

Często zadawane pytania





Spis treści

PRZED INSTALACJĄ	4
JAKIE SĄ WYMAGANIA SYSTEMOWE TEGO PRODUKTU?	4
Windows	4
MAC	5
Android	5
iOS	5
Windows Phone 8	5
Obsługiwane jezyki	5
JAKIE SA RÓŻNICE W OCHRONIE INTERNETU NA POSZCZEGÓLNYCH SYSTEMACH OPERACYJNYCH?	6
Jak można sprawdzić używana wersje systemu Windows?	6
JAK USTALIĆ. CZY NA KOMPUTERZE JEST ZAINSTALOWANA 32- CZY 64-BITOWA WERSJA SYSTEMU WINDOWS XP?	7
JAK RECZNIE USUNAĆ Z KOMPUTERA INNY PROGRAM ANTYWIRUSOWY?	8
Czy można zainstalować produkt Ochrona Internetu na tablecie z systemem Windows RT?	9
MAM KOMPUTER Z SYSTEMEM WINDOWS 8. CZY OPROGRAMOWANIE OCHRONA INTERNETU JEST NADAL POTRZEBNE?	10
POBIERANIE I INSTALACIA OCHRONY INTERNETU	11
Jak się zalogować, aby zarządzać usługą Ochrona Internetu?	11
DLACZEGO NIE MOGĘ SIĘ ZALOGOWAĆ, ABY ZARZĄDZAĆ USŁUGĄ OCHRONA INTERNETU?	12
JAK POBRAĆ INSTALATOR PROGRAMU OCHRONA INTERNETU?	13
Pobieranie instalatora bezpośrednio na urządzenie	13
Wysyłanie instalatora na e-mail	15
Wysyłanie instalatora wiadomością SMS	18
Jak zainstalować Ochronę Internetu na komputerze z systemem Windows?	22
JAK ODINSTALOWAĆ OCHRONĘ INTERNETU Z KOMPUTERA?	23
OBSŁUGA OCHRONY INTERNETU	24
CO TO JEST PANEL GŁÓWNY?	24
OCHRONA INTERNETU	25
Co to jest Ochrona Internetu?	25
Co się stało z zaporą w systemie Windows?	25
JAK ZEZWOLIĆ APLIKACJI NA DOSTEP DO KOMPUTERA PRZEZ ZAPORĘ?	26
JAK TYMCZASOWO ZEZWOLIĆ NA CAŁY RUCH SIECIOWY?	26
JAK ZAPOBIEC POBIERANIU SZKODLIWYCH PLIKÓW PRZEZ APLIKACJE?	26
JAK ZEZWOLIĆ NA APLIKACJĘ ZABLOKOWANĄ PRZEZ FUNKCJĘ DEEPGUARD?	27
JAK EDYTOWAĆ USTAWIENIA FUNKCJI DEEPGUARD?	27
JAK WYŁĄCZYĆ WSZYSTKIE FUNKCJE ZABEZPIECZEŃ?	28
SKANOWANIE	29
	20
JAK WYKLUCZYC PLIK LUB FOLDER ZE SKANOWANIA ?	29
JAK WYKLUCZYC APLIKACJĘ ZE SKANOWANIA ?	30
JAK USUNĄC ZŁOŚLIWE OPROGRAMOWANIE Z FOLDERU KOSZ ?	31
PEŁNE SKANOWANIE KOMPUTERA PRZEBIEGŁO BARDZO SZYBKO. CZY PRODUKT NA PEWNO SZCZEGOŁOWO SPRAWDZIŁ CAŁY KOMPUTER?	31
CZY RĘCZNE SKANOWANIE DYSKOW TWARDYCH KAŻDEGO DNIA JEST KONIECZNE?	32
JAK WYCZYSCIC ZAINFEKOWANY FOLDER SYSTEM VOLUME INFORMATION LUB FOLDER FUNKCJI PRZYWRACANIE SYSTEMU?	33
USUWANIE PLIKÓW OPROGRAMOWANIA REKLAMOWEGO	35
CZYSZCZENIE TYMCZASOWYCH PLIKÓW INTERNETOWYCH W PROGRAMIE INTERNET EXPLORER	36
JAK PRZESYŁAĆ PRÓBKI DO FIRMY F-SECURE?	38

Zapisywanie raportu skanowania w pliku	
Zapisywanie w pliku wiadomości phishingowych, zawierających spam lub niepoprawnie uznanych za niebezpi	ieczne39
AKTUALIZACJE	40
Produkt wskazuje, że definicje wirusów są nieaktualne. Co mogę zrobić?	40
JAK SPRAWDZIĆ, CZY NAJNOWSZE AKTUALIZACJE SĄ ZAINSTALOWANE?	41
JAK MOGĘ SPRAWDZIĆ, CZY MÓJ KOMPUTER JEST CHRONIONY I AKTUALIZACJE AUTOMATYCZNE SĄ WŁĄCZONE?	42
Używam produktu Ochrona Internetu i chcę uaktualnić system Windows 7 do wersji Windows 8. Czy oprogramowan	NIE
ZABEZPIECZAJĄCE BĘDZIE DZIAŁAĆ PO UAKTUALNIENIU?	43
OCHRONA RODZICIELSKA	43
Co to jest Ochrona Rodzicielska?	43
JAK TWORZYĆ NOWE KONTA UŻYTKOWNIKÓW?	44
DLACZEGO NA KOMPUTERZE NALEŻY KORZYSTAĆ Z RÓŻNYCH KONT UŻYTKOWNIKÓW?	45
JAK OGRANICZYĆ CZAS, JAKI DZIECKO SPĘDZA NA PRZEGLĄDANIU INTERNETU?	45
JAK BLOKOWAĆ STRONY INTERNETOWE NA PODSTAWIE ICH ZAWARTOŚCI?	45
JAK AKTYWOWAĆ OCHRONĘ PRZEGLĄDANIA?	46
JAK WYŁĄCZYĆ WYŚWIETLANIE KLASYFIKACJI BEZPIECZEŃSTWA DLA WITRYN INTERNETOWYCH?	46
OCHRONA BANKOWOŚCI	47
Co to jest Ochrona bankowości?	47
Niektóre banki już oferują klientom rozwiązania zabezpieczające. Jakie korzyści zapewnia operatorowi taka usługa?	47
W JAKI SPOSÓB OCHRONA BANKOWOŚCI POPRAWIA MOJE BEZPIECZEŃSTWO W INTERNECIE?	47
JAKIE PRZEGLĄDARKI INTERNETOWE OBSŁUGUJE OCHRONA BANKOWOŚCI?	47
Czy Ochrona Bankowości działa na komputerze Mac?	48
CZY OCHRONA BANKOWOŚCI DZIAŁA NA TELEFONACH KOMÓRKOWYCH LUB TABLETACH?	48
JAK WŁĄCZYĆ OCHRONĘ BANKOWOŚCI?	48
DLACZEGO PRZEGLĄDARKA DZIAŁA NIEPRAWIDŁOWO PO UŻYCIU OCHRONY BANKOWOŚCI?	48
JAK ZEZWOLIĆ NA KORZYSTANIE Z INNYCH WITRYN PODCZAS SESJI BANKOWOŚCI ONLINE?	49
Jak dodać witrynę banku do listy chronionych witryn banków internetowych?	49
TRYB GIER	49
Co to jest tryb gier?	49
JAK WŁĄCZYĆ TRYB GIER DLA SYTEMU WINDOWS?	50

PRZED INSTALACJĄ

Jakie są wymagania systemowe tego produktu?

Obsługiwane platformy / systemy operacyjne / mobilne platformy operacyjne:

- Windows
- MAC
- Android
- iOS
- Windows Phone 8

Windows

Ochrona Internetu współpracuje z następującymi wersjami systemu operacyjnego Windows:

- Windows 8.1 32-bit i 64-bit: wszystkie wersje (nie obsługuje tabletek ARM)
- Windows 8 32-bit i 64-bit: wszystkie wersje (nie obsługuje tabletek ARM)
- Windows 7 32-bit i 64-bit: wszystkie wersje
- Windows Vista 32-bit i 64-bit: wszystkie wersje. Service Pack 2 lub nowszy.
- Windows XP 32-bit: Home, edycję Professional i Media Center : Service Pack 3 lub nowszy.

Wymagania systemowe:

Dla Microsoft Windows Vista, 7, 8 i 8.1:

- Procesor: Intel Pentium 4 lub porównywalne
- Pamięć: 1 GB lub więcej
- Wolne miejsce na dysku: przynajmniej 800MB
- Wymagane połączenie z Internetem w celu potwierdzenia subskrypcji i otrzymywania aktualizacji
- Włączony Javascript musi być włączony w ustawieniach przeglądarki użytkownika

Dla Microsoft Windows XP:

- Processor: Intel Pentium III 1GHz lub wyższy
- Pamięć: 512 MB lub więcej
- Wolne miejsce na dysku: przynajmniej 800MB
- Połączenie z Internetem jest wymagane w celu potwierdzenia subskrypcji i otrzymywania aktualizacji
- Javascript musi być włączony w ustawieniach przeglądarki użytkownika

Obsługiwane przeglądarki:

- Internet Explorer 11 (Windows 8.1) (32-bit i 64-bit)
- Internet Explorer 10 (Windows 8) (32-bit i 64-bit)
- Internet Explorer 10 & 11 (Windows 7) (32-bit i 64-bit)
- Internet Explorer 8 & 9 (Windows Vista) (32-bit i 64-bit)
- Internet Explorer 7 & 8 (Windows XP)

- Firefox (32-bit), dwie ostatnie główne wersje
- Chrome (32-bit), dwie ostatnie główne wersje.

Obsługiwane programy do odbioru poczty e-mail:

- Windows Mail
- Microsoft Outlook
- Microsoft Outlook Express
- Mozilla Thunderbird
- Opera Mail
- Eudora.

MAC

Ochrona Internetu współpracuje z następującymi systemami operacyjnymi:

- OS X version 10.6 (Snow Leopard, version 10.6.8 lub nowszy)
- OS X version 10.7 (Lion)
- OS X version 10.8 (Mountain Lion)
- OS X version 10.9 (Mavericks).

Wymagania systemowe:

- Intel procesor
- 250 MB wolnego miejsca na dysku
- Pamięć: 1 GB lub więcej
- Połączenie z Internetem jest wymagane w celu potwierdzenia subskrypcji i otrzymywania aktualizacji.

Android

Obsługuje urządzenia z systemem Android 2.2-4.3. Instalacja aplikacji wymaga około 6 MB wolnego miejsca na dysku

iOS

UWAGA: aplikacja będzie dostępna wkrótce

Obsługuje urządzenia Apples iPhone i iPad uruchomione na Apple iOS 6 i 7. Instalacja aplikacji wymaga około 2 MB wolnego miejsca na dysku.

Windows Phone 8

Obsługuje urządzenia działające na WP8 lub nowsze. Ze względu na ograniczenia systemu operacyjnego produkt jest dostępny tylko dla urządzeń z pamięcią 1 GB (nie mniej niż 512KB).

Obsługiwane języki

Polski Angielski

Jakie są różnice w Ochronie Internetu na poszczególnych systemach operacyjnych?

Ze względu na ograniczenia systemowe niektóre funkcjonalności Ochrony Internetu nie występują w niektórych systemach operacyjnych. Dostępność funkcjonalności na poszczególne systemy operacyjne można sprawdzić w poniższej tabeli.

