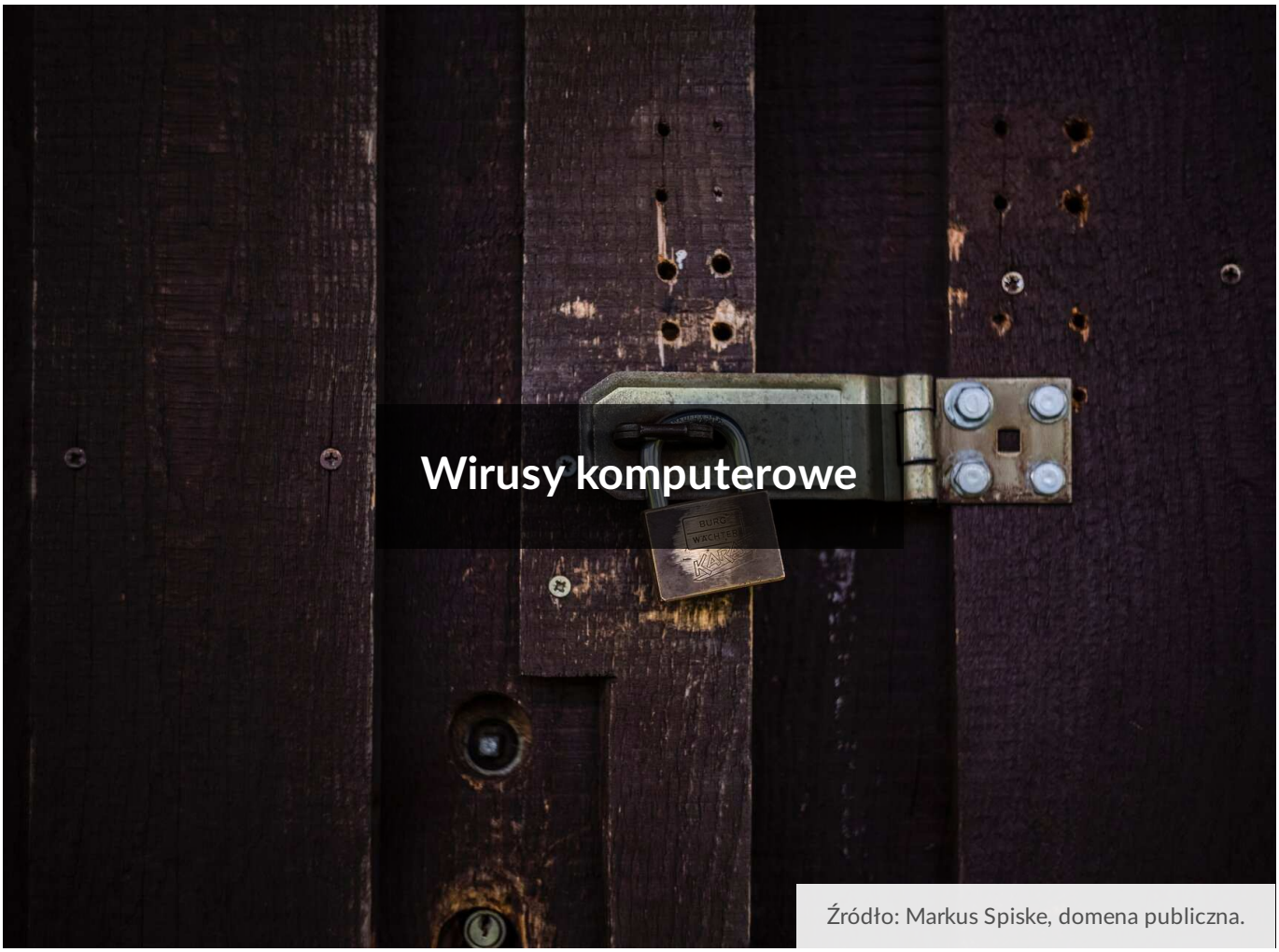
Wirusy komputerowe



Źródło: Markus Spiske, domena publiczna.

