

PLANY LEKCJI DLA DOROSŁYCH EDUKATORÓW / NAUCZYCIELI / TRENERÓW

Nazwa modułu: Komunikacja i współpraca	
Temat 4 Tytuł: Obywatelstwo cyfrowe	
Plan lekcji 35 - Netykieta	
Czas trwania: 90 minut	
Cel	Głównym celem tego planu lekcji jest zapewnienie wszystkich niezbędnych informacji dotyczących praw i obowiązków cyfrowych, cyfrowego bezpieczeństwa i prywatności oraz zdrowia i dobrego samopoczucia w sieci.
Grupa docelowa	Dorośli (seniorzy)
Obiekt / wyposażenie	• Sala lekcyjna • Dostęp do Internetu • Projektor • Biała tablica
Narzędzia / materiały	•
Główne zadania	1. Zadanie 1: Wprowadzenie do netykiety 1.1 Rozpocznij zadanie od filmu wideo https://www.youtube.com/watch?v=FWMk_Zv7nB8 & ab channel = AngelRivera (3 minuty) 1.2 Pytania do dyskusji odnoszące się do filmu (15 minut) • Czym jest “netykieta”? • Dlaczego netykieta jest ważna? 2. Zadanie 2: Podstawowe zasady netykiety - co można robić

	online! 2.1 Osoby prowadzące szkolenie powinny wyjaśnić uczniom kilka podstawowych zasad netykiety i dać parę wskazówek na temat tego co można robić online (<u>patrz Załącznik 1</u>) (20 minut) 3. Zadanie 3: Czego <i>NIE</i> należy publikować online? Podstawowe wskazówki! 3.1 Rozpocznij zadanie od filmu wideo https://www.youtube.com/watch?v=iup8_fLhCiQ & ab_channel = Vickpoint (3 minuty) 3.2 Osoby prowadzące szkolenie powinny wyjaśnić uczniom podstawowe zasady netykiety i dać parę wskazówek na temat tego czego nie można publikować online (<u>patrz Załącznik 2</u>) (20 minut) 4. Zadanie 4: Wskazówki jak się chronić! 4.1 Osoby prowadzące szkolenie powinny wyjaśnić uczniom podstawowe zasady netykiety i dać parę wskazówek na temat tego czego nie można publikować online (<u>patrz Załącznik 3</u>) (20 minut) 5. Zadanie 5: Podsumowanie (10 minut)
--	---

Załącznik 1: Podstawowe zasady i wskazówki dotyczące netykiety

- 1.** Niech prawdziwi ludzie będą priorytetem: kiedy przebywasz z ludźmi w prawdziwym życiu, angażuj się w kontakt z nimi, a nie ze swoimi urządzeniami!
- 2.** Pamiętaj o swoich odbiorcach - wiedz, gdzie jesteś: zasady netykiety różnią się w zależności od tego, co robisz online!
- 3.** Okaż szacunek: nie zapominaj, że w trybie online wchodzisz w interakcję z prawdziwymi ludźmi, nawet jeśli widzisz tylko nazwę użytkownika lub zdjęcie. Dlatego bądź miły i pełen szacunku! Nie zachowuj się tak, jakbyś nie robił tego w prawdziwym świecie.
- 4.** Bądź etyczny: postępuj zgodnie z prawami i zasadami (pisemnymi lub niepisanymi), tak jak w prawdziwym świecie. Pamiętaj, że wszystkie nasze działania mają konsekwencje etyczne!
- 5.** Zadbaj o swój wygląd w Internecie - udostępniaj dyskretnie: upewnij się, że dbasz o treści które udostępniasz. Lepiej nie udostępniać niczego zawstydzającego, nielegalnego lub niewłaściwego! Pomyśl dwa razy, zanim opublikujesz post online!
- 6.** Szanuj czas innych ludzi: kiedy publikujesz posty online, komentujesz lub wysyłasz wiadomość/e-mail, potrzeba czasu, aby inni ją przeczytali! Powinieneś upewnić się, że czas spędzony na przeczytaniu twojego postu nie jest stracony!
- 7.** Szanuj prywatność ludzi: powinieneś być bardzo ostrożny podczas obchodzenia się z informacjami, do których masz uprzywilejowany dostęp i które dotyczą innych! Musisz upewnić się, że nie udostępniasz prywatnych informacji innym osobom i nigdy nie korzystasz z ich kont lub urządzeń bez pozwolenia!



