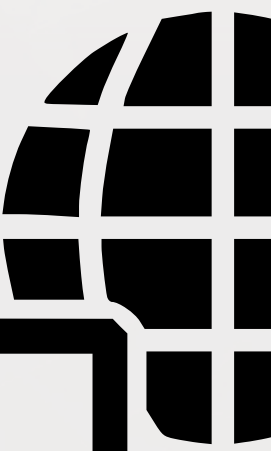


CYBERBAKCYL BEZPIECZEŃSTWO W SIECI (10-11)



WPROWADZENIE DO TEMATU

Internet, a zwłaszcza media społecznościowe, nieustannie zachęcają nas do dzielenia się: wiedzą, informacjami, interesującymi treściami, ale też naszymi umiejętnościami, osiągnięciami, pasjami, przemyśleniami, słowem: naszym życiem. Wirtualne wspólnoty funkcjonują na zasadzie wymiany: każdy, kto tylko jest ich częścią, może korzystać z treści udostępnianych bądź stworzonych przez innych użytkowników, a także sam oferować innym to, co uważa za ciekawe czy wartościowe.

W tej sieci wymiany istnieje jednak szereg zagrożeń, których należy być świadomym, by bezpiecznie i odpowiedzialnie funkcjonować w wirtualnym świecie.

Pierwsze z tych zagrożeń dotyczą naruszenia naszej prywatności, nadmiernego udostępniania siebie i swojego życia w mediach społecznościowych. Drugie z kolei związane są z udostępnianiem danych, które mogą być łatwo wykorzystane przeciwko nam przez różnych internetowych oszustów, złodziei i naciągaczy. Dlatego niezwykle ważna jest umiejętność rozróżniania tych treści, którymi bezpiecznie można dzielić się z innymi, od tych, które narażają nas na różnego rodzaju ryzyko (zobacz plakaty CyberBakcyla - do pobrania <https://cyberbakcyl.pl/do-pobrania/>)

Podczas zajęć dzieci lepiej zrozumieją funkcjonowanie Internetu i mediów społecznościowych. Wspólnie z nauczycielem zastanowią się jakie treści warto udostępniać innym, a które lepiej zachować dla siebie i dla czego. Nauczą się też, jak zachować czujność i ostrożność wobec innych użytkowników internetu.

CYBERBAKCYL

CYBERBAKCYL

CYBERBAKCYL

CHARAKTERYSTYKA ZAJĘĆ

Odbiorcy

- Zajęcia przeznaczone są dla uczniów V-VI klasy SP.
- Mogą być realizowane podczas godziny wychowawczej, lekcji informatyki lub zajęć pozalekcyjnych.

Cele zajęć

- Poinformowanie uczniów o podstawowych zasadach bezpieczeństwa podczas korzystania z Internetu, zagrożeniach dla prywatności i konieczności ochrony swoich danych, a także często spotykanych formach oszustw w przestrzeni wirtualnej.

Czas trwania

- Zajęcia przewidziane są na jedną godzinę dydaktyczną (45 min).

Osoby prowadzące

- Zajęcia zostały stworzone z myślą o nauczycielach, pedagogach i innych osobach, które w swojej codziennej pracy mają kontakt z dziećmi w wieku 10-11 lat (V-VI klasa). Prowadzący zajęcia powinien mieć podstawową wiedzę dotyczącą korzystania z Internetu, portali społecznościowych i komunikatorów.

Materiały potrzebne do realizacji zajęć

- Do realizacji zajęć w formie podstawowej nie są potrzebne żadne dodatkowe materiały.
- Do wykonania zadań dodatkowych konieczna jest tablica multimedialna z połączeniem do Internetu.
- Zajęcia można też przeprowadzić w sali informatycznej, gdzie każdy z uczniów będzie miał dostęp do komputera lub wykorzystać podłączony do projektora/rzutnika komputer.

GRA WPROWADZAJĄCA

Nauczyciel podaje informacje, jeśli któraś z nich prawdziwa w odniesieniu do Was, zasygnalizujcie to wstając. Np. „Mam psa” – jeśli to zdanie jest prawdziwe w stosunku do Was – wstańcie, jeśli nie, to zostańcie na swoich miejscach.

Po każdej informacji rozejrzyjcie się dookoła, żeby sprawdzić kto jeszcze wstał lub nie.