Przypomnij sobie, jak w filmach przedstawiany jest atak wirusa komputerowego. Być może przed oczami masz czerwony migający napis. Często działanie wirusa jest dużo mniej spektakularne – a przynajmniej pod względem wizualnym.

Komputery i inne urządzenia elektroniczne na stałe wpisały się w codzienność milionów użytkowników – pandemia koronawirusa Covid-19 dokonała pod tym względem prawdziwej rewolucji, uczyliśmy się i pracowaliśmy, nie ruszając sprzed monitora.

Przywiązanie użytkowników do sieci i jej dobrodziejstw nie uszło uwadze przestępców. Osoby, które wykorzystują komputery i sieć by powodować szkodę, mogą zagrażać właściwie każdemu.

Używając komputera powinniśmy mieć świadomość związanych z tym zagrożeń, a także ich przyczyn oraz negatywnych skutków.

Więcej informacji na temat wirusów komputerowych znajdziesz w e-materiałach:

- Wirusy komputerowe – implementacja w języku C++,
- Wirusy komputerowe – implementacja w języku Java,
- Wirusy komputerowe – implementacja w języku Python.

> **Twoje cele**

- Wyjaśnisz pojęcie „złośliwe oprogramowanie”.
- Rozróżnisz odmiany złośliwego oprogramowania.
- Opiszesz, w jaki sposób ograniczyć ryzyko zainfekowania komputera złośliwym oprogramowaniem.

Przeczytaj

Czym jest złośliwe oprogramowanie?

Termin „złośliwe oprogramowanie” jest pojęciem bardzo szerokim. Obejmuje ono świadomie przygotowane fragmenty kodu i programy, których działanie jest szkodliwe zarówno dla systemu operacyjnego komputera, telefonu czy tabletu (i innych urządzeń korzystających z sieci Internet), jak i ich użytkownika.

Istnieje wiele odmian złośliwego oprogramowania. Zależnie od rodzaju służy ono do wykradania danych i wrażliwych informacji z systemu operacyjnego ofiary, niszczenia plików (przypadkowych lub wybranych) albo do całkowitego uniemożliwienia pracy z komputerem.

Wirusy

Wirusami komputerowymi nazywamy programy, które po uruchomieniu są w stanie dokonać własnej replikacji poprzez modyfikację istniejących procesów i wstrzykiwanie do nich swojego kodu. Gdy replikacja się powiedzie, zmodyfikowane pliki i procesy nazywamy zainfekowanymi przez wirusa.

Wirusy mogą być niezwykle szkodliwe dla systemu operacyjnego. Często powodują jego awarie, niszczą lokalne pliki lub zauważalnie zwiększają zużycie zasobów urządzenia (pamięci operacyjnej, czasu procesora, przestrzeni dyskowej). Mogą również wykradać wrażliwe dane użytkowników.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Do skutecznego wykrywania i neutralizacji działań wirusów stosuje się programy antywirusowe. Dostępne są zarówno narzędzia bezpłatne, jak i komercyjne, dostarczane np. przez producentów systemów operacyjnych. Trzeba zdawać sobie jednak sprawę z faktu, że autorzy złośliwego oprogramowania stale wymyślają nowe sposoby ukrywania się w systemie przed programami antywirusowymi. Może to być nowa metoda wstrzykiwania lub bardziej skomplikowany wariant obfuskacji własnego kodu. Walka między twórcami wirusów a dostawcami programów antywirusowych trwa nieustannie.