Opis	Windows	Android	WP8	MAC	iOS
Ochrona zdjęć, filmów oraz prywatnych plików przed kradzieżą lub zniszczeniem	ТАК	ТАК	NIE	ТАК	NIE
Ochrona przed programami wymuszającymi okup	ТАК	ТАК	NIE	ТАК	NIE
Ochrona bankowości online zgodna z zaleceniami banków	ТАК	ТАК	ТАК	NIE	ТАК
Ochrona przed kradzieżą numeru karty kredytowej	ТАК	TAK	ТАК	ТАК	ТАК
Ochrona przed przejęciem Twoich kont w sklepach internetowych i portalach społecznościowych	ТАК	ТАК	ТАК	NIE	NIE
Pomoc w odnalezieniu telefonu, dzięki sygnałowi dźwiękowemu (nawet w przypadku wyciszonego dźwięku)	NIE	ТАК	NIE	NIE	NIE
Lokalizacja zagubionego telefonu, a w przypadku kradzieży możliwość blokady lub usunięcia wszystkich swoich danych znajdujących się w pamięci	NIE	ТАК	NIE	NIE	NIE
Ochrona konta w mediach społecznościowych	ТАК	ТАК	ТАК	NIE	NIE
Blokowanie połączeń, wiadomości SMS i MMS od niechcianych numerów	NIE	ТАК	NIE	NIE	NIE
Blokowanie dostępu do szkodliwych dla dzieci treści w internecie, takich jak: treści pornograficzne, obrazujące przemoc, związane z hazardem, czy też zachęcające i umożliwiające zdobycie narkotyków	ТАК	ТАК	ТАК	ТАК	ТАК
Określenie limitu czasu, jaki dziecko spędza surfując w Internecie	ТАК	NIE	NIE	NIE	NIE
Kontrola nad grami i aplikacjami, które Twoje dziecko instaluje na urządzeniu	NIE	ТАК	NIE	NIE	NIE
Blokowanie połączeń, wiadomości SMS i MMS od numerów, które mogą zagrażać Twojemu dziecku	NIE	ТАК	NIE	NIE	NIE
Lokalizacja urządzenia	NIE	ТАК	NIE	NIE	NIE

Jak można sprawdzić używaną wersję systemu Windows?

Wersję systemu operacyjnego można sprawdzić we właściwościach systemu Windows.

Aby sprawdzić właściwości systemu w systemie Microsoft Windows:

- 1. Kliknij przycisk Start.
- 2. Kliknij polecenie Panel sterowania.
- 3. Wykonaj jedną z następujących czynności:
 - W systemie Windows 7/8:
 - 1. Wybierz aplet System i zabezpieczenia.
 - 2. Kliknij pozycję **System**.
 - W systemie Windows Vista:
 - 1. Wybierz kategorię **Wydajność i konserwacja**.
 - Uwaga: na niektórych komputerach nie trzeba wykonywać tej czynności.
 - 2. Kliknij pozycję **System**. Zostanie otwarte okno Właściwości systemu.
 - W systemie Windows XP:

- 1. Wybierz kategorię **Wydajność i konserwacja**.
 - Uwaga: na niektórych komputerach nie trzeba wykonywać tej czynności.
- Kliknij dwukrotnie pozycję System. Zostanie otwarte okno Właściwości systemu. Uwaga: aby sprawdzić, czy system Windows XP jest w wersji 32-bitowej, czy 64-bitowej, kliknij tutaj.

Zostaną wyświetlone właściwości komputera, takie jak wersja systemu operacyjnego, informacje o procesorze i ilość pamięci RAM.

Jak ustalić, czy na komputerze jest zainstalowana 32- czy 64-bitowa wersja systemu Windows XP?

Wersję systemu Windows XP zainstalowaną na komputerze (32- lub 64-bitowa) można ustalić na kilka sposobów.

- 1. W przypadku używania klawiatury systemu Windows naciśnij jednocześnie klawisze **Windows** i **Pause/Break**, aby wyświetlić okno dialogowe Właściwości systemu. Jeśli w informacjach o systemie nie ma wzmianki o wersji 32- lub 64-bitowej, na komputerze jest zainstalowana 32-bitowa wersja systemu Windows XP.
- 2. Otwórz okno Mój komputer w celu sprawdzenia właściwości systemu:
 - 1. Kliknij przycisk **Start**.
 - 2. Kliknij prawym przyciskiem myszy ikonę **Mój komputer** i wybierz polecenie **Właściwości**. Zostanie otwarte okno Właściwości systemu.
 - 3. Na karcie Ogólne sprawdź treść pierwszego wiersza pod pozycją Komputer:
 - W 64-bitowych wersjach systemu XP będzie wyświetlana wartość Itanium lub Itanium 2.
 - W 32-bitowej wersji systemu Windows XP będzie wyświetlana inna wartość.
- 3. Otwórz narzędzie Winmsd.exe, aby sprawdzić typ systemu lub procesor:
 - 1. Wybierz kolejno opcje **Start > Uruchom**.
 - 2. W polu Otwórz wpisz winmsd.exe i kliknij przycisk OK.
 - 3. Wykonaj jedną z następujących czynności:
 - W okienku po prawej znajdź pozycję **Typ systemu** w kolumnie **Element**. Sprawdź wartość:
 - W 64-bitowej wersji systemu Windows XP ta wartość to Komputer z procesorem Itanium.
 - W 32-bitowej wersji systemu Windows XP ta wartość to Komputer z procesorem x86.
 - W okienku po prawej znajdź pozycję **Procesor** w kolumnie **Element**. Sprawdź wartość:
 - W 64-bitowej wersji systemu Windows XP ta wartość rozpoczyna się od ia64.
 - W 32-bitowej wersji systemu Windows XP ta wartość rozpoczyna się od x86.
- 4. Sprawdź wersję przy użyciu narzędzia diagnostycznego:
 - 1. Wybierz kolejno opcje Start > Uruchom.
 - 2. W polu Otwórz wpisz dxdiag i kliknij przycisk OK. Uwaga: W przypadku wyświetlenia okna dialogowego systemu Windows z monitem o potwierdzenie sterowników możesz bez obaw kliknąć przycisk Nie i kontynuować. Zostanie otwarte okno dialogowe Narzędzie diagnostyczne DirectX. Poczekaj, aż program zakończy ładowanie.

- 3. Znajdź pozycję **System operacyjny** w obszarze Informacje o systemie: w 64-bitowej wersji systemu Windows XP wyświetlana wartość to na przykład Microsoft Windows XP 64-bit Edition.
- 4. Znajdź pozycję **Procesor** w obszarze Informacje o systemie: w 64-bitowej wersji systemu Windows XP wyświetlana wartość to **Itanium** lub **Itanium2**.

Jak ręcznie usunąć z komputera inny program Antywirusowy?

Zaleca się używanie na komputerze tylko jednego dobrego produktu zabezpieczającego. Produkt zabezpieczający musi otworzyć plik, aby go przeskanować. Jeśli inny produkt zabezpieczający próbuje otworzyć ten sam plik w tym samym czasie, musi poczekać na zwolnienie pliku przez pierwszy produkt. Często powoduje to problemy — na przykład niepoprawne uruchamianie się programów lub awarie całego systemu.

Podczas instalacji produkt zabezpieczający automatycznie wykrywa i usuwa oprogramowanie oraz zapory **największych producentów**. Usunięcie tych programów może się jednak z różnych przyczyn nie powieść. W takim przypadku należy ręcznie usunąć produkty zabezpieczające lub zapory innych producentów. Można to też zrobić przed rozpoczęciem instalacji.

Ręczne usuwanie produktów zabezpieczających

Jeśli znasz nazwę produktu zabezpieczającego, możesz spróbować odinstalować go w następujący sposób:

- 1. Kliknij kolejno opcje **Start > Panel sterowania**.
- 2. Kliknij dwukrotnie aplet Dodaj lub usuń programy.
- 3. Jeśli produkt jest widoczny na liście obecnie zainstalowanych programów, usuń (odinstaluj) go.

Jeśli produktu nie można odinstalować, zwróć się o pomoc do dostawcy oprogramowania, prosząc ewentualnie o narzędzie do usuwania.

Poniżej można znaleźć szczegółowe instrukcje odinstalowywania dla kilku produktów zabezpieczających dostępnych obecnie na rynku:

- Odinstalowywanie oprogramowania AVG 6
- Odinstalowywanie oprogramowania PC-cillin
- Odinstalowwanie oprogramowania Ad-Aware
- Odinstalowywanie oprogramowania McAfee
- Odinstalowywanie oprogramowania Norton

Aby odinstalować oprogramowanie AVG 6:

- 1. Kliknij kolejno opcje **Start > Uruchom**.
- 2. W polu **Otwórz** wpisz tekst: "C:\Program Files\Grisoft\AVG6\Setup.exe /uninstall", a następnie kliknij przycisk **OK**.
- 3. Jeśli pojawi się pytanie, czy chcesz uruchomić program Virus Vault, kliknij przycisk Nie.
- 4. Jeśli pojawi się pytanie, czy chcesz kontynuować odinstalowywanie, kliknij przycisk Tak.
- 5. Wybierz opcję Uruchom ponownie komputer, a następnie kliknij przycisk OK.

Aby odinstalować oprogramowanie PC-cillin:

Odinstaluj produkt firmy Trend Micro przy użyciu zestawu narzędzi Trend Micro Diagnostic Toolkit.

Aby odinstalować oprogramowanie Ad-Aware:

- 1. Kliknij ikonę Mój komputer.
- 2. Przejdź do folderu C:\Program Files\Lavasoft\Ad-Aware.
- 3. Uruchom plik unregaaw.exe.
- 4. Usuń cały folder Ad-Aware.
- 5. Usuń łącze Lavasoft Ad-Aware z menu **Start** oraz ikony oprogramowania Ad-Aware z pulpitu (jeśli istnieją).
- 6. Przejdź do folderu C:\Documents and Settings\[Nazwa użytkownika]\Application Data\Lavasoft\
- 7. Usuń cały folder Lavasoft.
- 8. Opróżnij Kosz.
- 9. Ponownie uruchom komputer.

Aby odinstalować oprogramowanie McAfee:

Odinstaluj produkt firmy McAfee przy użyciu narzędzia McAfee Consumer Products Removal Tool (MCPR.exe). Narzędzie można wyszukać w Internecie, wpisując słowa kluczowe "McAfee Consumer Products Removal tool (MCPR.exe)".

Aby odinstalować oprogramowanie Norton:

Odinstaluj produkt zabezpieczający Norton przy użyciu narzędzia Nortol Removal Tool.

Więcej informacji

Jeśli jednak po zainstalowaniu produktu firmy F-Secure komputer nadal nie uruchamia się poprawnie, wykonaj następujące czynności:

- 1. Uruchom komputer w trybie awaryjnym.
- 2. Usuń produkt Ochrona Internetu.
- 3. Ponownie uruchom komputer.
- 4. Utwórz plik FSDiag. Instrukcje można znaleźć w artykule "Tworzenie pliku FSDiag".
- 5. Wyślij plik FSDiag do pomocy technicznej firmy F-Secure, tworząc odpowiednie zgłoszenie.

Czy można zainstalować produkt Ochrona Internetu na tablecie z systemem Windows RT?

Nie. Tablety i inne urządzenia oparte na platformie Windows RT nie są obsługiwane. Zwykłą wersję produktu Ochrona Internetu można jednak zainstalować na tablecie z procesorem Intel obsługującym system operacyjny Windows dla komputerów.

Mam komputer z systemem Windows 8. Czy oprogramowanie Ochrona Internetu jest nadal potrzebne?

Tak. System Windows 8 zawiera program Windows Defender oraz filtr SmartScreen dla przeglądarki Internet Explorer. Windows Defender to produkt oferujący tylko podstawowe funkcje ochrony antywirusowej bez zabezpieczeń opartych na analizie zachowań ani funkcji ochrony sieci. Mimo że filtr SmartScreen dla przeglądarki Internet Explorer oferuje podstawową ochronę podczas przeglądania Internetu, współdziała tylko z programem Internet Explorer, a jego możliwości są znacznie ograniczone w porównaniu z pełnym pakietem zabezpieczającym. Produkt Ochrona Internetu zapewnia znacznie wyższy poziom zabezpieczeń niż program Windows Defender dzięki dodatkowym funkcjom, takim jak Ochrona bankowości, technologia Deep Guard, obsługa wielu przeglądarek i skanowanie w sieci rozproszonej.

POBIERANIE I INSTALACJA OCHRONY INTERNETU

Jak się zalogować, aby zarządzać usługą Ochrona Internetu?

