane e-usługi dla rodziców:
   - wniosek o wydanie Karty Dużej Rodziny,
   - wniosek o przyznanie świadczenia 500+.

Zagadnienia i podstawowe umiejętności cyfrowe realizowane w Module 5.

3.2. Wiedza na temat ogólnych zasad bezpieczeństwa, których powinno przestrzegać dziecko w internecie, w tym: sposoby reagowania na zagrożenia w sieci (hate, trolling, kradzież treści) i znajomość instytucji świadczących pomoc w tym zakresie (np. telefon dla rodziców 800 100 100), tworzenie bezpiecznych haseł, logowanie się przez sprawdzone sieci WiFi etc., bezpieczne zarządzanie prywatnością w sieci, w tym publikowanie różnych treści przez rodziców i dzieci, dbałość o wizerunek dziecka w internecie.

5.1. Założenie konta w ePUAP i profilu zaufanego.

5.2. Wykorzystanie profilu zaufanego.

5.3. Złożenie wniosku Rodzina 500+.

5.4. Uzyskanie Karty Dużej Rodziny.

Moduł 6. Zakończenie szkolenia

30 min. 88-91

Cele modułu

1. Podsumowanie szkolenia przez OP i OU.
2. Ewaluacja szkolenia.

1. Podsumuj i uporządkuj materiały dydaktyczne do wykorzystania przez OU po szkoleniu, poinformuj w jaki sposób można korzystać z materiałów po zakończeniu szkolenia. Pokaż OU zakładkę z materiałami szkoleniowymi na stronie programu *Ja w internecie*, jawinternecie.edu.pl/strefaedukacji.
2. Poproś OU o wypełnienie ankiety ewaluacyjnej online. Link do strony, na której znajduje się ankieta: badania.koduj.gov.pl.
3. Zaproś OU do krótkiego podsumowania szkolenia: z jaką refleksją, wrażeniami kończą szkolenie?