Opis scenariusza warsztatów Rodzic w internecie

Szkolenie powinno odbywać się w sali komputerowej wyposażonej w liczbę stanowisk komputerowych odpowiadającą liczbie osób uczestniczących, z dostępem do szerokopasmowego internetu, rzutnik z ekranem lub tablicę multimedialną.

Materiały dydaktyczne do opracowania przed szkoleniem:

- prezentacja szkoleniowa z najważniejszymi zagrożeniami dzieci w sieci (pomoce: http://www.saferinternet.pl/pliki/publikacje/Bezpieczestwo%20dzieci%20online.%20Kompendium%20dla%20rodzicw%20i%20profesjonalistw.pdf i https://panoptykon.org/sites/default/files/publikacje/podr-online-dwiestrony_0.pdf)
- webquest na temat wyszukiwania i odkrywania zasobów służących do rozrywki i edukacji dla dzieci i młodzieży,
- prezentacja na temat e-usług publicznych

Numeracja zagadnień realizowanych:

1.1-3 - umiejętności informacyjne

2.1-1 - umiejętności komunikacyjne

3.1-12 - umiejętności rozwiązywania problemów

4.1-2 - umiejętności związane z oprogramowaniem

5.1 - umiejętność korzystania z usług publicznych

Moduł	Przebieg oraz opis metod szkoleniowych	Zagadnienie realizowane
Dzień I		
Wprowadzenie do szkolenia **30 min.**	1. przedstawienie się osób uczestniczących (dalej OU) i osób prowadzących (dalej OP), **10 min.** 2. OP prezentują plan szkolenia oraz metody aktywne (ćwiczenia i prace w grupach, które mają służyć lepszemu zrozumieniu sytuacji ich dzieci w sieci oraz przećwiczeniu skutecznych reakcji i sposobów rozmowy z nimi), **10 min.** 3. OP pyta o oczekiwania OU np. w formie zebrania na kartkach po jednym konkretnym pytaniu od osoby, dot. aktywności dzieci w sieci lub ich jako rodziców, na jakie chcieliby uzyskać odpowiedź. **10 min.**	
Bezpieczeństwo techniczne urządzeń z których korzystamy, wprowadzenie najważniejszych pojęć **1 godz. 50 min.**	1. OP pyta OU o wszelkie technologie wykorzystywane przez o OU na co dzień: a. z jakich urządzeń korzystają na co dzień (dopytuje o komputery, tablety, smartfony, inne urządzenia podłączone do sieci np. smartwatche, inteligentne opaski sportowe, kamery wifi takie jak monitory dziecięce), b. dopytuje szczegółowo czy znają systemy operacyjne, zwraca uwagę na różne wersje systemów w ich smartfonach, c. z jakich aplikacji mobilnych korzystają i czy wiedzą jakie mają one uprawnienia do danych, d. z jakich usług korzystają (zakupy online, bankowość elektroniczna, usługi publiczne, usługi dot. zdrowia, rejestracje online etc.) e. podłączenie ich do różnych sieci (3G, WiFi), pyta o to czy wiedzą kiedy każde z nich było aktualizowane. f. Z dyskusji wypisuje na tablicy lub listę tych technologii, aplikacji, stron WWW, wyjaśnia jeśli dane pojęcia nie są znane	4.1. Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem. 4.2. Korzystanie z narzędzi kontroli rodzicielskiej na komputerach i urządzeniach mobilnych. 1.2. 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