Usługa Ochrona Internetu pozwala na elastyczne zarządzanie dostępnymi licencjami oprogramowania chroniącego Twoje urządzenie. W każdej chwili możesz zmienić chronione urządzenie na inne – usunąć jedną licencję, aby zainstalować program na innym urządzeniu. Aby zarządzać usługą Ochrona Internetu należy się zalogować na stronie <u>http://www.plus.pl/zarzadzaj-chmura-ochrona</u>. Po zalogowaniu będziesz mógł:

- Ściągnąć oprogramowanie Ochrona Internetu
- Zobaczyć, na jakich urządzeniach zainstalowałeś dostępne licencje
- Usuwać licencje i instalować oprogramowanie ponownie na innych lub tych samych urządzeniach
- Zmieniać nazwy chronionych urządzeń

Aby się zalogować:

- 1. Wejdź na http://www.plus.pl/zarzadzaj-chmura-ochrona.
- 2. Gdy pojawi się okno "Zarządzanie usługami" wpisz w wyznaczone miejsce numer telefoniczny karty SIM, na którym jest aktywna usługa Plus Chmura. Następnie kliknij przycisk "Wyślij kod". Na podany przez Ciebie numer telefonu otrzymasz wiadomość SMS z kodem.

Lecowanie	
Aby się zalogować podaj num	er <u>MSISDN</u> kar nieszczonej w Twoim telefonie, modemie
lub routerze). Na podany num	ier zostalitier zostalitier zostalitier zostalitier zostalitier zostalitier zostalitier zostalitier zostalitier
Numer <u>MSISDN</u> karty SIM	+48 500 500 500
	wyshij kod

Uwaga:

Jeśli korzystasz z oferty **Plus Internet**, wiadomość SMS możesz odebrać wyjmując kartę SIM z routera lub modemu i przekładając ja do telefonu. Jeśli nie chcesz przekładać karty SIM, możesz zalogować się przez <u>Plus Online</u> (zakładka usługi).

3. Wpisz kod z wiadomości SMS w wyznaczone miejsce i kliknij "Zaloguj".

Logowani	3				
Aby się zalog lub routerze)	ować podaj numer <u>MSISDN</u> Na podany numer zostani	<u>N</u> karty SIM (umiesa ie wysłana wiadom	cczonej w Twoim te lość SMS z kodem. J	efonie, modemie ak odebrać kod?	
Numer <u>I</u>	SISDN karty SIM +48		×.		
	Kod SMS				
	Zal	loguj			

4. Pojawi się nowe okno, z którego będziesz miał dostęp do usługi Ochrona Internetu.

Plus Usłu	Jgi	٥
c	Ochrona Internetu Dhroni Twój komputer smatfon i tablet prsed wirusami, spamem, oprogramowaniem szpiegującym oraz niepożądanymi treściami w internecie.	Plus Chmura Bezpieczne przechowywanie plików tworzenie kopii zapasowej dołumentów, błyskawiczny dostęp i możliwość dzielenia się plikami z Twojego komputera oraz urządzeń mobilnych.
	Zainstaluj Dostępne licencje: 2 / 3	Zainstaluj Dostępny limit miejsca: 5GB <u>Otwórz usługe Plus Chmura</u>
woje urząc	dzenia Brak nazwy urząd Usuń Zainstaluj ponowni Licencja nie jest używana.	e

Uwaga: Jeśli posiadasz również Plus Chmurę, usługa ta będzie widoczna w oknie "Zarządzanie usługami". Będziesz mógł założyć konto do Plus Chmury lub (jeśli już je założyłeś) otworzyć usługę Plus Chmura oraz ściągnąć aplikację na swoje urządzenie.

Dlaczego nie mogę się zalogować, aby zarządzać usługą Ochrona Internetu?

Prawdopodobnie usługa nie została aktywowana. Możliwość zalogowania uzyskasz do **5 dni** roboczych licząc od dnia aktywowania usługi. Jeśli nie minęło jeszcze 5 dni, spróbuj zalogować się w późniejszym terminie.

Jak pobrać instalator programu Ochrona Internetu?

Pobieranie instalatora bezpośrednio na urządzenie

- 1. Zaloguj się na <u>http://www.plus.pl/zarzadzaj-chmura-ochrona</u>. (**Zobacz**: <u>Jak się zalogować, aby zarządzać usługą Ochrona Internetu?</u>)</u>
- 2. Po zalogowaniu, kliknij przycisk "Zainstaluj".

	l
Ochrona Internetu	18
Chroni Twój komputer, smartfon i tablet przed wirusami, spamem, oprogramowaniem szpiegującym oraz niepożadanymi treściami w internecie. Zainstaluj Dostępne licencje: 3 / 3	

3. Gdy pojawi się okno "Pobierz i zainstaluj", kliknij przycisk "Pobierz".

Pobierz i za	instaluj	\otimes
W j	aki sposób chcesz uzyskać instalator produktu Och Internetu?	
Pobierz	Pobierz instalator bezpośrednio.	obierz
Poczta e-mail	v	Vyślij
	Przykład: name@email.com	
	lub	
SMS	+48	Vyślij
	Przykład: +48601123456	

4. Program podpowie Ci z jakiego systemu operacyjnego korzystasz na danym urządzeniu. Jeśli ściągasz instalator na inny system operacyjny, zaznacz odpowiednią ikonę, a następnie kliknij przycisk "Dalej".



5. W wyznaczonym miejscu wpisz nazwę dla swojego urządzenia, na którym zainstalujesz oprogramowanie (np. Mój Komputer), a następnie kliknij "Dalej".

Nazwij urządzenie	\otimes
Nadaj nazwę dla urządzenia.	- 1
Windows Mój Komputer	
Wstecz Dalej	

6. Kliknij przycisk "Pobierz".



7. Zapisz plik na urządzeniu.

)twieranie Ochrona Internetu_	×
Rozpoczęto pobieranie pliku: Chrona Internetu_exe Typ pliku: Biococ Sila († 1 MP)	
Adres: https://download.sp.f-secur Czy zapisać ten plik?	e.com
	Zapisz plik Anuluj

Wysyłanie instalatora na e-mail

- 1. Zaloguj się na http://www.plus.pl/zarzadzaj-chmura-ochrona.
- 2. Po zalogowaniu, kliknij przycisk "Zainstaluj".

$\overline{\bigcirc}$
Ochrona Internetu
Chroni Twój komputer, smartfon i tablet przed wirusami, spamem, oprogramowaniem szpiegującym oraz niepożadanymi treściami w internecie. Zainstaluj
Dostępne licencje: 3 / 3

3. Gdy pojawi się okno "Pobierz i zainstaluj" wpisz w wyznaczone miejsce adres e-mail, na który chcesz wysłać instalator. Następnie kliknij przycisk "Wyślij", który znajduje się obok.

Pobierz i za	instaluj 🛞
W ja	aki sposób chcesz uzyskać instalator produktu Ochrona Internetu?
Pobierz	Pobierz instalator bezpośrednio.
	Przykład@poczta.pl Wyślij Przykład: name@email.com Iub
SMS	+48 Wyślij Przykład: +48601123456

4. Na podany adres e-mail zostanie wysłany link instalacyjny. Otwórz maila na urządzeniu, na którym chcesz zainstalować oprogramowanie i postępuj zgodnie z instrukcją podaną w mailu. Jeśli mail nie wyświetla się poprawnie, kliknij w swojej poczcie e-mail "Pokaż obrazki".



5. Po kliknięciu w link instalacyjny w przeglądarce otworzy się okno., gdzie należy wybrać system operacyjny urządzenia, na którym będzie instalowane oprogramowanie. Program podpowie Ci z jakiego systemu operacyjnego korzystasz na danym urządzeniu. Jeśli ściągasz instalator na inny system operacyjny, zaznacz odpowiednią ikonę, a następnie kliknij przycisk "Dalej".



6. W wyznaczonym miejscu wpisz nazwę dla swojego urządzenia, na którym zainstalujesz oprogramowanie (np. Mój Komputer), a następnie kliknij "Dalej".



7. Pobierz instalator i zapisz na urządzeniu.



Wysyłanie instalatora wiadomością SMS

- 1. Zaloguj się na http://www.plus.pl/zarzadzaj-chmura-ochrona.
- 2. Po zalogowaniu, kliknij przycisk "Zainstaluj".

Ochrona Internetu	
Chroni Twój komputer, smartfon i tablet przed wirusami, spamem, oprogramowaniem szpiegującym oraz niepo Zainstaluj Dostępne licencje: 3 / 3	

3. Gdy pojawi się okno "Pobierz i zainstaluj" wpisz w wyznaczone miejsce numer telefonu, na który chcesz wysłać instalator. Następnie kliknij przycisk "Wyślij", który znajduje się obok.

W ja	aki sposób chcesz uzyskać instalator produ Internetu?	uktu Ochrona
Pobierz	Pobierz instalator bezpośrednio.	Pobierz
Poczta e-mail		Wyślij
	Przykład: name@email.com	
SMS	+481234-6789	Wyślij
0100	+48123456789	Vvyślij

4. Na podany numer telefonu zostanie wysłana wiadomość SMS z linkiem instalacyjnym.



5. Program podpowie Ci z jakiego systemu operacyjnego korzystasz na danym urządzeniu. Jeśli ściągasz instalator na inny system operacyjny, zaznacz odpowiednią ikonę, a następnie kliknij przycisk "Dalej".

tident	ps://sateavenu /fikowaliśmy pla	tforme tego urządz	4
Liacin	jako: 'A	ndroid'	erna
To obsług klikną	ustawienie może iwaną platformę ć przycisk "Dalej	esz zmienić na inna poniżej, ale możes ", aby pobrać licen	ą z też cję.
		Mac	
	Android	Mac	
	Windows Phone	Windows	

6. W wyznaczonym miejscu wpisz nazwę dla swojego urządzenia, na którym zainstalujesz oprogramowanie (np. Mój Telefon), a następnie kliknij "Dalej".



7. Zostaniesz przekierowany do odpowiedniego sklepu, aby pobrać i zainstalować aplikację.



Jak zainstalować Ochronę Internetu na komputerze z systemem Windows?

Zanim będzie można rozpocząć instalację produktu zabezpieczającego, należy przygotować następujące elementy:

- produkt pobrany z Internetu (produkt pobierzesz po zalogowaniu na <u>http://www.plus.pl/zarzadzaj-chmura-ochrona</u>),
- połączenie z Internetem.

Jeśli komputer jest używany przez więcej niż jedną osobę i dla wszystkich tych osób utworzono konta użytkowników, przed rozpoczęciem instalacji należy się zalogować jako użytkownik z uprawnieniami administratora.

Uwaga: produktu nie można zainstalować na komputerze, na którym są używane inne programy antywirusowe lub zapory.

Podczas instalacji produkt zabezpieczający automatycznie wykrywa i usuwa oprogramowanie oraz zapory najpopularniejszych producentów. Usunięcie tych programów może się jednak z różnych przyczyn nie powieść. W takim przypadku należy ręcznie usunąć produkty zabezpieczające lub zapory innych producentów. Więcej informacji można znaleźć w artykule na temat usuwania oprogramowania zabezpieczającego innych producentów.

Instalowanie produktu zabezpieczającego

Po pobraniu pakietu instalacyjnego kliknij dwukrotnie plik instalatora (z rozszerzeniem exe), aby rozpocząć instalację.

Zostanie wyświetlone okno dialogowe Witamy w instalatorze oprogramowania.

- 1. Wybierz język i kliknij przycisk **Instaluj**. Zostanie wyświetlone okno z warunkami licencji.
- 2. Przeczytaj warunki licencji. Jeśli je akceptujesz, kliknij przycisk Akceptuję warunki licencji.
- 3. Po zaakceptowaniu warunków licencji rozpocznie się pobieranie plików. Może to potrwać kilka minut. Gdy pobieranie plików dobiegnie końca, zostanie wyświetlone okno Instalacja automatyczna.
- 4. Kliknij przycisk **Dalej**, aby kontynuować instalację. Zostanie wyświetlone okno Sieć ochrony w czasie rzeczywistym.
- 5. Jeśli chcesz przekazywać anonimowe dane do analiz w celu poprawy skuteczności wykrywania, kliknij przycisk Dalej. Jeśli nie chcesz przekazywać takich danych, przed kliknięciem przycisku Dalej usuń zaznaczenie opcji. Rozpocznie się usuwanie oprogramowania powodującego konflikty, a następnie instalacja programów Ochrona Internetu i Ochrona Rodzicielska.

