

Wprowadzenie do cyberbezpieczeństwa

Czym jest cyberbezpieczeństwo?

Klasy IV–VIII (10–16 lat) · 45 minut · bez kont uczniów

michal.kids/blog/akademia/cyberbezpieczenstwo-wprowadzenie

Cele i zakres

Uczniowie poznają:

- Co to jest cyberbezpieczeństwo?
- Dlaczego cyberbezpieczeństwo dotyczy każdego

Przebieg (45 minut)

10 min – Wprowadzenie

Zadaj pierwsze pytanie do rozmowy i przeczytajcie pierwszą część lekcji.

- Jak stworzyć bezpieczne hasło i dlaczego jest to ważne?
- Co to jest cyberbezpieczeństwo?

15 min – Treść lekcji

Przeczytajcie kolejne części (na rzutniku albo z konspektu) i omówcie pytania po każdej z nich.

- Dlaczego cyberbezpieczeństwo dotyczy każdego

15 min – Karta pracy

Uczniowie samodzielnie odpowiadają na pytania, potem sprawdzacie odpowiedzi razem – klucz jest w konspekcie.

5 min – Podsumowanie

Uczniowie uzupełniają część „Co zrobię, gdy...” i zabierają kartę do domu – na dole jest krótka informacja dla rodzica.

- Co zrobisz, gdy dostaniesz dziwną wiadomość od nieznajomego?

Pytania do rozmowy

- Co zrobisz, gdy dostaniesz dziwną wiadomość od nieznajomego?
- Jak stworzyć bezpieczne hasło i dlaczego jest to ważne?
- Czy wiesz, co to phishing i jak go unikać?

Karta pracy – klucz odpowiedzi

1. Konto kolegi pisze do ciebie: „Pożycz kod z karty podarunkowej, oddam jutro”. Co robisz?

- A. Wysyłam kod, bo kolegom trzeba pomagać
- B. Wysyłam tylko połowę kodu na próbę
- C. Odpisuję na tym czacie: „To na pewno ty?” i czekam
- D. Pytam kolegę na żywo, czy to on, i mówię dorosłemu

Prawidłowa odpowiedź: D. Pytam kolegę na żywo, czy to on, i mówię dorosłemu

Gdy konto jest przejęte, na czacie odpisze oszust. Sprawdź innym sposobem – na żywo albo telefonem – i powiedz dorosłemu.

2. Co chroni cyberbezpieczeństwo?

- A. Twoje urządzenia, konta i informacje
- B. Tylko komputery dużych firm i banków
- C. Tylko ekran telefonu przed z biciem
- D. Tylko czas, który spędzasz na graniu

Prawidłowa odpowiedź: A. Twoje urządzenia, konta i informacje

Cyberbezpieczeństwo chroni urządzenia (telefon, komputer, konsolę), konta (gry, Discord, TikTok) i informacje (zdjęcia, hasła, adres). Dotyczy każdego, nie tylko firm.

3. Ktoś pisze na czacie gry: „Kliknij link i odbierz darmowe Robuxy”. Co robisz?

- A. Klikam, bo za darmo nic nie tracę
- B. Wysyłam link znajomym, żeby też dostali
- C. Klikam, ale nie podaję od razu hasła
- D. Nie klikam i pokazuję to dorosłemu

Prawidłowa odpowiedź: D. Nie klikam i pokazuję to dorosłemu

„Darmowe” Robuxy, V-Bucks czy skiny to częsty sposób na kradzież konta. Samo kliknięcie może zainstalować coś złego. Lepiej nie klikać i pokazać wiadomość rodzicowi albo innemu zaufanemu dorosłemu.

4. Które z tych informacji warto chronić przed obcymi w internecie?

- A. Pogodę na jutro w twoim mieście
- B. Zdjęcia, hasła i adres domu
- C. Godziny otwarcia sklepu
- D. Wynik meczu z telewizji

Prawidłowa odpowiedź: B. Zdjęcia, hasła i adres domu

Zdjęcia, hasła i adres mówią coś o tobie i otwierają twoje konta. Pogoda czy wynik meczu to informacje, które i tak zna każdy.

5. Ktoś próbował cię oszukać w internecie. Co warto zrobić najpierw?

- A. Nic nikomu nie mówić, bo to wstyd
- B. Odpisać i zagrozić tej osobie
- C. Powiedzieć rodzicowi albo innemu zaufanemu dorosłemu
- D. Usunąć wszystkie konta i nigdy nie wracać do internetu

Prawidłowa odpowiedź: C. Powiedzieć rodzicowi albo innemu zaufanemu dorosłemu

To nie twoja wina, że ktoś próbował oszukać. Dorosły pomoże zabezpieczyć konto i zgłosić sprawę. Gdy ktoś grozi albo czujesz się bardzo źle, zadzwoń pod 116 111.