Robaki

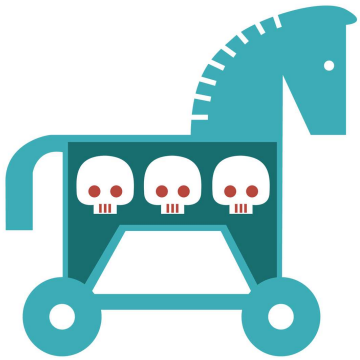
Robaki – podobnie jak wirusy – mają zdolność replikacji i rozprzestrzeniania się. Tym, co odróżnia je od wirusów, jest samodzielność. Powielanie robaków następuje bez wykorzystania istniejących plików lub procesów. Robaki najczęściej rozprzestrzeniają się przez sieci komputerowe (w tym Internet), wykorzystując luki systemu operacyjnego albo posługując się technikami manipulacji.

Po zainfekowaniu systemu operacyjnego ofiary robaki mogą niszczyć pliki, wysyłać wiadomości pocztą elektroniczną lub po prostu biernie czekać na instrukcje od atakującego. Komputery zarażone robakami niejednokrotnie tworzą botnety, czyli sieci zainfekowanych maszyn wykorzystywanych do przeprowadzania dalszych ataków. Dzięki temu atakujący zyskuje większą anonimowość oraz moc obliczeniową.

Konie trojańskie (trojany)

Konie trojańskie (popularnie nazywane trojanami) to programy, które wprowadzają użytkownika w błąd co do ich rzeczywistego działania. Oprogramowanie tego rodzaju udaje przydatne aplikacje, w istocie jednak realizuje zadania inne, niż sugeruje opis – np. oprócz katalogowania zdjęć wykrada dane z książki adresowej albo niszczy wybrane pliki na dysku urządzenia, np. komputera. Sama nazwa „koń trojański" jest nawiązaniem do podarunku, który przyczynił się do upadku Troi.

Najczęstszą przyczyną zainfekowania komputera trojanem jest pobieranie plików z nieautoryzowanych źródeł. Atakujący często modyfikują kod takich aplikacji, aby użytkownik nie zauważył różnicy między zmodyfikowaną a oryginalną wersją programu. Konie trojańskie zazwyczaj nie podejmują prób dokonania samoreplikacji. Natomiast ze względu na działanie mogą być równie szkodliwe jak wirusy komputerowe.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

> **Ważne!**
>
> Do nieautoryzowanych źródeł możemy zaliczyć serwisy, w których to użytkownicy udostępniają programy do pobrania (często nielegalne kopie). Jednak nieautoryzowanym źródłem mogą być nie tylko serwisy P2P, ale też strony, które zamiast przekierować użytkownika na witrynę wydawcy oprogramowania, umieszczają pliki na swoich serwerach, z których użytkownik pobiera dany program.

Oprogramowanie szpiegujące

Aplikacje, które gromadzą informacje na temat użytkownika bez jego wiedzy i zgody, nazywamy oprogramowaniem szpiegującym. Może ono zbierać dane takie jak numery kart

kredytowych, loginy i hasła, treść dokumentów przechowywanych na dyskach albo sprawdzać aktywność użytkownika w internecie (np. tworzyć listę odwiedzanych stron WWW). Zazwyczaj oprogramowanie szpiegujące jest jednym z elementów większego zestawu złośliwego oprogramowania.

Bomby dekompresyjne

Bomba dekompresyjna jest złośliwym plikiem. Twórcy bomb dekompresyjnych wykorzystują metody kompresji i dekompresji archiwów, aby utworzyć plik, który po rozpakowaniu jest bardzo duży – zazwyczaj powiększa się do kilku petabajtów. Obecnie bomby dekompresyjne są skutecznie wykrywane przez programy antywirusowe i nie stanowią dużego zagrożenia.

Ograniczenie ryzyka zainfekowania systemu

Aby zmniejszyć ryzyko zainfekowania komputera (ale też telefonu czy tabletu) złośliwym oprogramowaniem należy przede wszystkim stosować programy antywirusowe. Do wyboru mamy zarówno aplikacje płatne, jak i darmowe; warto się nimi zainteresować w celu zwiększenia poziomu bezpieczeństwa systemu.