Instalacja produktu dobiegła końca.

Uwaga: jeśli na komputerze działa system Windows XP, należy go ponownie uruchomić w celu dokończenia instalacji.

Aby otworzyć interfejs użytkownika produktu, kliknij ikonę Ochrona Internetu. Zostanie wyświetlony panel główny zawierający wszystkie zainstalowane aplikacje.



Aby otworzyć dowolną z dostępnych aplikacji, kliknij jej ikonę. W panelu głównym możesz też zmieniać wspólne ustawienia i zarządzać subskrypcjami. Po prostu kliknij prawym przyciskiem myszy ikonę znajdującą się najdalej na prawo w panelu głównym i wybierz odpowiednie polecenie w menu.

Jak odinstalować Ochronę Internetu z komputera?

Aby odinstalować produkt z systemu Windows XP:

- 1. Kliknij kolejno opcje **Start > Panel sterowania**.
- 2. Kliknij dwukrotnie aplet Dodaj lub usuń programy.
- 3. Przewiń widok do pozycji produktu Ochrona Internetu i kliknij przycisk Zmień/usuń.
- 4. Po wyświetleniu monitu ponownie uruchom komputer.

Aby odinstalować produkt z systemu Windows Vista:

- 1. Kliknij kolejno opcje **Start > Panel sterowania**.
- 2. Kliknij pozycję Odinstaluj program.
- 3. Przewiń widok do pozycji produktu Ochrona Internetu i kliknij przycisk Odinstaluj/zmień.
- 4. Po wyświetleniu monitu ponownie uruchom komputer.

Aby odinstalować produkt z systemu Windows 7 lub 8:

- 1. Kliknij kolejno opcje **Start > Panel sterowania**.
- 2. Kliknij dwukrotnie aplet **Programy i funkcje**.
- 3. Przewiń widok do pozycji produktu Ochrona Internetu i kliknij przycisk Odinstaluj/zmień.
- 4. Po wyświetleniu monitu ponownie uruchom komputer.

Obsługa Ochrony Internetu

Co to jest panel główny?

Po pobraniu instalatora sieciowego firmy F-Secure i zainstalowaniu produktu na komputerze z systemem Windows w dolnej części ekranu zostaje wyświetlony panel główny:



Jeśli panel główny nie jest widoczny, możesz go otworzyć przy użyciu ikony Ochrona Internetu na pulpicie lub na pasku zadań.

W panelu głównym widoczne są zainstalowane aplikacje:

- Ochrona Internetu
- Ochrona Rodzicielska
- Plus Chmura (w przypadku posiadania aplikacji Plus Chmura)

Możesz też skorzystać z menu Plus , które zawiera przydatne polecenia związane z zainstalowanymi aplikacjami:

- **Plus** otwiera witrynę internetową plus.pl.
- Wyświetl moje subskrypcje pokazuje informacje o subskrypcjach i instalacjach.
- **FAQ** otwiera witrynę internetową na której znajdują się odpowiedzi na najczęściej zadawane pytania.
- **Narzędzie pomocy technicznej** uruchamia narzędzie pomocy technicznej, które gromadzi dzienniki produktów w pliku fsdiag.zip na pulpicie.
- Tryb gier włącza/wyłącza tryb gier.
- Otwórz centrum akcji wyświetla listę akcji, które oczekują na działanie ze strony użytkownika.
- Otwórz historię powiadomień pokazuje powiadomienia aplikacji z przeszłości.
- Otwórz typowe ustawienia wyświetla ustawienia obowiązujące wszystkie aplikacje.
- **Sprawdź dostępność aktualizacji** sprawdza, czy dostępne są aktualizacje, i w razie potrzeby natychmiast je instaluje.

Uwaga: ze względów bezpieczeństwa zmiana niektórych ustawień wymaga uprawnień administratora.

Więcej informacji o panelu głównym:

1. Otwórz **> Pomoc**.

OCHRONA INTERNETU

Co to jest Ochrona Internetu?

Program Ochrona Internetu chroni komputer przed wszystkim rodzajami złośliwych ataków, uniemożliwiając wirusom, robakom i programom szpiegowskim przedostanie się do komputera. Blokuje także spam i phishing.

Rozwiązanie DeepGuard 5 zapewnia ochronę luk w zabezpieczeniach przy użyciu technologii dynamicznej, proaktywnej analizy działania, która skutecznie identyfikuje i zatrzymuje próby wykonywania szkodliwych operacji. Jest to kompleksowe zabezpieczenie punktu końcowego o minimalnych wymaganiach i niezauważalnym dla użytkownika działaniu.

Zapora uniemożliwia intruzom uzyskiwanie dostępu do komputera za pośrednictwem Internetu i chroni przed działaniami hakerów.

W przypadku korzystania z systemu Microsoft Windows 7 lub Windows 8 odpowiednie funkcje aplikacji zapewniają, że Twój rachunek telefoniczny za korzystanie z komórkowej transmisji danych nigdy Cię nie zaskoczy.

Uwaga: ze względów bezpieczeństwa zmiana niektórych ustawień wymaga uprawnień administratora.

Więcej informacji o sposobie obsługi programu Ochrona Internetu znajdziesz:

- 1. W panelu głównym F-Secure kliknij prawym przyciskiem myszy ikonę Ochrona Internetu Zostanie wyświetlone menu podręczne.
- 2. Po wybraniu polecenia **Pomoc**.

Co się stało z zaporą w systemie Windows?

Funkcja zapory w produkcie została przeprojektowana. Nowa zapora jeszcze bardziej ułatwia korzystanie z produktu.

Do obsługi podstawowych funkcji zapory, takich jak filtrowanie przychodzącego ruchu sieciowego, ustawienia zależne od lokalizacji oraz obsługa grupy domowej, produkt używa teraz wbudowanej Zapory systemu Windows. Poza podstawową ochroną zapewnianą przez Zaporę systemu Windows produkt oferuje następujące mechanizmy zabezpieczeń:

- Blokowanie pobierania programów wykorzystujących luki w zabezpieczeniach i innych niebezpiecznych plików. Każdy pobrany plik jest skanowany, a wszystkie szkodliwe pliki są automatycznie blokowane.
- Zapobieganie dostępowi podejrzanych aplikacji do Internetu. Jeśli nie można zweryfikować poziomu bezpieczeństwa aplikacji, funkcja DeepGuard rozpoczyna monitorowanie jej działań.

Na podstawie analizy tych działań funkcja DeepGuard zezwala lub nie zezwala na dostęp do sieci lub prosi użytkownika o podjęcie decyzji.

• Wykrywanie manipulowania przeglądarką. Funkcja DeepGuard wykrywa, czy złośliwe oprogramowanie próbuje manipulować przeglądarką użytkownika i blokuje takie działania.

Jak zezwolić aplikacji na dostęp do komputera przez zaporę?

Gdy zapora jest włączona, ogranicza dostęp do i z komputera. Niektóre aplikacje do poprawnego działania mogą wymagać zezwolenia na dostęp przez zaporę. Produkt zapewnia ochronę komputera za pomocą Zapory systemu Windows.

Aby zmienić ustawienia Zapory systemu Windows, wykonaj następujące czynności:

- 1. Otwórz program Ochrona Internetu.
- 2. Na głównej stronie programu Ochrona Internetu kliknij przycisk **Ustawienia**. **Uwaga**: do zmiany tych ustawień wymagane są uprawnienia administratora.
- 3. Wybierz opcje Ochrona Internetu > Zapora.
- Kliknij pozycję Zmień ustawienia zapory systemu Windows.
 Uwaga: do edytowania tych ustawień wymagane są uprawnienia administratora.

Więcej informacji na temat Zapory systemu Windows znajduje się w dokumentacji systemu Microsoft Windows.

Jak tymczasowo zezwolić na cały ruch sieciowy?

Wyłączenie zapory pozwala zezwolić na cały ruch sieciowy.

Ostrzeżenie: Wyłączanie zapory nie jest zalecane, ponieważ powoduje to narażenie komputera na ataki sieciowe. Jeśli aplikacja przestanie działać, ponieważ nie może nawiązać połączenia z Internetem, należy zmienić ustawienia zapory, a nie wyłączyć zaporę.

Włączanie i wyłączanie zapory:

- W panelu głównym otwórz program Ochrona Internetu
 Na konzie Stanowie Stanowi
- Na karcie Stan wybierz opcję Ustawienia.
 Uwaga: do wyłączania funkcji zabezpieczeń wymagane są uprawnienia administratora.
- 3. W ustawieniach programu Computer Security wybierz opcję Zapora.
- 4. Kliknij odpowiedni suwak, aby włączyć ulub Wyłączyć zaporę.

Jak zapobiec pobieraniu szkodliwych plików przez aplikacje?

Istnieje możliwość zapobiegania pobieraniu przez aplikacje szkodliwych plików z Internetu.

Niektóre witryny internetowe zawierają programy wykorzystujące luki w zabezpieczeniach i inne szkodliwe pliki, które mogą wyrządzić szkody na komputerze. Zaawansowana ochrona sieciowa umożliwia zapobieganie pobieraniu szkodliwych plików przez aplikacje, zanim takie pliki dotrą na komputer.

Aby zablokować pobieranie szkodliwych plików przez dowolną aplikację:

- 1. Otwórz program Ochrona Internetu.
- 2. Na stronie głównej programu Ochrona Internetu kliknij pozycję **Ustawienia**. **Uwaga**: zmiana ustawień wymaga uprawnień administratora.
- 3. Wybierz kolejno opcje **Ochrona Internetu > Zapora**.
- 4. Wybierz opcję **Nie zezwalaj aplikacjom na pobieranie szkodliwych plików**. **Uwaga**: to ustawienie jest aktywne nawet w przypadku wyłączonej zapory.

Jak zezwolić na aplikację zablokowaną przez funkcję DeepGuard?

Zdarza się, że funkcja DeepGuard blokuje uruchomienie aplikacji, z której użytkownik chce skorzystać i o której wie, że jest bezpieczna. Dzieje się tak, ponieważ aplikacja próbuje wprowadzić potencjalnie szkodliwe zmiany w systemie. Może się też zdarzyć, że aplikacja zostanie przypadkowo zablokowana przez użytkownika po wyświetleniu okna podręcznego funkcji DeepGuard.

Aby zezwolić na działanie aplikacji zablokowanej przez funkcję DeepGuard:

Otwórz panel główny i wybierz opcję Ochrona Internetu

- 1. Wybierz kartę **Narzędzia** i kliknij opcję **Uprawnienia aplikacji**. Pojawi się lista **Aplikacje monitorowane**.
- Znajdź aplikację, na działanie której chcesz zezwolić.
 Uwaga: klikając nagłówki kolumn, możesz sortować listę. Aby na przykład posortować listę według grup dozwolonych i zablokowanych programów, kliknij kolumnę Uprawnienie.
- 3. Kliknij prawym przyciskiem myszy pozycję Zezwalaj w kolumnie Uprawnienie.
- 4. Kliknij przycisk Zamknij.

Następnym razem funkcja DeepGuard umożliwi aplikacji wprowadzanie zmian w systemie.

Jak edytować ustawienia funkcji DeepGuard?

Funkcja DeepGuard monitoruje ważne ustawienia i pliki systemowe oraz próby wyłączenia ważnych aplikacji, takich jak ten produkt zabezpieczający. Analizuje działanie komputera i zatrzymuje ataki z wykorzystaniem luk w zabezpieczeniach popularnych programów mające na celu instalowanie złośliwego oprogramowania. Funkcja DeepGuard jest w stanie wykryć i zablokować operacje charakterystyczne dla prób wykorzystania luk w zabezpieczeniach, zapobiegając naruszaniu bezpieczeństwa i infekcjom. Dzięki temu komputer jest chroniony nawet wtedy, gdy są na nim zainstalowane programy zawierające luki w zabezpieczeniach.