8. Sprawdzenie faktów przed ponownym opublikowaniem: Internet pełen jest informacji pochodzących z różnych źródeł. Podając lub udostępniając informacje, należy zachować ostrożność. Powinieneś sprawdzić wszystko, co przeczytałeś, zwłaszcza przed ponownym opublikowaniem!

9. Szybko odpowiadaj innym: jeśli jesteś online i ktoś będzie chciał się z Tobą skontaktować, oczekuje, że mu odpowiesz, radzimy to zrobić!

10. Zaktualizuj informacje online: Nie zostawiaj niedokładnych lub błędnych informacji w internecie, jeśli jesteś w stanie je poprawić!

11. Podziel się swoją wiedzą: jedną z głównych zasad społeczności internetowych jest dzielenie się! Jeśli masz wiedzę lub doświadczenie na określony temat, bądź miły i podziel się nim z innymi!

12. Zachowaj zdrowy rozsądek: W porządku jest się nie zgadzać z kimś online! Pamiętaj tylko, że jeśli dojdzie do nieporozumienia, ważne jest, aby zachować uprzejmość i wiedzieć, kiedy przestać!

13. Nie krzycz, proszę: na wszystko jest czas i miejsce - ALE W WIĘKSZOŚCI SYTUACJI PISANIE WIELKIMI LITERAMI JEST NIEWŁĄŚCIWE. Większość czytelników postrzega to jako krzyk! Więc prosimy, nie rób tego!

14. Przeczytaj i zastanów się, zanim zadasz pytanie: jeśli utkniesz z pytaniem, lepiej poszukać odpowiedzi w Internecie, zanim zadasz je innym. W większości przypadków nie ma potrzeby włączania stron trzecich.

15. Nie zbaczaj z tematu: kiedy toczy się dyskusja online, łatwo jest odejść od początkowego tematu, zwłaszcza gdy bierze w niej udział wiele osób! Podążanie za tematem gwarantuje, że niepotrzebne informacje i komentarze nie przeszkadzają innym w znalezieniu wartościowych informacji.



Załącznik 2: Czego NIE należy publikować w Internecie? Podstawowe wskazówki

1.

Twoja osobista lokalizacja: udostępnianie swojej osobistej lokalizacji może być ryzykowne. Informowanie ludzi o swoim miejscu pobytu może być dla Ciebie potencjalnie szkodliwe, ponieważ pozwala stalkerom ustalić, gdzie jesteś, a potencjalnym złodziejom wiedzieć, gdzie Cię nie ma (np. nie ma Cię w domu kiedy jesteś na wakacjach).

2.

Twój adres domowy lub osobisty numer telefonu: Adres i numery telefonów to dwa typy danych, które złodzieje tożsamości mogą wykorzystać do kradzieży Twojej tożsamości! Ponieważ nie wykrzykujesz swojego adresu ani numeru telefonu w przestrzeni publicznej w prawdziwym świecie, radzimy również nie robić tego online!

3.

Twój status finansowy - informacje bankowe i dane karty: bardzo ważne jest, aby takie informacje pozostały poufne! Dzielenie się informacjami o stanie finansowym może grozić potencjalną kradzieżą tożsamości! Za wszelką cenę należy unikać zdjęć wszelkich informacji bankowych i danych karty kredytowej!

4.

Informacje, zdjęcia i filmy innych osób bez pytania: jeśli chcesz udostępniać treści, które dotyczą innych osób, najpierw uzyskaj ich zgodę. Powinni mieć wybór, czy chcą aby takie treści pojawiły się w internecie, czy nie!

5.