Bardzo ważne jest także świadome korzystanie z komputera. Przeglądając zasoby internetu, należy stale pamiętać, że w globalnej sieci można paść ofiarą złośliwego oprogramowania.

Podczas sprawdzania skrzynki odbiorczej poczty elektronicznej nie należy klikać hiperłączy znajdujących się w podejrzanych wiadomości e-mail. Poza tym oprogramowanie zawsze należy pobierać ze strony producenta lub innego autoryzowanego źródła. Powinniśmy również odwiedzać wyłącznie zaufane strony internetowe.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Innym sposobem na to, by zabezpieczyć siebie i swój komputer czy telefon przed złośliwym oprogramowaniem, jest wykonywanie regularnych aktualizacji systemu operacyjnego oraz oprogramowania zainstalowanego na urządzeniu.

> **Ciekawostka**
>
> W 2018 roku pewien haker wykradł bazę danych sklepu Morele.net – doprowadziło to do wycieku danych ponad 2 miliony użytkowników. Serwis nie zdecydował się na wykupienie danych od hakera – w konsekwencji klienci sklepu zaczęli otrzymywać SMS-y, w których informowano ich, że muszą dopłacić złotówkę do jakiegoś zamówienia.

> Link z wiadomości prowadził do bramki płatności elektronicznej, która umożliwiała oszustowi zdobycie loginu i hasła do banku.
>
> Urząd Ochrony Danych Osobowych nałożył na spółkę karę 600 tys. euro (prawie 3 miliony złotych). Urząd w ten sposób motywował swoją decyzję:
>
> “ Morele.net, mając na uwadze, że przetwarza dane osobowe 2,2 mln osób, a także zakres tych danych i kontekst, powinno skutecznie oceniać związane z tym ryzyko i zagrożenia.

Słynne wirusy i robaki

Jednym ze znanych wirusów, który doprowadził do wyłączenia serwerów mailowych firmy Microsoft, była **Melissa**. Złośliwe oprogramowanie rozprzestrzeniało się przez wiadomości e-mail – po aktywacji program wysyłał wiadomość do 50 osób ze skrzynki e-mail ofiary.

Innym programem (robakiem), który przyprawił wielu użytkowników o ból głowy, był robak **ILOVEYOU**. Do wiadomości e-mail dołączony był plik `LOVE-LETTER-FOR-YOU.TXT.vbs`. Tak jak w przypadku Melissy, po aktywacji robaka program przesyłał e-mail 50 kolejnym adresatom. Robak ponadto kopiował się i ukrywał w różnych folderach na dysku. Do rejestru w systemie operacyjnym MS Windows dodawał również klucze, usuwał pliki, zastępując je kopiami samego siebie. Co więcej, był w stanie ściągnąć z sieci plik o nazwie `WIN-BUGSFIX.EXE`, który odpowiedzialny był za wykradanie haseł.

Melissa oraz ILOVEYOU to programy, które siały spustoszenie pod koniec ubiegłego wieku. W 2012 r. program **Flame** został uznany za najbardziej rozwiniętego technologicznie robaka.

Ten robak waży prawie 20 megabajtów. W paczce znajduje się np. maszyna wirtualna oraz biblioteki umożliwiające kompresję.

Główne zadanie Flame'a to wykradanie danych – jest w stanie nawet nagrywać dźwięk z mikrofonu czy zbierać informacje pochodzące ze znajdujących się w pobliżu urządzeń z interfejsem Bluetooth. Flame potrafi też rozprzestrzeniać się nie tylko przy pomocy sieci lokalnej, ale przez strony internetowe, maile czy za pośrednictwem dysków zewnętrznych. Atakuje zarówno instytucje rządowe, jak i osoby prywatne.

Inne wirusy, o których warto poczytać to **CryptoLocker**, **Stuxnet**, **My Doom** czy **Code Red**.