	całej grupie. **20 min** 2. W następnej kolejności OP prosi o zapisanie na kartkach samoprzylepnych ryzyk i zagrożeń które OU kojarzą, znają lub byli ich ofiarą i prosi o przylepienie do odpowiednich przykładów, **15 min.** 3. OP porządkuje z grupą zagrożenia w poniższe kategorie po czym omawia je ze wsparciem prezentacji: a. fizyczne (np. utrata, zniszczenie, uszkodzenie sieci elektrycznej) b. cyfrowa awaria (utrata danych, brak możliwości pracy) c. podatność na wirusy, złośliwe oprogramowanie, ransomware d. wyciek prywatnych danych e. finansowe (utrata kontroli nad kontem, kartą płatniczą, oszustwa internetowe, wyłudzanie płatnych sms-ów i połączeń) f. zagrożenia wynikające z profilowania przez reklamodawców (ze szczególnym uwzględnieniem wpływu na dzieci) g. celowe ataki np. stalking za pomocą podsłuchu lub ataku na czyjś sprzęt, h. wizerunkowe (szkody moralne, utrata pracy, przyjaciół, reputacji) **30 min.** 4. Przy pomocy prezentacji OP przedstawia zasady dbania o bezpieczeństwo sprzętu, zwracając uwagę na to, że nie są to nigdy rozwiązania w pełni skuteczne i ważniejsze od nich są zasady ograniczonego zaufania w sieci oraz aktualizacja własnej wiedzy z racji na zmieniające się zagrożenia. OP omawia w prezentacji, **45 min**: a. rolę aktualizacji oprogramowania oraz świadomości jego ustawień na przykładzie popularnych przeglądarek internetowych i smartfonów b. rolę oprogramowania antywirusowego na różnych typach	dziecka w internecie. 5. 2. Wykorzystanie profilu zaufanego.

	sprzętu c. zasady ograniczania ryzyka infekcji złośliwym oprogramowaniem (podejrzane załączniki, phishing w mailach, sms-ach, wynikach wyszukiwania), niezaufany sprzęt USB etc. d. różnorodne poziomy bezpieczeństwa sieci przez które łączymy się z Internetem (różnice między siecią domową, 3G, wifi w miejscu publicznym) e. bezpieczeństwo przeglądarki internetowej f. różnice między bezpieczeństwem komputera a smartfonu oraz urządzeń tzw. IoT (Internet rzeczy) g. zarządzanie danymi o sobie w sieci i ustawienia prywatności h. zasady ograniczonego zaufania wobec nieznanych stron i usług, zwłaszcza wymagających podawania danych czy płatności online lub sms W wersji dla grupy o podstawowych kompetencjach wydłużone zostają punkty 3 i 4 (do odpowiednio 45 min. oraz 60 min). OP dodatkowy czas przeznacza na szczegółową prezentację zastosowania ochrony przed zagrożeniami, na które mogą być wyjątkowo podatne osoby zaczynające dopiero pracę w sieci i przestawia więcej przykładów. W tej części należy zwrócić większą uwagę na masowe oszustwa typu phishing (prezentacja przykładów w poczcie mailowe, sms-ach, róznych banków), zasady ograniczonego zaufania, polecane oprogramowanie antywirusowe, uważność podczas pobierania oprogramowania, ocena źródeł miejsc pobierania oprogramowania, alternatywne kanały weryfikacji komunikacji i weryfikacji tożsamości (np. z bankiem) oraz umiejętność blokowania kont w przypadku utraty kontroli.	
Korzystanie z sieci dzieci i dorosłych, teoria a praktyka **1 godz. 40 min.**	1. Na bazie poprzedniego moduły OP prosi OU podanie technologii, z jakich korzystają ich dzieci, oszacowanie czasu ile z nimi spędzają oraz podanie przykładów tego co robią w sieci. OP wypisuje odpowiedzi na tablicy lub w prezentacji., **20 min.**	1.1. Umiejętność nadzorowania aktywności dziecka w sieci. 1.2. Wiedza na temat ogólnych zasad bezpieczeństwa, których powinno