6. Dlaczego oszust może chcieć przejąć konto dziecka w grze?

- A. Bo konta dzieci nie mają żadnej wartości
- B. Bo chce za darmo pomóc w przejściu trudnego poziomu
- C. Bo przedmioty i postępy w grze da się sprzedać
- D. Bo gra co roku sama przekazuje konta innym

Prawidłowa odpowiedź: C. Bo przedmioty i postępy w grze da się sprzedać

Konta w grach mają wartość – przedmioty, skiny i postępy da się sprzedać. Dlatego chroń je długim hasłem i logowaniem dwuetapowym.

7. Dostajesz wiadomość: „Masz 5 minut, inaczej konto zostanie usunięte. Kliknij tutaj!”. Co to najczęściej oznacza?

- A. Próbę oszustwa – pośpiech ma cię nabrać
- B. Ważną wiadomość od gry, trzeba kliknąć od razu
- C. Błąd w aplikacji, który sam zniknie
- D. Prezent od twórców gry dla najlepszych graczy

Prawidłowa odpowiedź: A. Próbę oszustwa – pośpiech ma cię nabrać

Pośpiech to typowa sztuczka oszustów: nie dają czasu na myślenie. Nie klikaj. Pokaż wiadomość dorosłemu albo sprawdź konto, otwierając aplikację samodzielnie, nie przez link.

8. Które informacje oszust najchętniej by od ciebie zdobył?

- A. Ulubiony kolor twojego plecaka
- B. Prognozę pogody na jutro
- C. Tytuł filmu, który oglądała cała klasa
- D. Hasło, adres domu i nazwę szkoły

Prawidłowa odpowiedź: D. Hasło, adres domu i nazwę szkoły

Hasło otwiera konto, a adres i szkoła mówią, gdzie cię znaleźć. Tych informacji nie podawaj obcym w internecie.

Gdzie szukać pomocy

116 111 – telefon zaufania dla dzieci i młodzieży (bezpłatny),
800 12 12 12 – Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka (bezpłatny),
112 – gdy zagrożone jest życie.

Powiązanie z podstawą programową

Informatyka, klasy IV–VI – wymagania:

- 4.1) korzysta w sposób celowy i bezpieczny z urządzeń cyfrowych, w tym z zestawu komputerowego;
- 4.3) rozpoznaje podejrzane treści on-line i podejmuje podstawowe działania obronne – moduł medialny;
- 5.4) ocenia konsekwencje różnych zagrożeń cyfrowych oraz wskazuje sposoby reagowania na nie i możliwości uzyskania wsparcia;
- 5.5) chroni dane osobowe, stosując hasła i podstawowe ustawienia prywatności;
- Godzina wychowawcza: zadania wychowawczo-profilaktyczne szkoły (załącznik nr 2, część IV) – realizowane w programie wychowawczo-profilaktycznym szkoły.

Źródło: rozporządzenie Ministra Edukacji z dnia 11 marca 2026 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej (Dz. U. z 2026 r. poz. 378, ze zm.), załącznik nr 2: informatyka, klasy IV–VI, oraz część IV „Zadania wychowawczo-profilaktyczne szkoły”. W roku szkolnym 2026/2027 ta podstawa obowiązuje w klasie IV; w klasach V–VIII obowiązuje dotychczasowa podstawa z 2017 r. (Dz. U. z 2017 r. poz. 356 z późn. zm.).

Treść lekcji

Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to dbanie o to, żeby nikt obcy nie dostał się do twoich urządzeń, kont i informacji. Urządzenia to telefon, komputer, tablet albo konsola. Konta to na przykład konto w grze, na Discordzie albo na TikToku.

Chronimy trzy rzeczy:

- **urządzenia** – żeby działały i nikt ich nie przejął,

- **konta** – żeby nikt inny się na nie nie logował,
- **informacje** – zdjęcia, wiadomości, hasła, adres domu.

Z internetu korzystamy codziennie: w szkole (dziennik elektroniczny, lekcje online), w grach i w rozmowach ze znajomymi. Dlatego cyberbezpieczeństwo dotyczy każdego – także dzieci, nie tylko firm i informatyków.

Dobra wiadomość: najwięcej dają proste nawyki. Nie podajesz nikomu hasła. Nie klikasz w linki typu „darmowe Robuxy”. Pytasz dorosłego, gdy coś wygląda dziwnie. Tego wszystkiego nauczysz się w tym kursie.

Co zrobić, gdy coś pójdzie nie tak?

Powiedz rodzicowi albo innemu zaufanemu dorosłemu – na przykład wychowawcy albo pedagogowi szkolnemu. To nie twoja wina, że ktoś próbował cię oszukać. Jeśli ktoś ci grozi albo czujesz się z tym bardzo źle, możesz bezpłatnie zadzwonić pod **116 111** – to telefon zaufania dla dzieci i młodzieży.

Czas na quiz!

1. Co chroni cyberbezpieczeństwo?

- A. Twoje urządzenia, konta i informacje
- B. Tylko komputery dużych firm i banków
- C. Tylko ekran telefonu przed zbicciem
- D. Tylko czas, który spędzasz na graniu

Prawidłowa odpowiedź: A. Twoje urządzenia, konta i informacje

Cyberbezpieczeństwo chroni urządzenia (telefon, komputer, konsolę), konta (gry, Discord, TikTok) i informacje (zdjęcia, hasła, adres). Dotyczy każdego, nie tylko firm.

