

# Ochrona przed wirusami komputerowymi

scenariusz lekcji dla uczniów szkół podstawowych klas 1-3



## ***Przegląd***

Lekcja ta została zaprojektowana z myślą o dzieciach chodzących do klasy trzeciej szkoły podstawowej i przynależy do scenariuszy stworzonych dla uczniów pierwszego etapu edukacyjnego.

Scenariusz ten koncentruje się na wypracowaniu odpowiednich reakcji na sytuacje stanowiące zagrożenie dla komputerów dzieci, takich jak ściąganie z Internetu wirusów i innych złośliwych programów. Obejmuje także inne zagrożenia, takie np. wyludzanie informacji lub próby włamania do komputera. Opiera się on na założeniu, że w większości sytuacji ryzykownych dziecko będzie pozostawało samo i że zapewnienie mu ochrony, wymaga nauczenia pewnych podstawowych, automatycznych reakcji na najbardziej typowe zagrożenia.

## ***Agenda***

- Sprawy organizacyjne (3 min.)
- Wprowadzenie (7 min.)
- Zaintrygowanie (15 minut)
- Rysunek (15 minut)
- Podsumowanie (20 minut)

## ***Cele***

- Zbudowanie w uczniach świadomości tego, że nieprzemyślane klikanie na wyskakujące okna i linki może doprowadzić do popsucia komputera.
- Wycwiczenie podstawowych strategii reagowania na potencjalnie ryzykowne sytuacje w Internecie.

## ***Przygotowanie***

Jedynym narzędziem, potrzebnym do realizacji zajęć jest program do rysowania (Paint, Paint 3D, Photoshop lub inny). W ostateczności uczniowie mogą korzystać z przyborów do rysowania (kredki, flamastry i papier).

## Przebieg lekcji

### Sprawy organizacyjne (3 min.)

Sprawdzenie obecności.

Inne sprawy organizacyjne.

### Wprowadzenie (7 min.)

**Spytaj dzieci, które z nich korzystają już z komputera.** Poproś, żeby powiedziały Ci, co na nim robią – możesz spisać najważniejsze hasła na online tablicy (np. gry, YouTube, słuchanie muzyki itd.).

**Spytaj, czy któreś z nich kiedykolwiek popsło komputer.** Nie wchodź w szczegóły tego, co znaczy „popsuć” – wystarczy, że skierujesz ich uwagę na istnienie takiego ryzyka.

### Zaintrygowanie (15 min.)

Powiedz, że przedstawiś im historię.

*Był sobie chłopak, o imieniu Maciek, który bardzo lubił grać w gry komputerowe. Tata pozwalał mu w soboty i niedziele zagrać na swoim komputerze. Był to komputer, którego tata Maćka używał też do pracy, do robienia przelewów bankowych i do zakupów przez Internet. Maciek bardzo chciał dostać najnowszą grę strategiczną, reklamowaną w telewizji – ale rodzice powiedzieli mu, że jest za droga i na razie nie mogą mu jej kupić. Maciek był bardzo smutny, aż do momentu, w którym dowiedział się od kolegi w szkole, że może tę grę ściągnąć bezpłatnie z Internetu. Wprawdzie Maciek domyślał się, że jest to nielegalne i nie wolno tego robić, ale kolega powiedział mu, że nikt mu z tego powodu nic nie zrobi. Maciek po powrocie do domu włączył więc komputer, znalazł nielegalną kopię gry w Internecie i zainstalował ją na komputerze taty. Wprawdzie, kiedy ją ściągał, program antywirusowy na komputerze wyświetlił informację, pisząc, że jest to program, który może być niebezpieczny, ale Maciek zignorował ostrzeżenie.*

*Przez dwa dni udawało mu się grać bez problemu, aż do momentu, kiedy gra zawiesiła się i więcej nie udało mu się jej włączyć. Przez jakiś czas był z tego powodu zmartwiony, aż w końcu odinstalował ją i zapomniał o całej sprawie.*

*Tymczasem kilka dni później jego tato przyszedł do domu bardzo zdenerwowany i powiedział mamie, że z jego karty kredytowej ukradziono bardzo dużo pieniędzy. Najdziwniejsze było to, że złodzieje mieli wszystkie dane jego karty – a tata nigdy ich nikomu nie podawał.*

*Okazało się, że na jego komputerze ktoś zainstalował program, który zapisał i wysłał do złodziei dane jego karty kredytowej, kiedy tata płacił nią za zakupy. Tata nie miał jednak pojęcia, jak to się mogło stać. Nie wiedział, że gdy Maciek instalował na jego komputerze piracką – czyli nielegalną - wersję gry, do gry tej dołączony był wirus, który zapisywał wszystko co ktokolwiek robił na komputerze. Przez to dane karty kredytowej taty Maćka zostały wykradzione i złodzieje mogli zabrać z niej pieniądze. Tata w końcu zorientował się, że była to wina Maćka i był na syna bardzo zły. Ale i tak nigdy nie udało się im już odzyskać większości ze straconych pieniędzy.*

**Po zakończeniu spytaj ich, co zrobił Maciek niewłaściwie.** Posłuchaj odpowiedzi i wydobądź z nich dwa kluczowe wątki, podkreślając i mówiąc wprost, że to są dwa największe błędy Maćka:

- **zainstalowanie nielegalnej gry** – warto tutaj odwołać się do tematów takich jak uczciwość i przestrzeganie prawa,
- **fakt, że Maciek nie powiedział rodzicom o tym, co zrobił** – to kluczowy wątek tej lekcji.

Te dwa błędy warto zapisać na online tablicy.