Aby wybrać, co monitoruje funkcja DeepGuard

- 1. W panelu głównym wybierz opcję Ochrona Internetu
- 2. Wybierz pozycję Ustawienia. Zostanie otwarte okno Ustawienia.
- 3. W ustawieniach programu Ochrona Internetu wybierz opcję DeepGuard.
- 4. Upewnij się, że funkcja DeepGuard jest włączona:
- 5. Wybierz ustawienia funkcji DeepGuard:

Ustawienie	Opis
Ostrzegaj o podejrzanych działaniach	Pozostaw tę opcję włączoną, aby otrzymywać ostrzeżenia o podejrzanych działaniach aplikacji. Jeśli ją wyłączysz, funkcja DeepGuard przestanie monitorować podejrzane działania, co obniża poziom zabezpieczeń.
Ostrzegaj o lukach w zabezpieczeniach aplikacji	Pozostaw tę opcję włączoną, aby otrzymywać ostrzeżenia o potencjalnych próbach wykorzystania luk w zabezpieczeniach. Jeśli ją wyłączysz, szkodliwe strony internetowe i dokumenty będą mogły wykorzystywać luki w zabezpieczeniach aplikacji, co obniża poziom zabezpieczeń.
Pytaj o pozwolenie na nawiązanie połączenia internetowego	Pozostaw tę opcję włączoną, aby otrzymywać powiadomienia od funkcji DeepGuard, gdy nieznane aplikacje próbują nawiązać połączenie z Internetem.
Wybierz opcję Użyj trybu zgodności (zmniejsza poziom zabezpieczeń)	W celu zapewnienia maksymalnej ochrony funkcja DeepGuard tymczasowo modyfikuje uruchomione programy. Niektóre programy sprawdzają, czy nie zostały uszkodzone lub zmodyfikowane, i mogą nie być zgodne z tą funkcją. Na przykład gry internetowe zawierające narzędzia zapobiegające oszukiwaniu po uruchomieniu stale sprawdzają, czy nie zostały w jakikolwiek sposób zmodyfikowane. W takich przypadkach można włączyć tryb zgodności.

6. Wybierz przycisk **OK.**

Jak wyłączyć wszystkie funkcje zabezpieczeń?

Wyłączanie funkcji zabezpieczeń jest niezalecane, ponieważ pozostawia to komputer bez ochrony przed atakami, jednak czasami jest to konieczne. W takim przypadku należy wykonać poniższe czynności.

Wyłączanie wszystkich funkcji zabezpieczeń

- 1. W panelu głównym wybierz opcję Ochrona Internetu
- 2. Wybierz kartę Narzędzia.

- Wybierz pozycję Wyłącz wszystkie funkcje zabezpieczeń.
 Uwaga! Zostanie wyświetlone ostrzeżenie, że wyłączenie wszystkich funkcji zabezpieczeń pozostawia komputer bez ochrony przed atakami.
- 4. Potwierdź, wybierając opcję Wyłącz.

Sprawdzanie stanu funkcji zabezpieczeń — bez włączania produktu

- 1. W panelu głównym kliknij prawym przyciskiem myszy opcję **Ochrona Internetu** .
- 2. Jeśli zobaczysz polecenie Włącz, to znaczy, że funkcje zabezpieczeń są wyłączone.

Włączanie wszystkich funkcji zabezpieczeń

- 1. W panelu głównym wybierz opcję **Ochrona Internetu**
- 2. Wszystkie funkcje zabezpieczeń zostają włączone wraz z otwarciem programu Ochrona Internetu.

SKANOWANIE

Jak wykluczyć plik lub folder ze skanowania?

Niekiedy zachodzi potrzeba wykluczenia pliku lub folderu ze skanowania. Wykluczone elementy nie są skanowane, dopóki nie zostaną usunięte z listy wykluczonych elementów.

Uwaga: Funkcje skanowania ręcznego i skanowania w czasie rzeczywistym mają oddzielne listy wykluczeń. Jeśli na przykład plik zostanie wykluczony ze skanowania w czasie rzeczywistym, będzie nadal skanowany podczas skanowania ręcznego, chyba że zostanie wykluczony także ze skanowania ręcznego.

Aby wykluczyć plik lub folder ze skanowania:

- 1. Otwórz program Ochrona Internetu.
- 2. Na stronie głównej programu Ochrona Internetu kliknij opcję Ustawienia.
- 3. Wykonaj jedną z następujących czynności:
 - Wybierz kolejno opcje Ochrona Internetu > Skanowanie w poszukiwaniu wirusów.
 - Wybierz kolejno opcje Inne ustawienia > Skanowanie ręczne.
- 4. Kliknij łącze **Wyklucz pliki ze skanowania**. Zostanie wyświetlone okno dialogowe Wyklucz ze skanowania.
- 5. W zależności od tego, jakie elementy mają zostać wykluczone ze skanowania, wykonaj jedną z następujących czynności:
 - Aby wykluczyć plik, napęd lub folder:
 - 1. Wybierz kartę **Obiekty**.

- 2. Zaznacz pole wyboru **Wyklucz obiekty** (**pliki, foldery itd.**).
- 3. Kliknij przycisk **Dodaj**.
- 4. Wybierz plik, napęd lub folder, który ma zostać wykluczony ze skanowania w poszukiwaniu wirusów.

Uwaga: Niektóre napędy mogą być wymienne, na przykład napędy CD i DVD oraz napędy sieciowe. Nie można wykluczać napędów sieciowych ani pustych napędów wymiennych.

- 5. Kliknij przycisk OK, aby zamknąć okno dialogowe Wyklucz ze skanowania.
- Aby wykluczyć pliki określonego typu:

0

- 1. Wybierz kartę **Typy plików**.
- 2. Zaznacz pole wyboru Wyklucz pliki z tymi rozszerzeniami.
- 3. W polu obok przycisku **Dodaj** wpisz rozszerzenie określające typ plików, które chcesz wykluczyć.
- 4. Kliknij przycisk **Dodaj**.
- 5. Powtórz kroki 3 i 4 dla pozostałych rozszerzeń plików, które chcesz wykluczyć ze skanowania.
- 6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe Wyklucz ze skanowania.

Uwaga: niektóre pliki, takie jak pliki wykonywalne, są zawsze skanowane i nie można ich wykluczać.

Jak wykluczyć aplikację ze skanowania?

Aplikacji nie można wykluczać bezpośrednio. Nowe aplikacje pojawiają się na liście wykluczeń tylko w wyniku wykluczenia ich w trakcie skanowania.

Jeśli funkcja skanowania wykryje aplikację, która zachowuje się jak oprogramowanie szpiegujące lub ryzykowne, ale użytkownik wie, że jest ona bezpieczna, może wykluczyć ją ze skanowania, tak aby produkt nie wyświetlał więcej ostrzeżeń dotyczących tej aplikacji. Jeśli jednak aplikacja zachowuje się jak wirus lub inne złośliwe oprogramowanie, nie można jej wykluczyć.

Aplikacje wykluczone ze skanowania można wyświetlać i usuwać z listy elementów wykluczonych, gdyby w przyszłości miały być znowu uwzględniane podczas skanowania. Aby wyświetlić aplikacje wykluczone ze skanowania:

- 1. Otwórz program Ochrona Internetu.
- 2. Na stronie głównej programu Ochrona Internetu kliknij opcję Ustawienia.
- 3. Wykonaj jedną z następujących czynności:
 - Wybierz kolejno opcje Ochrona Internetu > Skanowanie w poszukiwaniu wirusów.
 - Wybierz kolejno opcje Inne ustawienia > Skanowanie ręczne.
- 4. Kliknij łącze **Wyklucz pliki ze skanowania**. Zostanie wyświetlone okno dialogowe Wyklucz ze skanowania.
- 5. Na karcie Aplikacje wyświetlane są aplikacje wykluczone ze skanowania.

Jak usunąć złośliwe oprogramowanie z folderu Kosz?

Produkt firmy F-Secure może wykrywać zainfekowane pliki wewnątrz folderów Kosz. Foldery Kosz są używane do przechowywania usuniętych plików. Zazwyczaj znajdują się w następujących miejscach:

- C:\RECYCLED
- C:\RECYCLER
- C:\\$RECYCLE.BIN\

Aby usunąć zainfekowane pliki z tych folderów, należy opróżnić Kosz.

Aby opróżnić Kosz, wykonaj następujące czynności:

- 1. Kliknij dwukrotnie ikonę Kosz na pulpicie.
- 2. Z menu Plik wybierz polecenie Opróżnij Kosz.
- 3. Kliknij przycisk OK.

Zostaną usunięte wszystkie pliki znajdujące się w folderach Kosz na wszystkich napędach. Są to pliki przeznaczone do usunięcia, zatem operacja nie powoduje utraty żadnych faktycznych danych.

Pełne skanowanie komputera przebiegło bardzo szybko. Czy produkt na pewno szczegółowo sprawdził cały komputer?

Przy użyciu pełnego skanowania komputera wszystkie dyski twarde są sprawdzane pod kątem obecności złośliwego oprogramowania, takiego jak wirusy, programy typu rootkit i oprogramowanie szpiegujące. Drugie pełne skanowanie komputera (i każde kolejne) przebiega znacznie szybciej, ponieważ sprawdzane są tylko zmienione pliki. W ten sposób zmienia się liczba skanowanych plików podczas kolejnych operacji skanowania.

Jeśli archiwum nie zostało zmienione w czasie między operacjami skanowania, to podczas kolejnego skanowania nie zostanie sprawdzone. Archiwum zawierające 100 plików powoduje zwiększenie liczby plików sprawdzanych podczas pierwszego skanowania o 101. Drugie skanowanie ręczne zwykle trwa kilka minut.

Pomijane są również pliki zawierające cyfrowe podpisy od zaufanych dostawców, których podpis nie został naruszony, na przykład pliki systemu Windows i programów Adobe Acrobat Reader, Microsoft Excel. Niezmodyfikowane pliki pochodzące od firmy F-Secure też nie są skanowane. Są tworzone przez oprogramowanie zabezpieczające, więc nie ma potrzeby, aby je sprawdzać.

Warto zaznaczyć, że skanowanie zaplanowane może wykryć więcej wirusów niż skanowanie ręczne, ponieważ skanowanie zaplanowane jest uruchamiane z uprawnieniami administratora, przez co może mieć dostęp do dodatkowych plików.

Czy ręczne skanowanie dysków twardych każdego dnia jest konieczne?

Zazwyczaj ręczne skanowanie dysków twardych nie jest potrzebne. Skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego obejmuje skanowanie w czasie rzeczywistym. Oznacza to, że komputer jest skanowany w poszukiwaniu wirusów w czasie rzeczywistym. Dodatkowo można wykonać ręczne skanowanie komputera w poszukiwaniu wirusów za pomocą skanowania zaplanowanego.

Uwaga: Skanowanie w poszukiwaniu złośliwego oprogramowania jest intensywnym procesem. Wymaga pełnej mocy komputera i zajmuje nieco czasu. Z tego powodu korzystne jest skonfigurowanie programu do przeprowadzania skanowania w czasie, gdy komputer nie jest używany.

Konfigurowanie skanowania zaplanowanego

Komputer może być skanowany przez program w regularnych odstępach czasu, na przykład codziennie, co tydzień lub co miesiąc. Aby ustawić harmonogram skanowania:

- 1. Otwórz program Ochrona Internetu.
- 2. Na stronie głównej programu Ochrona Internetu kliknij opcję Ustawienia.
- 3. Wybierz kolejno opcje Inne ustawienia > Skanowanie zaplanowane.
- 4. Wybierz opcję Włącz skanowanie zaplanowane.
- 5. Wybierz dni, w jakie regularnie ma odbywać się skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego:

Opcja	Opis		
Codziennie	Codzienne skanowanie.		
Co tydzień	Skanowanie jest wykonywane w wybrane dni tygodnia. Z listy po prawej stronie wybierz dni, w których ma być przeprowadzane skanowanie.		
Co miesiąc	 Skanowanie jest wykonywane w maksymalnie trzy dni miesiąca. Aby wybrać dni skanowania: 1. Wybierz jedną z opcji Dzień. 2. Z listy obok wybranego dnia wybierz odpowiedni dzień miesiąca. 3. Powtórz czynność, jeśli skanowanie ma być przeprowadzane jeszcze innego dnia. 		