2. Ktoś pisze na czacie gry: „Kliknij link i odbierz darmowe Robuxy”. Co robisz?

- A. Klikam, bo za darmo nic nie tracę
- B. Wysyłam link znajomym, żeby też dostali
- C. Klikam, ale nie podaję od razu hasła
- D. Nie klikam i pokazuję to dorosłemu

Prawidłowa odpowiedź: D. Nie klikam i pokazuję to dorosłemu

„Darmowe” Robuxy, V-Bucks czy skiny to częsty sposób na kradzież konta. Samo kliknięcie może zainstalować coś złego. Lepiej nie klikać i pokazać wiadomość rodzicowi albo innemu zaufanemu dorosłemu.

3. Które z tych informacji warto chronić przed obcymi w internecie?

- A. Pogodę na jutro w twoim mieście
- B. Zdjęcia, hasła i adres domu
- C. Godziny otwarcia sklepu
- D. Wynik meczu z telewizji

Prawidłowa odpowiedź: B. Zdjęcia, hasła i adres domu

Zdjęcia, hasła i adres mówią coś o tobie i otwierają twoje konta. Pogoda czy wynik meczu to informacje, które i tak zna każdy.

4. Ktoś próbował cię oszukać w internecie. Co warto zrobić najpierw?

- A. Nic nikomu nie mówić, bo to wstyd
- B. Odpisać i zagrozić tej osobie
- C. Powiedzieć rodzicowi albo innemu zaufanemu dorosłemu
- D. Usunąć wszystkie konta i nigdy nie wracać do internetu

Prawidłowa odpowiedź: C. Powiedzieć rodzicowi albo innemu zaufanemu dorosłemu

To nie twoja wina, że ktoś próbował oszukać. Dorosły pomoże zabezpieczyć konto i zgłosić sprawę. Gdy ktoś grozi albo czujesz się bardzo źle, zadzwoń pod 116 111.

Dlaczego cyberbezpieczeństwo dotyczy każdego

Wiele osób myśli: „Kto by chciał coś ode mnie? Nie mam pieniędzy”. To błąd. **Każdy, kto korzysta z internetu, ma coś cennego** – także dzieci.

Czego może chcieć oszust?

- **twojego konta w grze** – przedmioty, skiny i postępy da się sprzedać,
- **twojego konta na Discordzie, Instagramie albo TikToku** – żeby pisać z niego do twoich znajomych i prosić ich o pieniądze, kody albo zdjęcia,
- **twoich zdjęć i informacji** – na przykład adresu domu, nazwy szkoły albo tego, gdzie teraz jesteś.

Oszuści często poganają: „Masz 5 minut, inaczej konto zostanie usunięte!”. Albo udają kogoś znajomego. Pośpiech w wiadomości to sygnał: zatrzymaj się i zapytaj dorosłego.

Jeśli coś cię zaniepokoi, powiedz rodzicowi albo innemu zaufanemu dorosłemu. Nikt nie oczekuje, że ze wszystkim poradzisz sobie bez pomocy.

Czas na quiz!

1. Dlaczego oszust może chcieć przejąć konto dziecka w grze?

- A. Bo konta dzieci nie mają żadnej wartości
- B. Bo chce za darmo pomóc w przejściu trudnego poziomu
- C. Bo przedmioty i postępy w grze da się sprzedać
- D. Bo gra co roku sama przekazuje konta innym

Prawidłowa odpowiedź: C. Bo przedmioty i postępy w grze da się sprzedać

Konta w grach mają wartość – przedmioty, skiny i postępy da się sprzedać. Dlatego chroń je długim hasłem i logowaniem dwuetapowym.

2. Dostajesz wiadomość: „Masz 5 minut, inaczej konto zostanie usunięte. Kliknij tutaj!”. Co to najczęściej oznacza?

- A. Próbę oszustwa – pośpiech ma cię nabrać
- B. Ważną wiadomość od gry, trzeba kliknąć od razu
- C. Błąd w aplikacji, który sam zniknie
- D. Prezent od twórców gry dla najlepszych graczy

Prawidłowa odpowiedź: A. Próbę oszustwa – pośpiech ma cię nabrać

Pośpiech to typowa sztuczka oszustów: nie dają czasu na myślenie. Nie klikaj. Pokaż wiadomość dorosłemu albo sprawdź konto, otwierając aplikację samodzielnie, nie przez link.

3. Które informacje oszust najchętniej by od ciebie zdobył?

- A. Ulubiony kolor twojego plecaka
- B. Prognozę pogody na jutro
- C. Tytuł filmu, który oglądała cała klasa
- D. Hasło, adres domu i nazwę szkoły

Prawidłowa odpowiedź: D. Hasło, adres domu i nazwę szkoły

Hasło otwiera konto, a adres i szkoła mówią, gdzie cię znaleźć. Tych informacji nie podawaj obcym w internecie.

Materiały możesz bezpłatnie drukować i kopiować na potrzeby zajęć.