- Mam dwójkę lub więcej rodzeństwa
- Mam jakieś zwierzę (psa, kota, rybki itd.)
- Oglądam filmy na YouTube
- Gram w gry online z innymi uczestnikami
- Lubię grać w piłkę
- Ładnie śpiewam

Pytania do uczniów:

- Jak myślicie, jaki był cel tej gry?
- Czego się z niej dowiedzieliście?

Celem tej gry było pokazanie Wam, że dzielenie się pewnymi informacjami o sobie jest w naturalne, również w Internecie, ale trzeba wiedzieć, których informacji możemy udzielać, a które powinniśmy zachować dla siebie, ponieważ są prywatne.

CYBERBAKCYL

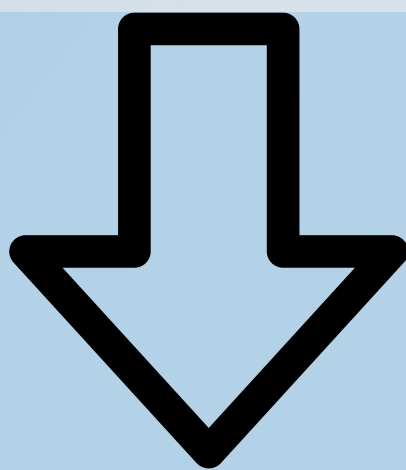


PRZYKŁADY INFORMACJI



Uczniowie decydują, czy dana informacja może być publikowana, czy powinniśmy ją zachować dla siebie.

- Moja ulubiona piosenka to.. (możemy publikować)
- Mój adres ... (prywatne, nie możemy publikować)
- Gdzie pracują moi rodzice (prywatne, nie możemy publikować)
- Gdzie chodzę na zajęcia pozalekcyjne (prywatne, nie możemy publikować)
- Jakim autobusem jeżdżę do szkoły (prywatne, nie możemy publikować)
- Jaki samochód mają rodzice (jeśli mają)
- Imię mojego zwierzaka (możemy publikować)
- Data urodzenia (prywatne, nie możemy publikować)
- Moje ulubione danie (możemy publikować)



Ważne jest, by pamiętać, że dzielenie się prywatnymi informacjami z nieznanymi osobami może być bardzo ryzykowne.

Z tego powodu nigdy nie należy udostępniać prywatnych informacji bez zgody zaufanej osoby dorosłej, która dysponuje wiedzą o internecie. Prywatne informacje to informacje o Tobie, których można użyć do odgadnięcia Twojego imienia i nazwiska, czy adresu zamieszkania. Nieznane osoby mogą wysyłać nam też wiadomości w postaci tzw. „łańcuszków” albo linków, które mogą być niebezpieczne.

WYŁUDZANIE DANYCH (PHISHING), SPAM I FAŁSZYWE SKLEPY INTERNETOWE - NAJCZĘSTSZE PRZESTĘPSTWA

- **Phishing** - to wyłudzenie danych polegające na podszywaniu się pod inną osobę lub instytucję.

Takie działania dotyczą jednak nie tylko instytucji finansowych, gdyż często cyberprzestępcy podszywają się pod dostawców poczty elektronicznej, czy ich współpracowników. Trzeba uważać też na SMS-owe kampanie phishingowe, np. wiadomości sms na temat dopłat do przesyłek pocztowych.

- **Fałszywe sklepy internetowe** - uważaj na podejrzenie niskie ceny, zwróć uwagę czy w adresie sklepu pojawia się: <https://>

Oznacza to, że strona jest bezpieczna i szyfrowana.

W zakładce „Kontakt” na stronie internetowej sklepu powinieneś bez problemu znaleźć takie informacje, jak adres firmy, numer telefonu, a także numer NIP (Numer Identyfikacji Podatkowej) lub KRS (Krajowy Rejestr Sądowy). Każda firma legalnie działająca musi dysponować takim numerem. W trakcie zakupów zwróć uwagę, czy musisz zaznaczyć, że zapoznałeś/aś się z klauzulą RODO.

RODO to prawo chroniące ludzi mieszkających w Unii Europejskiej przed kradzieżą danych. Fałszywe sklepy internetowe nie zwracają uwagi na takie detale.

- **Spam** - wśród oszustw komputerowych powtarza się też spam, w ramach którego oszust proponuje ofierze np. podział wysokiej kwoty pieniężnej po spełnieniu różnych warunków i dokonaniu przelewu na jego konto.

Pieniądze do ofiary oczywiście nie trafiają.

Każdy może zgłosić incydent w sieci do NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy za pośrednictwem formularza na stronie <https://incydent.cert.pl>