	2. OU rozwiązują samodzielnie na komputerach quiz programu Cybernauci https://cybernauci.edu.pl/materialy-edukacyjne/rodzice/ , **15 min.** 3. OP rozpoczyna dyskusję na temat odpowiedzi w quizie, podkreślając, że nie służy on ocenie, a skonfrontowaniu ich z różnorodnością zagadnień dot. aktywności w sieci, które dla nich i dla ich dzieci mogą być niebezpieczne lub trudne. Przechodząc wspólnie przez pytania OP pyta najpierw o to co dzieje się w danym pytaniu (np. o jaką technologię chodzi, czy ją znają i prosi chętnych o wyjaśnienie oraz notuje hasła na tablicy, o jakie zagrożenie chodzi w danej sytuacji itd.) a potem krótko komentuje prawidłowe odpowiedzi które posłużą jako wstęp do pozostałych modułów, **30 min.** 4. OP przechodzi do prezentacji wybranych wyników najważniejszych badań dotyczących korzystania dzieci z sieci: a. badania NASK, Nastolatki 3.0, 2017 https://akademia.nask.pl/publikacje/Raport_z_badania_Nastolatki_3_0.pdf) b. wyniki badań dot. opnii dorosłych o praktykach dzieci w sieci (badania Fundacji Orange i Fundacji Dzieci Niczyje 2013 Bezpieczeństwo dzieci w internecie https://panoptykon.org/files/bezpieczenstwo_dzieci_w_internecie_2013.pdf) W trakcie prezentacji prosi OU o komentarze np. przed wyświetlaniem niektórych wyników zadaje pytanie badawcze OU, a potem dyskutuje z nimi o ew. różnice w ich odpowiedziach, a w badaniach, co ich zaskoczyło, czy mają poczucie, że obiektywnie oceniają działanai swoich dzieci w sieci, czy chcieliby z nimi więcej o tym rozmawiać i spędzać więcej czasu wspólnie, **35 min.** W wersji dla grupy o podstawowych kompetencjach skrócona zostaje dyskusja o badaniach (do której OP może wrócić w razie potrzeby drugiego dnia w	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. 1.3. Symptomy nadużywania internetu przez dziecko i reakcja na nie. 1.4. 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.

	module o diagnozowaniu zagrożeń). Wydłużony zostaje poprzedzający moduł dot. bezpieczeństwa technicznego.	
Wyszukiwanie i korzystanie treści w sieci, podstawy rozpoznawania nielegalnych treści oraz zagrożeń technicznych i prawnych **2 godz.**	1. Wyszukiwanie i prawo autorskie: OP przedstawia w prezentacji podstawy techniczne wyszukiwania treści w sieci na przykładach popularnych wyszukiwarek, wyjaśnia najważniejsze różnice pomiędzy zasobami kultury i rozrywki dostępnymi w sieci zgodnie z prawem i nielegalnie (prezentuje opcje wyszukiwania zaawansowanego i na ich bazie tłumaczy podstawowe informacje dot. prawa autorskiego: granice dozwolonego użytku prywatnego i publicznego, różnice między dostępnością zasobów chronionych, udostępnianych na otwartych licencjach, a zasobami udostępnionymi nielegalnie), OP zwraca uwagę na konsekwencje korzystania z takich treści oraz ich rozpowszechniania, w tym rolę odpowiedzialności rodziców za działania dzieci, **40 min.** 2. Wyszukiwanie i bezpieczeństwo techniczne: OP dalej prezentuje również różnice między stronami dostępnymi z zabezpieczeniami (wprowadzenie zagadnień bezpieczeństwa przesyłu danych, szyfrowania stron z SSL/https, certyfikatów i wykrywania niebezpiecznych stron przez przeglądarki i wyszukiwarki), innych metod oceny treści w sieci (np. sprawdzania źródeł i recenzji) oraz różnice między dostępem do treści za pomocą różnych protokołów (www, streaming, sieci rozproszone jak bittorrent) oraz uwarunkowania prawne z nimi związane (konsekwencje prawne udostępniania w sieci torrrent, fałszywe serwisy streamingowe). OP używa przykładów popularnych e-usług komercyjnych (bankowość elektroniczna, zakupy online) oraz publicznych (profil zaufany, strony publiczne z zasobami kultury i rozrywki jak Polona czy Ninateka), OP podaje konsekwencje związane z brakiem stosowania tych zabezpieczeń nawiązując do	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 . 1.4. Prawo autorskie w zakresie istotnym dla rodziców i dzieci. 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). 3.6. Udostępnianie treści kultury w sieci. Odpowiedzialność prawna, plagiat,