Określ godzinę rozpoczęcia skanowania w wybrane dni:

Opcja	Opis
Godzina rozpoczęcia	Godzina rozpoczęcia skanowania. Wybierz porę, gdy komputer zwykle nie jest używany.

Jeżeli komputer nie jest	Wybierz okres bezczynności, po którym rozpoczyna się skanowanie,
używany przez	jeśli komputer nie jest używany.

7. Kliknij przycisk OK.

Jak wyczyścić zainfekowany folder System Volume Information lub folder funkcji Przywracanie systemu?

W przypadku zainfekowania komputera przez wirusa możliwe jest, że w folderze funkcji Przywracanie systemu została utworzona kopia tego wirusa. Przywracanie systemu to funkcja systemu operacyjnego Windows.

Aby przeskanować i wyczyścić folder funkcji Przywracanie systemu, konieczne jest wyłączenie tej funkcji. Wyłączenie funkcji Przywracanie systemu powoduje utratę ostatniego punktu przywracania systemu. Niestety nie istnieje inny sposób usuwania infekcji z folderu funkcji Przywracania systemu. Aby nadal korzystać z funkcji Przywracanie systemu, należy pamiętać o jej włączeniu po usunięciu zainfekowanych plików.

Aby wyłączyć funkcję Przywracanie systemu w systemie Windows 7:

- 1. Zamknij wszystkie otwarte programy.
- 2. Kliknij prawym przyciskiem myszy ikonę **Komputer** i wybierz polecenie **Właściwości**. Zostanie otwarte okno dialogowe Wyświetl podstawowe informacje o tym komputerze.
- 3. Kliknij pozycję **Ochrona systemu**. Zostanie wyświetlone okno dialogowe Właściwości systemu.
- 4. Kliknij kartę Ochrona systemu.
- 5. Kliknij przycisk Konfiguruj.
- 6. Wybierz opcję Wyłącz ochronę systemu.
- 7. Kliknij przycisk Zastosuj.
- 8. Jeśli pojawi się pytanie, czy chcesz wyłączyć ochronę systemu, kliknij przycisk Tak.
- 9. Kliknij przycisk OK.
- 10. Przeskanuj wszystkie dyski twarde i wszystkie pliki w poszukiwaniu wirusów przy użyciu produktu zabezpieczającego firmy F-Secure.

Po przeprowadzeniu skanowania i czyszczenia plików możesz włączyć funkcję Przywracanie systemu w systemie Windows 7, wykonując następujące czynności:

- 1. Kliknij prawym przyciskiem myszy ikonę **Komputer** i wybierz polecenie **Właściwości**. Zostanie otwarte okno dialogowe Wyświetl podstawowe informacje o tym komputerze.
- 2. Kliknij pozycję Ochrona systemu.
- 3. Kliknij kartę **Ochrona systemu**.
- 4. Kliknij przycisk **Konfiguruj**.
- 5. Wybierz opcję Przywróć ustawienia systemu oraz poprzednie wersje plików.

- 6. Kliknij przycisk **Zastosuj**.
- 7. Kliknij przycisk OK.

Aby wyłączyć funkcję Przywracanie systemu w systemie Windows XP:

- 1. Zamknij wszystkie otwarte programy.
- 2. Kliknij prawym przyciskiem myszy ikonę **Mój komputer** i wybierz polecenie **Właściwości**. Zostanie otwarte okno dialogowe **Właściwości systemu**.
- 3. Kliknij kartę Przywracanie systemu.
- 4. Zaznacz pole wyboru Wyłącz Przywracanie systemu na wszystkich dyskach.
- 5. Kliknij przycisk Zastosuj.
- 6. Jeśli pojawi się pytanie, czy chcesz wyłączyć funkcję Przywracanie systemu, kliknij przycisk **Tak**.
- 7. Kliknij przycisk OK.
- 8. Przeskanuj wszystkie dyski twarde i wszystkie pliki w poszukiwaniu wirusów przy użyciu produktu zabezpieczającego firmy F-Secure.

Po przeprowadzeniu skanowania i czyszczenia plików możesz włączyć funkcję Przywracanie systemu w systemie Windows XP, wykonując następujące czynności:

- 1. Kliknij prawym przyciskiem myszy ikonę Mój komputer i wybierz polecenie Właściwości. Zostanie otwarte okno dialogowe Właściwości systemu.
- 2. Kliknij kartę Przywracanie systemu.
- 3. Usuń zaznaczenie pola wyboru Wyłącz Przywracanie systemu na wszystkich dyskach.
- 4. Kliknij kolejno przyciski Zastosuj i OK.

Aby wyłączyć funkcję Przywracanie systemu w systemie Windows Vista:

- 1. Zamknij wszystkie otwarte programy.
- 2. Kliknij przycisk Start.
- 3. Wybierz kolejno opcje **Wszystkie programy > Konserwacja**.
- 4. Wybierz kolejno opcje Konserwacja > Centrum kopii zapasowych i przywracania.
- 5. Kliknij pozycję Utwórz punkt przywracania lub zmień ustawienia. W razie potrzeby kliknij przycisk Kontynuuj.
- 6. W obszarze Dostępne dyski usuń zaznaczenia pól wyboru dla wszystkich napędów.
- 7. Kliknij przycisk Zastosuj.
- 8. Jeśli pojawi się pytanie, czy chcesz wyłączyć funkcję Przywracanie systemu, kliknij przycisk **Wyłącz Przywracanie systemu**.
- 9. Kliknij przycisk OK.
- 10. Ponownie uruchom komputer.
- 11. Przeskanuj wszystkie dyski twarde i wszystkie pliki w poszukiwaniu wirusów przy użyciu produktu zabezpieczającego firmy F-Secure.

Po przeprowadzeniu skanowania i czyszczenia plików możesz włączyć funkcję Przywracanie systemu w systemie Windows Vista, wykonując następujące czynności:

- 1. Zamknij wszystkie otwarte programy.
- 2. Kliknij przycisk Start.
- 3. Wybierz kolejno opcje Wszystkie programy > Konserwacja.
- 4. Wybierz kolejno opcje Konserwacja > Centrum kopii zapasowych i przywracania.
- 5. Kliknij pozycję Utwórz punkt przywracania lub zmień ustawienia. W razie potrzeby kliknij przycisk Kontynuuj.
- 6. W obszarze Dostępne dyski zaznacz wszystkie napędy.
- 7. Kliknij przycisk Zastosuj.
- 8. Jeśli pojawi się pytanie, czy chcesz włączyć funkcję Przywracanie systemu, kliknij przycisk Włącz Przywracanie systemu.
- 9. Kliknij przycisk OK.

Usuwanie plików oprogramowania reklamowego

Co to jest oprogramowanie reklamowe (adware)?

Oprogramowanie reklamowe, wspierające reklamy lub adware to może być każda aplikacja wyświetlająca reklamy. Bardzo często oprogramowanie reklamowe można też sklasyfikować jako oprogramowanie szpiegujące. Zainstalowanie takiego oprogramowania na komputerze może doprowadzić do zapisania na dysku bardzo dużej liczby plików adware, zwłaszcza jeśli do korzystania z Internetu używany jest program Internet Explorer. Użytkownicy zwykle przypadkowo instalują oprogramowanie reklamowe ze stron internetowych lub razem z bezpłatnym oprogramowaniem, które jest pobierane w pakiecie z adware (na przykład niektóre aplikacje klienckie do bezpłatnej wymiany plików peer-to-peer, takie jak Kazaa i Grokster, są rozpowszechniane z oprogramowaniem szpiegującym w pakiecie).

Usuwanie plików oprogramowania reklamowego

Jeśli podczas przeglądania Internetu wyświetlane są niechciane okna podręczne lub podczas pracy na komputerze można zauważyć podejrzane aktywności, to istnieje możliwość, że na komputerze działa oprogramowanie reklamowe.

Produkt firmy F-Secure powinien automatycznie usunąć z komputera oprogramowanie reklamowe. Dla pewności zalecamy uruchomienie skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego:

- 1. W panelu głównym wybierz opcję **Ochrona Internetu**
- 2. Wybierz opcję Skanuj. Zostanie uruchomiony kreator skanowania.
- 3. Postępuj zgodnie z instrukcjami tego kreatora, aby przeprowadzić skanowanie.

W przypadku infekcji oprogramowaniem reklamowym, którego narzędzia firmy F-Secure nie wykrywają, można wysłać do nas próbkę przy użyciu <u>Systemu analizy próbek</u>.

Czyszczenie tymczasowych plików internetowych w programie Internet Explorer

W tym artykule opisano, co można zrobić w przypadku wykrycia złośliwego oprogramowania w folderze tymczasowych plików internetowych.

Złośliwe oprogramowanie w tymczasowych plikach internetowych

Folder tymczasowych plików internetowych w systemach Microsoft Windows zawiera pliki (takie jak obrazy, strony HTML, pliki wykonywalne i pliki skryptów), które zostały pobrane przez program Internet Explorer z witryn internetowych odwiedzonych przez użytkownika. Czasami produkt firmy F-Secure może wykryć wewnątrz tego folderu wirusy i oprogramowanie reklamowe.

W systemie Windows XP lokalizacja tego folderu jest następująca:

• C:\Documents and Settings\Ustawienia lokalne\Temporary Internet Files\Content.IE5 Uwaga: W przypadku posiadania tylko jednego konta użytkownika w systemie Windows XP należy zastosować nazwę użytkownika Administrator.

W systemach Windows Vista i Windows 7 lokalizacja tego folderu jest następująca:

- C:\Uzytkownicy\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- C:\Uzytkownicy\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5

Uwaga: Te pliki to ukryte pliki systemowe. Aby móc uzyskać do nich dostęp, należy wprowadzić zmiany w opcjach folderu.

Usuwanie plików z folderu tymczasowych plików internetowych

Jeśli folder tymczasowych plików internetowych zawiera złośliwe oprogramowanie, zalecamy usunięcie wszystkich plików z tego folderu. Te pliki są tylko zbuforowanymi kopiami, dlatego żadne rzeczywiste dane nie zostaną utracone.

Usuwanie plików tymczasowych w systemie Windows XP:

- 1. Wykonaj jedną z następujących czynności:
 - Kliknij kolejno pozycje **Start > Panel sterowania > Opcje internetowe**.
 - Otwórz program Internet Explorer i wybierz kolejno pozycje Narzędzia > Opcje internetowe.

Zostanie otwarte okno dialogowe Właściwości internetowe.

2. W obszarze tymczasowych plików internetowych kliknij przycisk Usuń pliki. Zostanie otwarte okno dialogowe Usuwanie plików:

Internet Properties
General Security Privacy Content Connections Programs Advanced
Home page You can change which page to use for your home page. Address: https://kb-admin.f-secure.com/index.aspx?
Use Current Use Default Use Blank
Temporary Internet files Pages you view on the Internet are stored in a special folder for quick viewing later.
Delete Cookies Delete Files Settings
Delete Files
Delete all files in the Temporary Internet Files ed, for
You can also delete all your offline content stored locally.
Delete all offline content
OK Cancel essibility
OK Cancel Apply

3. Najpierw zaznacz pole wyboru Usuń całą zawartość offline, a następnie kliknij przycisk OK, aby usunąć tymczasowe pliki internetowe.