Słownik

> **botnet**
>
> grupa komputerów zainfekowanych szkodliwym oprogramowaniem; połączoną moc obliczeniową wielu jednostek atakujący wykorzystują np. do rozsyłania spamu,

przeprowadzania ataków DDoS lub łamania haseł
DDoS (ang. *distributed denial of service*, rozproszona odmowa usługi)

atak na system komputerowy lub usługę sieciową, który ma na celu uniemożliwienie działania; dzieje się tak przez zajęcie wszystkich wolnych zasobów; atak jest przeprowadzany równocześnie z wielu komputerów
manipulacja

stosowanie środków psychologicznych i metod mających na celu wyłudzenie informacji bądź nakłonienie do wykonania pewnych czynności
obfuskacja

technika przekształcania programów, która zachowuje ich działanie, ale znacząco utrudnia analizowanie ich kodu; istnieją trzy główne rodzaje transformacji obfuskacyjnych: transformacja wyglądu, transformacja danych i transformacja kontroli
P2P (ang. *peer to peer*)

sieć, która służy głównie do dzielenia się plikami pomiędzy użytkownikami internetu, przy użyciu odpowiedniej aplikacji

Animacja

Polecenie 1

Zapoznaj się z animacją. Wykonaj ćwiczenie.

Film dostępny pod adresem /preview/resource/R113dqO0bQAUu

Film nawiązujący do treści materiału: Wirusy komputerowe.

Ćwiczenie 1

Poszukaj informacji na temat głośnych przypadków cyberprzestępstw. Na czym polegały? Czy można było ich uniknąć?

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Wskaż, co nazywamy złośliwym oprogramowaniem.

- ◯ Nieświadomie przygotowane fragmenty kodu i programy, które są szkodliwe dla systemu operacyjnego lub jego użytkownika.
- ◯ Świadomie przygotowane fragmenty kodu i programy, które są szkodliwe dla systemu operacyjnego lub jego użytkownika.

Ćwiczenie 2

Wskaż, co jest charakterystyczną cechą wirusów komputerowych.

- ◯ Wprowadzają w błąd użytkownika, jeśli chodzi o ich rzeczywiste działanie.
- ◯ Są w stanie dokonać samoreplikacji poprzez modyfikację istniejących procesów i wstrzykiwanie do nich własnego kodu.
- ◯ Są w stanie dokonać samoreplikacji drogą internetową bez potrzeby wstrzykiwania własnego kodu do istniejących procesów.

Ćwiczenie 3

Wskaż zdanie prawdziwe.

- Robaki rozprzestrzeniają się, wykorzystując bomby kompresyjne, które polegają na tym, że cały system operacyjny kompresowany jest do jednego archiwum.
- Robaki rozprzestrzeniają się drogą internetową, wykorzystując luki systemu operacyjnego albo stosując techniki manipulacji.
- Robaki rozprzestrzeniają się wyłącznie poprzez pamięć zewnętrzną.

Ćwiczenie 4

Wskaż, czy konie trojańskie próbują dokonać samoreplikacji.

- nie
- tak

Ćwiczenie 5

Wskaż, jak nazywamy programy, które zbierają informacje o użytkowniku bez jego zgody.

- oprogramowanie śledzące
- oprogramowanie szpiegujące
- oprogramowanie monitorujące

Ćwiczenie 6

Zaznacz wszystkie zdania prawdziwe.

- [ ] Botnetem nazywamy komputer zainfekowany oprogramowaniem szpiegującym.
- [ ] Rozmiar bomb dekompresyjnych po dekompresji zazwyczaj sięga nawet kilku petabajtów.
- [ ] Można wyróżnić trzy główne rodzaje transformacji obfuskacyjnych.
- [ ] Pojęcie „trojan” nawiązuje do konia trojańskiego, który przyczynił się do upadku Troi.
- [ ] Aby ograniczyć ryzyko infekcji komputera, powinniśmy odwiedzać jedynie zaufane strony internetowe.

Ćwiczenie 7

Wstaw brakujące wyrażenia tak, aby tekst był prawdziwy.