	modułu dot. zagrożeń technicznych, **40 min.** 3. Wyszukiwanie a treści nieodpowiednie i niebezpieczne dla dzieci: OP pyta jakie treści na jakie można trafić łatwo w sieci mogą być szkodliwe lub niebezpieczne dla dzieci, czy można uniknąć całkowicie trafiania na nie (czy zdarzyło się im dorosłym, że zobaczyli coś czego sami nie chcieli etc.)? Na przykładzie popularnych wyszukiwarek OP prezentuje sposoby podstawowego filtrowania wyników (Safe search, kontrola rodzicielska) oraz zwraca uwagę, na to, że jest to rozwiązanie tylko częściowe i zawsze wymagające wsparcia i rozmów o zasadach z dziećmi. **30 min.** 4. Ćwiczenie indywidualne: OU korzystając ze zdobytej wiedzy o wyszukiwaniu mają znaleźć w sieci zadane przez OP zasoby (zadanie można podzielić na grupy np. pod kątem zainteresowań lub wieku dzieci OU), Zadania: znalezienie serwisów z wideolekcjami z określonych przedmiotów, znalezienie legalnej muzyki do wykorzystania do pokładu w projekcie szkolnym, wyszukanie rzetelnych informacji o polecanych aplikacjach mobilnych dla najmłodszych, wyszukanie informacji o wybranych grach i filmach popularnych wśród młodzieży i tego dla jakiego wieku są przeznaczone, wyszukanie materiałów edukacyjnych materiałów wideo dot. bezpiecznych ustawień prywatności w mediach społecznościowych.. Na koniec OP prosi OU o krótkie prezentacje dla pozostałych OU oraz dyskutuje z OU o kryteriach jakimi oceniali dane zasoby i strony, **40 min.** Metody: quiz, dyskusja, prezentacja, praca indywidualna z wsparciem trenera/ki, webquest W wersji z grupą o podstawowych kompetencjach przedłużone i zmienione zostaje ćwiczenie indywidualne (4), które można wykonać również w parach. OP poprzedza bardziej rozbudowaną prezentacją na temat mechaniki i	dozwolony użytek, prawo cytatu. 3.7. Korzystanie z banków zdjęć/klipów/dźwięków. Rodzaje licencji, warunki użytkowania. 5.5. Korzystanie z bibliotek, muzeów i archiwów cyfrowych.

	nawigacji po stronach internetowych i wyszukiwarkach. Celem zadania dla OP jest nie tylko odnalezienie zadanych informacji, ale również oswojenie się przed kolejnymi ćwiczeniami technicznymi z interfejsem przeglądarki i nawigacją stron i usług. **60 min**	
Dzień 2		
Wyszukiwanie i korzystanie treści w sieci, podstawy rozpoznawania nielegalnych treści oraz zagrożeń technicznych i prawnych c.d. **45 min.**		
Bezpieczeństwo komunikacji i ochrona danych i prywatności w sieci **1 godz. 30 min.**	1. OP pyta OU o wykorzystywane przez nie metody i kanały komunikacji (aplikacje, komunikatory, serwisy społecznościowe). W drugiej kolejności OP pyta o kanały komunikacji, z jakich korzystają dzieci (uzupełniając o przykłady z badań), nazwy serwisów i metod komunikacji wypisuje w dwóch kolumnach na tablicy. **15 min.** 2. Ćwiczenie w parach: OP przypomina, jedn~~g~~o z zagrożeń omawianych pierwszego dnia: wyciek danych i proponuje OU ~~uczestnikom~~ dokładne przyjrzenie się kwestii bezpieczeństwa internetowych haseł, podaje przykłady słabych haseł i pyta OU o to czego należy unikać w hasłach, a co mocne hasła powinny zawierać. OP dzieli OU na pary i prosi o przygotowanie mocnych a zarazem łatwych do zapamiętania haseł (co najmniej 8 znaków, znaki specjalne, cyfry, małe i wielkie litery) oraz ich wzajemną ocenę oraz opisanie metod zapamiętywania takiego hasła bez jego zapisywania. OP dodatkowo dopytuje jakie jeszcze zasady	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. 3.4. Uświadomienie dziecku sposobu i konsekwencji działania transakcji w