Usuwanie plików tymczasowych w systemach Windows Vista i Windows 7:

- 1. Wykonaj jedną z następujących czynności:
 - Kliknij kolejno pozycje Start > Panel sterowania > Opcje internetowe i na karcie
 Ogólne w obszarze Historia przeglądania kliknij przycisk Usuń.
 - Otwórz program Internet Explorer i kliknij kolejno pozycje Narzędzia > Opcje internetowe, a następnie na karcie Ogólne w obszarze Historia przeglądania kliknij przycisk Usuń.
 - Otwórz program Internet Explorer i kliknij kolejno pozycje Bezpieczeństwo > Usuń historię przeglądania.

Zostanie otwarte okno dialogowe Usuwanie historii przeglądania:

har Delete Browsing History
Preserve Favorites website data Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.
Temporary Internet files Copies of webpages, images, and media that are saved for faster viewing.
Cookies Files stored on your computer by websites to save preferences such as login information.
List of websites you have visited.
Form data Saved information that you have typed into forms.
Passwords Saved passwords that are automatically filled in when you sign in to a website you've previously visited.
InPrivate Filtering data Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.
About deleting browsing history Delete Cancel

2. Zaznacz pole wyboru **Tymczasowe pliki internetowe** i kliknij przycisk **Usuń**, aby usunąć tymczasowe pliki internetowe.

Jak przesyłać próbki do firmy F-Secure?

Dzięki systemowi analizy próbek (<u>Sample Analysis System, SAS</u>) użytkownicy mogą przesyłać podejrzane pliki znalezione w Internecie. Pliki zostaną natychmiast przeskanowane i w razie potrzeby nastąpi odpowiednia aktualizacja baz danych.

Uwaga: próbki można przesyłać anonimowo bez używania konta. Założenie konta jest niezbędne tylko w następujących przypadkach:

- Uzyskiwanie informacji zwrotnych dotyczących próbek
- Przesyłanie dużych partii próbek
- Przesyłanie adresów URL

Zadania związane z przesyłaniem próbek

Wskazane poniżej artykuły ułatwiają wykonywanie zadań koniecznych podczas wysyłania próbek do firmy F-Secure:

- <u>Tworzenie archiwum ZIP i zabezpieczanie go hasłem</u>
- Zapisywanie raportu skanowania w pliku
- Zapisywanie w pliku wiadomości phishingowych, zawierających spam lub niepoprawnie uznanych za niebezpieczne
- Jak sprawdzić, czy mam na komputerze najnowsze aktualizacje?

Zapisywanie raportu skanowania w pliku

Czasami trzeba wysłać raport skanowania do analizy w firmie F-Secure. Aby zapisać raport skanowania w pliku, należy postępować zgodnie z poniższymi instrukcjami.

Zapisywanie raportu skanowania w pliku

Aby zapisać raport skanowania w pliku, wykonaj te czynności:

- 1. Uruchom skanowanie w używanym produkcie antywirusowym firmy F-Secure. Po ukończeniu skanowania zostanie wyświetlona strona.
- 2. Kliknij przycisk **Pokaż raport**, aby wyświetlić szczegółowy raport:
- 3. Aby zapisać raport w pliku, wybierz opcje **Plik** > **Zapisz jako**, przejdź do folderu, w którym chcesz ten raport zapisać, wpisz dla niego nazwę i zapisz go.
- 4. Następnie możesz wysłać ten plik do analizy w firmie F-Secure.

Zapisywanie w pliku wiadomości phishingowych, zawierających spam lub niepoprawnie uznanych za niebezpieczne

Firma F-Secure przyjmuje próbki otrzymanych przez użytkowników wiadomości phishingowych, zawierających spam lub niepoprawnie uznanych za niebezpieczne.

Uwaga: Próbki wiadomości phishingowych, zawierających spam lub niepoprawnie uznanych za niebezpieczne należy przesyłać na określony adres e-mail. Szczegółowe instrukcje można znaleźć na stronie <u>http://www.f-secure.com/pl/web/labs_global/submit-samples/spam-submission</u>.

Zapisywanie próbki wiadomości w pliku

Aby zapisać wiadomość phishingową, zawierającą spam lub niepoprawnie uznaną za niebezpieczną, wykonaj następujące czynności:

- 1. Otwórz otrzymaną wiadomość phishingową, zawierającą spam lub niepoprawnie uznaną za niebezpieczną w programie poczty e-mail.
 - 2. Wybierz kolejno pozycje **Plik** > **Zapisz jako**. Jeśli korzystasz z programu poczty e-mail Microsoft Outlook, zostanie wyświetlone następujące okno dialogowe Zapisywanie jako:



- 3. Znajdź odpowiedni folder dla pliku, nadaj mu opisową nazwę (domyślną nazwą pliku jest temat zapisywanej wiadomości) i zapisz go.
- 4. Wyślij plik do firmy F-Secure.

AKTUALIZACJE

Produkt wskazuje, że definicje wirusów są nieaktualne. Co mogę zrobić?

Przyjmuje się, że aktualizacje stają się przestarzałe po siedmiu dniach. Należy pamiętać o regularnej aktualizacji bazy danych definicji wirusów, ponieważ zagrożenia mogą się zmieniać bardzo szybko. Firma F-Secure udostępnia aktualizacje nawet kilka razy dziennie.

Jeśli komputer został włączony pierwszy raz po kilku dniach nieużywania, na przykład po wakacjach, cały pakiet aktualizacji zostanie automatycznie pobrany i zainstalowany w ciągu 30 minut.

Jeśli produkt firmy F-Secure nadal wskazuje, że definicje wirusów są nieaktualne, spróbuj wykonać następujące czynności:

- 1. Otwórz panel główny Ochrony Internetu, kliknij prawym przyciskiem myszy ikonę Ochrona Internetu, a następnie wybierz polecenie **Sprawdź dostępność aktualizacji**.
- Otwórz panel główny Ochrony Internetu, kliknij prawym przyciskiem myszy ikonę Ochrona Internetu, a następnie wybierz polecenie Wyświetl moje subskrypcje. W oknie Moje subskrypcje możesz sprawdzić stan swojej subskrypcji.
- 3. Upewnij się, że ustawienia daty i godziny systemu Windows są poprawne, ponieważ nieprawidłowe ustawienia mogą powodować błędne zgłaszanie nieaktualnych definicji wirusów. Data i godzina są widoczne na pasku zadań systemu Windows. Ustawienia zegara można

zmienić w aplecie Właściwości daty i godziny. Aby otworzyć właściwości, kliknij dwukrotnie zegar.

- 4. Pobierz i uruchom plik <u>fsaua-reset.exe</u>. Po wyświetleniu okna wiersza polecenia naciśnij klawisz Y. Program samoczynnie zakończy działanie.
- 5. Pobierz i uruchom plik <u>fsdbupdate9.exe</u> zawierający nową kopię definicji wirusów.

Jeśli powyższe czynności okażą się nieskuteczne, zalecamy odinstalowanie i ponowne zainstalowanie produktu.

Jak sprawdzić, czy najnowsze aktualizacje są zainstalowane?

Aktualizacje automatyczne są włączane od razu po zainstalowaniu oprogramowania firmy F-Secure. Jeśli komputer jest połączony z Internetem, produkt firmy F-Secure co dwie godziny sprawdza dostępność nowych aktualizacji i w razie potrzeby pobiera je.

Cały pakiet aktualizacji jest dość duży, a czas pobierania zależy od szybkości połączenia internetowego. Jeśli komputer był wyłączony przez co najmniej siedem dni, to zostanie pobrany i zainstalowany cały pakiet aktualizacji, co może potrwać dłużej niż w przypadku zwykłych aktualizacji przeprowadzanych codzienne.

Uwaga: w celu maksymalnego skrócenia czasu potrzebnego na pobieranie zalecamy, aby komputer łączył się z Internetem co najmniej raz w tygodniu.

Sprawdzanie dostępności aktualizacji

Aby sprawdzić dostępność aktualizacji baz danych:

- 1. W panelu głównym kliknij opcję Ochrona Internetu 🧖
- 2. Na głównej stronie programu Ochrona Internetu kliknij przycisk Ustawienia.
- 3. Wybierz opcje **Inne ustawienia** > **Wersje baz danych**, aby wyświetlić stronę Wersje baz danych.

Na stronie będą widoczne data i wersja pakietu aktualizacji bazy danych o najwyższym numerze. Należy pamiętać, że pakiet aktualizacji o najwyższym numerze nie musi być najnowszą pobraną aktualizacją.

Aby wyświetlić najnowsze zainstalowane aktualizacje poszczególnych aparatów skanowania dostępnych w produkcie, wykonaj następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatnią ikonę po prawej



Zostanie wyświetlone menu podręczne.

- 2. Wybierz polecenie Otwórz typowe ustawienia.
- 3. Wybierz opcje Aktualizacje automatyczne > Pobrane pliki.

W tabeli Pobrane pliki możesz sprawdzić wersje ostatniej aktualizacji poszczególnych aparatów.

Uwaga: jeżeli dostęp do Internetu jest uzyskiwany za pomocą modemu lub łącza ISDN, to aby możliwe było sprawdzenie aktualizacji, połączenie musi być aktywne.

Ręczne sprawdzanie dostępnych aktualizacji

Produkt automatycznie pobiera najnowsze aktualizacje natychmiast po uzyskaniu połączenia z Internetem. Aby jednak upewnić się, że na komputerze są najnowsze aktualizacje, możesz wykonać następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatnią ikonę po prawej.



Zostanie wyświetlone menu podręczne.

2. Wybierz polecenie **Sprawdź dostępność aktualizacji**. Zostanie wyświetlone okno **Sprawdzanie dostępności aktualizacji**.

Produkt sprawdzi dostępność nowych aktualizacji i natychmiast je zainstaluje.

Jak mogę sprawdzić, czy mój komputer jest chroniony i aktualizacje automatyczne są włączone?

- 1. W panelu głównym otwórz program Ochrona Internetu
- 2. Na karcie **Stan** pokazywane jest podsumowanie funkcji zabezpieczeń wraz z ich aktualnym stanem.

Ikona stanu	Nazwa stanu	Opis
	ОК	Komputer jest chroniony. Funkcja jest włączona i działa poprawnie.

	Informacja	Produkt informuje o specjalnym stanie funkcji. Ta ikona jest wyświetlana między innymi podczas aktualizowania funkcji.
	Ostrzeżenie	Komputer nie jest w pełni chroniony. Na przykład produkt długo nie był aktualizowany lub stan funkcji wymaga uwagi użytkownika.
8	Błąd	Komputer nie jest chroniony. Na przykład wygasła ważność subskrypcji lub została wyłączona krytyczna funkcja.

Używam produktu Ochrona Internetu i chcę uaktualnić system Windows 7 do wersji Windows 8. Czy oprogramowanie zabezpieczające będzie działać po uaktualnieniu?

Tak. Oprogramowanie Ochrona Internetu jest obsługiwane przez systemy Windows 7 i 8, zatem przeprowadzenie uaktualnienia do wersji Windows 8 nie wpływa na działanie produktu Ochrona Internetu.

OCHRONA RODZICIELSKA

Co to jest Ochrona Rodzicielska?

Program Ochrona Rodzicielska ułatwia zapewnianie bezpieczeństwa podczas przeglądania Internetu dla całej rodziny, oferując ochronę przed złośliwym oprogramowaniem i szkodliwymi witrynami, a także umożliwiając ograniczanie typów zawartości dostępnych dla dzieci. Pozwala także kontrolować dozwolony czas dostępu do Internetu.

Dodatkowo program Ochrona Rodzicielska zawiera udoskonaloną funkcję **Ochrona bankowości**, która, niczym osobisty ochroniarz, zapewnia bezpieczeństwo i prywatność transakcji bankowych. Działanie tej funkcji polega na podnoszeniu poziomu zabezpieczeń podczas sesji bankowości online w celu dodatkowej ochrony.