Treści „dla dorosłych” - nieodpowiednie zdjęcia: Internet jest miejscem publicznym, nawet jeśli myślisz, że udostępniasz je prywatnie. Tak więc, zanim umieścisz selfie w swoim kostiumie kąpielowym, zastanów się, czy nie przeszkadza Ci to, gdyby ktoś Cię tak widział w biurze lub gdyby oglądały to dzieci.

6.

Fałszywe lub nieprawdziwe stwierdzenia: Udostępnianie fałszywych lub nieprawdziwych informacji jest złe! Nie mówiąc już o nieprawdziwych informacjach o konkretnej osobie!

7.

Fałszywe lub nieprawdziwe stwierdzenia: Udostępnianie fałszywych lub nieprawdziwych informacji jest złe! Nie mówiąc już o nieprawdziwych informacjach o konkretnej osobie!

8.

Zagrożenia: NIE jest w porządku grożenie ludziom w prawdziwym życiu, bez względu na ich pozycję i to samo dotyczy działania w internecie!

9.

Zagrożenia: NIE jest w porządku grożenie ludziom w prawdziwym życiu, bez względu na ich pozycję i to samo dotyczy działania w internecie!

10.

Wizerunki dzieci: Kontrolowanie treści opublikowanych online jest trudne, jeśli nie niemożliwe! W Internecie należy unikać zdjęć dzieci, ponieważ nikt nie wie, w jaki

sposób będą je wykorzystywać inni. Mogą być źródłem cyberprzemocy, a nawet przyczyną ataku przez niebezpiecznych ludzi!



HANDOUT 3: Wskazówki jak się chronić!

- 1. Używaj silnych haseł.** Dowiedz się, czym jest silne hasło i jak je utworzyć! Pamiętaj, że zaleca się używanie różnych haseł do różnych usług.
- 2. Poszukaj szyfrowania.** Spróbuj skorzystać z usług oferujących szyfrowanie (dowiedz się jak)! Pamiętaj, że poczta e-mail nie jest szyfrowana, więc nigdy nie udostępniaj przez nią danych osobowych!
- 3. Zainstaluj oprogramowanie antywirusowe.** Dowiedz się o ochronie antywirusowej i jej znaczeniu [tutaj](#).
- 4. Uważaj na e-maile / linki i załączniki.** Nie ufaj e-mailom, plikom i załącznikom od nieznanym! Dowiedz się więcej [tutaj](#)!
- 5. Upewnij się, że Twoje urządzenia są zaktualizowane.** Upewnij się, że Twoje urządzenia i usługi, z których korzystasz, są zaktualizowane! Aktualizacje często zawierają krytyczne poprawki wszelkich luk w zabezpieczeniach, które mogły zostać wykryte w programach lub urządzeniach. Dowiedz się więcej [tutaj](#)!
- 6. Użyj uwierzytelniania dwuetapowego, jeśli jest dostępne.** Uwierzytelnianie dwuetapowe wymaga zweryfikowania swojej tożsamości po zalogowaniu, nawet jeśli wyślesz swoją nazwę użytkownika i hasło. W niektórych przypadkach zostaniesz poproszony o zweryfikowanie swojej tożsamości poprzez wprowadzenie kodu przesłanego SMS-em na Twój telefon lub e-mailem.
- 7. Unikaj korzystania z niezabezpieczonych publicznych sieci Wi-Fi.** Należy unikać łączenia się z Internetem przy użyciu niezabezpieczonych publicznych sieci Wi-Fi na urządzeniach. Używanie go może narazić Cię na ataki. Ten link wyjaśnia dlaczego!
- 8. Uważaj, skąd się logujesz - unikaj korzystania z komputerów publicznych.** Komputery publiczne nie są tak bezpieczne jak komputery osobiste, więc musisz być ostrożny! Postępuj zgodnie ze wskazówkami, aby zachować bezpieczeństwo!
- 9. Wreszcie, jak już wspomnieliśmy, UWAGA NA TO, CO PUBLIKUJESZ W SIECI!**