	warto wprowadzić by hasło było bezpieczne długoterminowo (zmiany haseł, sprawdzanie informacji o wyciekach danych np. na www.niebezpiecznik.pl, **15 min.** 3. Kolejnym zagadnieniem z pierwszego dnia do którego OP wraca jest kwestie ochrony prywatnych danych przed osobami trzecimi. OP prezentuje rolę ustawień prywatności w mediach społecznościowych na bazie Facebooka (pokaz i omówienie ustawień) oraz w kontach mailowych na przykładzie Gmaila i testu Security Check-up https://myaccount.google.com/intro/security (jako ćwiczenie osoby posiadające konto na Gmailu mogą przejść przez nie samodzielnie), **30 min.** 4. Następnie OP prezentuje rolę stałego zwiększania zabezpieczeń, w kontekście korzystania z nich na różnych urządzeniach i w różnych miejscach, na przykładzie dwuetapowej weryfikacji podczas logowania do kluczowych kanałów komunikacji (poczta mailowa, bank, usługi publiczne) na przykładzie Facebooka i Gmaila, **20 min.** 5. Po prezentacji i ćwiczeniach OP prosi OU o zastanowienie się nad tym, ile z wiedzy prezentowanej w tym tylko module jest dostępnych i znanych ich dzieciom. OP prosi o spisanie przez OU w formie jednej porady, najważniejszej informacji, która chcieliby przekazać swoim dzieciom z tego modułu w taki sposób, który będzie dla dzieci zrozumiały, **10 min.**	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. 3.8. Korzystanie z serwisów społecznościowych przez dzieci i rodziców, w tym prowadzenie profilu na Facebooku, YouTube, Twitterze, Instagramie i in. (wiedza o ograniczeniach wiekowych na poszczególnych portalach).
Diagnozowanie i rozwiązywanie problemów dot. bezpieczeństwa korzystania przez dzieci z sieci **2 godz.**	1. Kontrola rodzicielska i diagnozowanie potrzeb: OP rozpoczyna od dyskusji zadając pytania OU, uzupełniając ich odpowiedzi nawiązaniami i slajdami z pierwszego dnia dot. wyników badań: Jak chętnie dzieci dzielą się informacjami o sobie? Jak możemy dbać o to, by ograniczać ilość informacji wypływających do sieci? Czy sądzicie, że rodzicielska kontrola (np. odpowiednie programy, filtry omawianie wcześniej podczas szkolenia) są w stanie zapewnić dzieciom bezpieczeństwo? Od jakiego wieku warto poruszać z dziećmi kwestie	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

	związane z bezpieczeństwem w sieci? W trakcie dyskusji OP prezentuje ponownie omawiane rozwiązania (np. programy, aplikacje mobilne i ustawienia urządzeń wspierające kontrolę rodzicielską) jednocześnie podkreślając rolę ustalania wspólnych zasad (zwłaszcza ze starszymi dziećmi i nastolatkami) a nie tylko kontroli. **30 min.** 2. Diagnozowanie zagrożeń i podstawowe porady dot. przeciwdziałania. OP prezentuje wymienione zagadnienia w nawiązaniu do danych o korzystaniu z sieci i dyskusji pierwszego dnia szkolenia. Podczas omawiania podaje opis zjawiska, skalę oraz podstawowe porady, źródła dodatkowej wiedzy (np. poradnik SaferInternet http://www.saferinternet.pl/pliki/publikacje/Bezpieczestwo%20dzieci%20online.%20Kompendium%20dla%20rodzicw%20i%20profesjonalistw.pdf) oraz zwraca uwagę na to, że rodzice nie biorący udziału w aktywnościach dzieci w sieci mogą mieć skłonność zarówno do niedostrzegania takich zjawisk lub ich przecenienia (np. nadinterpretacji czasu spędzanego w sieci jako uzależnienia bez analizy tego jak dziecko spędza ten czas np. na nauce), a. cyberprzemoc b. sexting c. zagrożenia dla prywatności i danych osobowych dzieci d. korzystanie z pornografii e. uzależnienie f. mowa nienawiści g. kradzież tożsamości h. promowanie zachowań autodestrukcyjnych i. treści przedstawiające wykorzystywanie seksualne dzieci Prezentacja uzupełniona jest podaniem miejsc, w których można uzyskać pomoc w trudnych przypadkach. W przypadku zetknięcia się się z pornografią z udziałem małoletnich, www.dyzurnet.pl http://fdds.pl/szukasz-pomocy/ (oraz telefoniczny hotline), który przyjmuje i reaguje na zgłoszenia, dotyczące występowania w	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). 4.1. Umiejętność nadzorowania aktywności dziecka w sieci. 4.2. 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. 4.3. Symptomy nadużywania internetu przez dziecko i reakcja na nie. 4.4. 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.