Aby ograniczyć ryzyko infekcji komputera, powinno się stosować _____ _____, którymi warto się zainteresować w celu _____ poziomu ochrony systemu. Dodatkowo należy pamiętać, aby _____ oraz żeby wszelkie oprogramowanie pobierać ze strony producenta lub _____ dystrybutora.
Innym istotnym elementem profilaktyki jest regularne _____ _____.

systemu operacyjnego oraz oprogramowania

nie klikać hiperłączy znajdujących się w podejrzanych wiadomościach e-mail

nieautoryzowanego

wyłącznie systemu operacyjnego – wirusy nie przenoszą się poprzez inne oprogramowanie

Dostępne są zarówno płatne, jak i darmowe narzędzia, ale tylko płatne są tymi

Dostępne są zarówno płatne, jak i darmowe narzędzia

podniesienia

resetowanie

autoryzowanego

programy antywirusowe

aktualizowanie

nie klikać hiperłączy znajdujących się w podejrzanych wiadomościach e-mail (chyba że wiadomość pochodzi od kogoś, kogo znamy - wtedy jest bezpieczna)

obniżenia

programy antysystemowe

Ćwiczenie 8

Połącz w pary pojęcia z ich definicjami.

Obfuskacja	technika przekształcania programów, która zachowuje ich działanie, ale znacząco utrudnia analizowanie ich kodu
Manipulacja	stosowanie środków psychologicznych i metod mających na celu wyłudzenie informacji bądź nakłonienie do wykonania pewnych czynności
Botnet	grupa komputerów zainfekowanych szkodliwym oprogramowaniem, wykorzystywana na przykład do rozsyłania spamu, przeprowadzania ataków DDoS lub łamania haseł

Dla nauczyciela

Autor: Bartosz Zadrożny
Przedmiot: Informatyka

Temat: Wirusy komputerowe

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy

Podstawa programowa:

Cele kształcenia – wymagania ogólne

> V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

> V. Przestrzeganie prawa i zasad bezpieczeństwa.
>
> Zakres podstawowy. Uczeń:
>
> 4) opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Wyjaśnisz pojęcie „złośliwe oprogramowanie”.
- Rozróżnisz odmiany złośliwego oprogramowania.
- Opiszesz, w jaki sposób ograniczyć ryzyko zainfekowania komputera złośliwym oprogramowaniem.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda;
- telefony z dostępem do internetu.

Przebieg lekcji

Przed lekcją:

1. Uczniowie w grupach przygotowują prezentacje dot. słynnych przykładów cyberprzestępstw. Analizują, co się wydarzyło, z jakiego powodu, jakie miało skutki i czy dało się tego uniknąć.
2. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Wirusy komputerowe". Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Wyświetlenie przez nauczyciela tematu i celów lekcji. Określenie wiążących dla uczniów kryteriów sukcesu.
2. **Rozpoznanie wiedzy uczniów.** Uczniowie tworzą pytania dotyczące tematu zajęć, na które odpowiedzą w trakcie lekcji.

Faza realizacyjna:

1. Uczniowie w grupach prezentują przygotowane przez siebie wystąpienia.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Animacja". Uczniowie przygotowują krótką notatkę z podsumowaniem najważniejszych informacji.

3. **Ćwiczenie umiejętności.** Uczniowie wykonują indywidualnie ćwiczenia nr 1–5 z sekcji „Sprawdź się", a następnie dzielą się wynikami swojej pracy z kolegą lub koleżanką.

Faza podsumowująca:

1. Nauczyciel wyświetla na tablicy temat lekcji i cele zawarte w sekcji „Wprowadzenie". W kontekście ich realizacji podsumowuje przebieg zajęć, a także wskazuje mocne i słabe strony pracy uczniów.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 6–8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Animację można wykorzystać w dyskusji o tym, w jaki sposób uczniowie zabezpieczają swoje urządzenia przed cyberprzestępcami.