Zapytaj dzieci, czy wiedzą, **co jeszcze złego mogło się wydarzyć w wyniku zarażenia komputera wirusem.** Jeżeli pojawią się właściwe odpowiedzi, zapisz je też na tablicy.

Gdy skończycie robić listę, spytaj dzieci, **w jakich sytuacjach powinny dać znać rodzicom, że dzieje się coś nieprzewidzianego.** Słuchaj odpowiedzi uważnie i podkreślaj te, które będą szczególnie trafne, a następnie zapisuj je na online tablicy. Wprawdzie dużo zależy od kompetencji technicznych zarówno dziecka, jak i jego rodziców, jednak warto przekazać dzieciom, że **w sytuacji, w której komputer robi coś dziwnego lub zaskakującego, zawsze lepiej, aby powiedziało o tym rodzicom.**

### **Rysunek (15 min.)**

Poproś uczniów o uruchomienie aplikacji do rysowania (np. Paint, Photoshop lub inny) a następnie **poproś uczniów o narysowanie obrazków, pokazujących, jak wyglądają wirusy komputerowe, ukryte w ładnym opakowaniu** – np. w prezencie. Daj im na to 5 minut. Dla uczniów niemających żadnych programów do rysowania poproś o przygotowanie przyborów do rysowania, a następnie wykonania zadania offline.

Po 10 minutach możesz poprosić uczniów o udostępnienie swoich ekranów i pokazania obrazków lub w przypadku uczniów wykonujących zadanie na kartce papieru poproś o ich krótkie zaprezentowanie.

## **Podsumowanie (5 min.)**

Podsumuj zajęcia, powtarzając uczniom dwa wnioski i zapisując je na online tablicy, które prawdopodobnie pojawiły się już wcześniej, w trakcie lekcji:

- **w sytuacji, kiedy ich komputer zrobi coś dziwnego lub zaskakującego, najlepiej aby powiedzieli o tym rodzicom, gdyż brak reakcji może doprowadzić do realnych problemów,**
- **nigdy nie powinni instalować programów, znalezionych w Internecie, o których nie mają pewności, że są bezpieczne.**

## **Materiały do przeprowadzenia lekcji**

### **Co może stać się z zainfekowanym komputerem**

Warto w trakcie lekcji, bezpośrednio po omówieniu historii Maćka, stworzyć z dziećmi katalog zagrożeń, które mogą bezpośrednio lub pośrednio być wynikiem zainfekowania ich komputerów przez złośliwe oprogramowanie. Jest prawdopodobne, że wiele z tych zagrożeń dzieci będą w stanie same wymieniwać, jednak jeżeli czegoś zabraknie na tej liście, możesz to dodać. Lista ta ma charakter ogólny, nie techniczny – bardziej służy dostrzeżeniu przez dzieci rodzajów zagrożeń niż ich edukacji informatycznej.

### **Zepsucie komputera**

Najbardziej oczywiste skojarzenie przy wirusie to ryzyko niewłaściwego działania sprzętu. W praktyce wirusy nie psują komputera „fizycznie“, ale prowadzą do wykasowania części potrzebnych do działania danych, co oznacza konieczność np. ponownej instalacji systemu, a czasami wręcz zakupu nowych części, np. dysku twardego. „Zepsucie“ może oznaczać także pojawianie się bez powodu wyskakujących okienek, dźwięków czy innych zakłóceń, utrudniających normalne korzystanie z komputera.

### **Kradzież plików**

Wiele wirusów jest w stanie przestać pliki umieszczone na dysku komputera gdzieś do osoby, która stworzyła wirusa. W większości wypadków nie niesie to ze sobą poważniejszych konsekwencji, bo nawet jeżeli trzymamy na komputerze zdjęcia czy gry, ich kradzież nie da zbyt wiele korzyści hakerom. Gorsza sytuacja ma miejsce, jeżeli na dysku komputera mieliśmy dokumenty związane z naszą pracą, dane wrażliwe lub tajne, których opublikowanie czy przechwycenie może mieć poważne konsekwencje.

### **Kradzież loginów i haseł**

Istnieją programy, których celem jest wykradanie i dostarczanie złodziejom danych logowania do różnych kont, stworzonych w Internecie. I tak, jak w przypadku plików, jeżeli w wyniku działania takiego programu wykradzione zostanie hasło do sklepu internetowego albo do gry, nie ma to jeszcze poważnych konsekwencji – gorsze skutki może jednak mieć zdobycie przez przestępców hasła do poczty mailowej, konta na Facebooku czy też, w najgorszym przypadku do banku.

## **Kasowanie danych**

Część wirusów może po prostu usunąć niektóre lub nawet wszystkie nasze pliki. Dlatego też tak ważne jest zabezpieczanie się poprzez tworzenie kopii zapasowych naszych wszystkich dokumentów. Dzisiaj jest to znacznie łatwiejsze niż kiedyś, choćby dzięki tzw. „dyskom chmurowym“, które pozwalają nam trzymać wszystkie dane na zewnętrznych serwerach i w razie awarii naszego komputera, odzyskać je w kilka minut.

## **Rozsyłanie spamu**

Obecnie istnieje wiele rodzajów złośliwego oprogramowania, które może służyć do wysyłania spamu, a więc tzw. śmieciowej poczty z naszego komputera. W efekcie nasi znajomi mogą otrzymywać wiadomości z reklamami lub pozornie wysłane przez nas zachęty do wejścia na jakąś stronę internetową, co spowoduje także zarażenie ich komputera wirusem.

Ta lista nie wyczerpuje oczywiście wszystkich zagrożeń związanych ze złośliwym oprogramowaniem – jednak z punktu widzenia uczniów klas 1-3 wystarczy do przekazania im podstawowego komunikatu: należy uważać na to, co robią w Internecie i jakie programy z niego ściągają.