	Internecie treści nielegalnych (pornografia dziecięca, treści rasistowskie i ksenofobiczne). W przypadku złamania prawa kontaktu z Policją. W przypadku włamania lub próby włamania do swojego komputera, jesteś nękany spamem przesyłanym za pośrednictwem polskich serwerów lub atakami hackerów, zgłoszenie do zespołu CERT Polska- www.cert.pl. W przypadku wątpliwości jak zareagować na problemy dziecka związanych z Internetem lub komputerem (zagrożenia, uzależnienie) - helpline.org.pl. W przypadku chęci podniesienia kompetencji nauczycieli i uczniów w szkole dzieci OU, OP sugeruje skorzystanie z oferty programów Cyfrowobezpieczni i Cybernauci oraz SaferInternet. **50 min.** 3. Ćwiczenie ogólnozespołowe: na bazie zdobytej do tej pory wiedzy oraz materiałów z w.w. programów OU mają opracować dekalog zasad dobrego i bezpiecznego korzystania z sieci, wspólny dla dzieci i rodziców, najpierw w formie burzy mózgów wypisują wszystkie zasady (5 min.). W drugiej fazie z pomocą OP omawiają proponowane zasady oraz ich skuteczność, OP zwraca uwagę w szczególności na ich język oraz poszanowanie praw dziecka, wspieranie go w realizacji tych zasad przez rodziców, a nie budowanie listy zakazów. OU mogą wykorzystać w tym ćwiczeniu porady, które zapisywali dla swoich dzieci we wcześniejszych ćwiczenia dot. bezpieczeństwa sprzętu i bezpiecznej komunikacji. **40 min** Metody: prezentacja, praca indywidualna z wsparciem trenera/ki z narzędziami współpracy online (np. google docs, padlet), praca grupowa	4.5. Nauka samodzielna i wspólna z dzieckiem z wykorzystaniem cyfrowych zasobów kultury i archiwów oraz źródeł internetowych (np. Wikipedia, TED, Khan Academy, Ninateka, POLONA).
Wygoda i bezpieczeństwo korzystania z usług publicznych **1 godz. 30 min.**	1. OP krótko podsumowuje dotychczasowe zagadnienia związane z bezpieczeństwem w sieci oraz korzyściami, korzystania z niej w sposób świadomy. OP pyta, z jakich usług publicznych w sieci do tej pory OU korzystali i z jakich chcieliby skorzystać? **10 min.** 2. OP przedstawia wybrane usługi ePUAP, profil zaufany, obywatel.gov.pl,	5. 1. Założenie konta w ePUAP i profilu zaufanego. 5. 2. Wykorzystanie profilu zaufanego. 5.3. Złożenie wniosku Rodzina 500+.

	serwis 500+ i ich zadania oraz korzyści płynące z ich wykorzystania, **20 min.** 3. OP prezentuje sposób zakładania konta w każdym z tych serwisów, **30 min.** 4. OU z pomocą OP oraz wcześniej przygotowanej instrukcji zakładają konto w jednej wybranej usłudze publicznej, 30 min.	5.4. Uzyskanie Karty Dużej Rodziny. 5. 6. Usługi związane ze zdrowiem.
Zakończenie szkolenia **15 min.**	- OP porządkują materiały dydaktyczne do wykorzystania przez osoby uczestniczące po szkoleniu, przekazują je poprzez przygotowany wcześniej jeden link z materiałami do pobrania, **5 min.** - osoby uczestniczące ewaluują szkolenie (ankieta online wypełniana na żywo), **10 min.**	