Z myślą o zwiększeniu poziomu bezpieczeństwa w wielu witrynach, na przykład w usługach Google, wdrożono **szyfrowanie ruchu sieciowego przy użyciu protokołu HTTPS**. Jest to skuteczna metoda uniemożliwiająca "podsłuchiwanie" informacji przesyłanych między Internetem i urządzeniem użytkownika w publicznych sieciach Wi-Fi (takich jak kawiarnie i lotniska). Program **Ochrona Rodzicielska** pozwala zabezpieczyć takie szyfrowane dane w taki sam sposób, w jaki chroniony jest ruch nieszyfrowany. Na przykład podczas korzystania z wyszukiwarki Google mogą być wyświetlane informacje o klasyfikacji bezpieczeństwa każdego wyniku wyszukiwania. Aby włączyć tę funkcję, po instalacji programu należy aktywować rozszerzenie Ochrona Rodzicielska dla przeglądarki. Ochrona protokołu HTTPS wymaga włączenia rozszerzenia lub wtyczki do swojej przeglądarki. Ta funkcja obecnie obsługuje przeglądarki IE 7–10, Firefox i Chrome.

Po aktywowaniu funkcji **Ochrona Rodzicielska** można zablokować wyświetlanie materiałów dla dorosłych w wynikach wyszukiwania.

Korzystanie z kont użytkowników systemu Windows

Produkt korzysta z kont użytkowników systemu Windows w celu kontrolowania ustawień dla poszczególnych członków rodziny. Tylko osoba z uprawnieniami administratora może zmieniać ustawienia produktu dla różnych kont użytkowników systemu Windows.

Zalecamy skonfigurowanie oddzielnego konta użytkownika systemu Windows dla każdego członka rodziny. Na przykład rodzice mogą mieć uprawnienia administracyjne, natomiast dzieci mogą korzystać z normalnych uprawnień na swoich kontach użytkowników systemu Windows.

Więcej informacji o korzystaniu z programu Ochrona Rodzicielska:

1. W panelu głównym Ochrona Internetu kliknij prawym przyciskiem myszy ikonę Ochrona

Rodzicielska . Zostanie wyświetlone menu podręczne.

2. Wybierz polecenie **Pomoc**.

Jak tworzyć nowe konta użytkowników?

Zalecamy skonfigurowanie oddzielnych kont użytkowników systemu Windows dla każdego członka rodziny. Gdy każdy użytkownik komputera ma swoje własne konto systemu Windows, możesz ustawić różne uprawnienia dla poszczególnych osób.

Aby utworzyć nowe konta użytkowników

- 1. W panelu głównym otwórz program **Ochrona Rodzicielska** . Zostanie otwarta lista kont użytkowników.
- 2. Aby utworzyć nowe konto, wybierz pozycję Utwórz nowe.



Spowoduje to otwarcie ustawień kont użytkowników w systemie Windows.

3. Podaj wymagane informacje, aby utworzyć lub edytować konto użytkownika.

Więcej informacji o kontach użytkowników można znaleźć w bazie wiedzy firmy Microsoft (<u>Windows 8, Windows 7, Windows Vista, Windows XP</u>).

Dlaczego na komputerze należy korzystać z różnych kont użytkowników?

Zalecamy skonfigurowanie oddzielnego konta systemu Windows dla każdego członka rodziny. Gdy każdy użytkownik komputera ma swoje własne konto systemu Windows, możesz ustawić różne uprawnienia dla poszczególnych osób. W ten sposób możesz na przykład ustawić porę dnia, kiedy dzieci mogą korzystać z Internetu oraz ograniczyć czas przeglądania i dostęp do nieodpowiednich treści.

Tylko osoba z administracyjnymi prawami dostępu może zmieniać ustawienia produktu dla poszczególnych kont użytkowników systemu Windows. Na przykład rodzice mogą mieć uprawnienia administracyjne, a dzieci mogą korzystać z normalnych praw dostępu na swoich kontach systemu Windows.

Jak ograniczyć czas, jaki dziecko spędza na przeglądaniu Internetu?

Jeśli chcesz kontrolować czas spędzany przez poszczególnych użytkowników komputera w Internecie albo uniemożliwić im przeglądanie na przykład po godzinie dziewiątej wieczorem, to wykonaj czynności opisane poniżej.

Ustawianie limitów czasu przeglądania

- 1. W panelu głównym otwórz program **Ochrona Rodzicielska** . Pojawi się lista kont użytkowników. Gdy każdy użytkownik komputera ma swoje własne konto systemu Windows, możesz ustawić różne uprawnienia dla poszczególnych osób.
- 2. Wybierz konto użytkownika, dla którego chcesz ograniczyć czas przeglądania.
- 3. Wybierz pozycję Ustawienia.
- 4. Wybierz opcję Ograniczenia czasu przeglądania.
- 5. Przesuń suwak w prawo, aby aktywować tę funkcję 💷.
- 6. Oznacz pory dnia, gdy przeglądanie ma być dozwolone.
- 7. Możesz też ograniczyć liczbę godzin, przez które dany użytkownik może korzystać z Internetu, określając różne ustawienia dla dni tygodnia i weekendów.
- 8. Wybierz przycisk OK. To wszystko gotowe!

Jak blokować strony internetowe na podstawie ich zawartości?

Jeśli chcesz ochronić swoją rodzinę przed witrynami z nieodpowiednią treścią, możesz włączyć funkcję Blokowanie zawartości. Poniżej znajdziesz odpowiednie instrukcje.

Blokowanie stron internetowych na podstawie ich zawartości

- 1. W panelu głównym otwórz program **Ochrona Rodzicielska** . Pojawi się lista kont użytkowników. Gdy każdy użytkownik komputera ma swoje własne konto systemu Windows, możesz ustawić różne uprawnienia dla poszczególnych osób.
- 2. Wybierz konto użytkownika, dla którego chcesz ograniczyć czas przeglądania.
- 3. Wybierz pozycję Ustawienia.
- 4. Wybierz opcję Blokowanie zawartości.
- 5. Przesuń suwak w prawo, aby aktywować tę funkcję 💷.

- 6. Zaznacz pola obok kategorii zawartości, które chcesz zablokować.
- 7. Wybierz przycisk **OK**. Gdy dany użytkownik spróbuje otworzyć witrynę internetową o nieodpowiedniej zawartości, w przeglądarce zostanie wyświetlony ekran blokady. Tylko użytkownicy z uprawnieniami administracyjnymi mogą ominąć ten ekran.

Zezwalanie na dostęp tylko do określonych stron internetowych

Aby jeszcze bardziej ograniczyć dostępność zawartości internetowej, możesz utworzyć "białą listę" dozwolonych witryn i zablokować wszystkie pozostałe.

- 1. W programie Ochrona Rodzicielska wybierz konto użytkownika, które chcesz edytować.
- 2. Wybierz pozycję Ustawienia.
- 3. Wybierz opcję Blokowanie zawartości.
- 4. Przesuń suwak w prawo, aby aktywować tę funkcję 💷 (jeśli nie jest już włączona).
- 5. Wybierz opcję Zezwalaj tylko na wybrane witryny i dodaj adresy, które mają być dostępne.
- 6. Wybierz przycisk **OK**. Użytkownik będzie mógł otwierać tylko zdefiniowane przez Ciebie strony internetowe.

Jak aktywować ochronę przeglądania?

Gdy ochrona przeglądania jest aktywna, nie można otwierać szkodliwych witryn internetowych.

Aby aktywować ochronę przeglądania

- 1. W panelu głównym otwórz program **Ochrona Rodzicielska** . Zostanie otwarta lista kont użytkowników.
- 2. Wybierz konto użytkownika, dla którego chcesz aktywować ochronę przeglądania.
- 3. Wybierz opcje Ustawienia > Ochrona przeglądania.
- 4. Przesuń suwak w prawo, aby aktywować tę funkcję 💷.
- 5. Jeśli masz otwartą przeglądarkę, zamknij ją i uruchom ponownie, aby zastosować zmienione ustawienia.

Jak wyłączyć wyświetlanie klasyfikacji bezpieczeństwa dla witryn internetowych?

Klasyfikację bezpieczeństwa w przeglądarce można wyłączyć, korzystając z następujących sposobów:

- 1. Otwórz panel główny i wybierz opcję Ochrona Rodzicielska
- Wybierz konto użytkownika, które chcesz edytować. Uwaga: do zmiany ustawień innych kont użytkowników wymagane są uprawnienia administratora.
- 3. Wybierz pozycję Ustawienia.
- 4. W ustawieniach funkcji Ochrona przeglądania usuń zaznaczenie pola Pokazuj klasyfikację reputacji witryn w wynikach wyszukiwania (Google, Yahoo i Bing).
- 5. Wybierz przycisk OK.

OCHRONA BANKOWOŚCI

Co to jest Ochrona bankowości?

Ochrona bankowości to nowa, dodatkowa warstwa ochrony dostępna w oprogramowaniu zabezpieczającym firmy F-Secure. Po otwarciu w przeglądarce witryny banku internetowego funkcja ta jest automatyczne aktywowana w celu podniesienia poziomu zabezpieczeń sesji internetowej. Po aktywacji u góry ekranu wyświetlana jest informacja o włączonym trybie Ochrony bankowości. Gdy ten tryb jest aktywny, blokowane są wszystkie nowe połączenia z komputera. Dzięki temu konie trojańskie i inne złośliwe programy nie mogą wysyłać do przestępców prywatnych informacji użytkownika, takich jak dane logowania.

Po rozpoczęciu korzystania z witryny banku internetowego Ochrona bankowości zawiesza wszystkie połączenia sieciowe, aby zapewnić bezpieczeństwo użytkownika, a następnie przywraca je po zakończeniu sesji. Jednocześnie funkcja zapewnia dostęp do niezbędnych witryn, których bezpieczeństwo zostało zweryfikowane przez firmę F-Secure.

Niektóre banki już oferują klientom rozwiązania zabezpieczające. Jakie korzyści zapewnia operatorowi taka usługa?

Część banków faktycznie podejmuje działania w celu ochrony komputerów swoich klientów przed końmi trojańskimi. Oczywiście fakt, że banki starają się dbać o bezpieczeństwo użytkowników, jest pozytywnym zjawiskiem. Zazwyczaj jednak oferowane rozwiązania współdziałają tylko z witryną konkretnego banku i obsługują wyłącznie wybrane przeglądarki (za pośrednictwem dodatków plug-in).

Oferowana przez firmę F-Secure funkcja Ochrona bankowości jest zgodna z witrynami wszystkich ważnych banków i działa niezależnie od używanej przeglądarki. Ponadto funkcja ta jest częścią rozbudowanego pakietu zabezpieczeń internetowych, zatem klienci nie muszą instalować dodatkowego oprogramowania, aby korzystać z Ochrony bankowości.

W jaki sposób Ochrona bankowości poprawia moje bezpieczeństwo w Internecie?

Ochrona bankowości współdziała z innymi warstwami zabezpieczeń w produkcie Ochrona Internetu, aby zapewnić użytkownikom pełne bezpieczeństwo online. Pakiet Ochrona Internetu obejmuje funkcję ochrony przed wirusami, programami szpiegującymi i złośliwym oprogramowaniem, funkcję ochrony przed spamem blokującą przypadki phishingu oraz ochronę przeglądarki, która wykrywa szkodliwe witryny. Ochrona bankowości to dodatkowa warstwa zabezpieczająca przed nowymi, nieznanymi końmi trojańskimi atakującymi otwarte sesje bankowe.

Jakie przeglądarki internetowe obsługuje Ochrona bankowości?

Ochrona bankowości obsługuje następujące przeglądarki internetowe:

- Internet Explorer 9 i nowsze wersje
- Mozilla Firefox 13 i nowsze wersje
- Google Chrome

Czy Ochrona bankowości działa na komputerze Mac?

Nie. Obecnie Ochrona bankowości jest dostępna na komputerach z systemem Windows oraz urządzeniach z systemem Android, Windows Phone 8 oraz iOS,

Czy Ochrona bankowości działa na telefonach komórkowych lub tabletach?

TAK. Ochrona bankowości jest dostępna na urządzeniach z systemem Android, Windows Phone 8 oraz iOS.

Jak włączyć Ochronę bankowości?

Po włączeniu funkcji Ochrona bankowości chronione są wszystkie sesje i transakcje bankowe.

Aby włączyć funkcję Ochrona bankowości:

- 1. W panelu głównym kliknij pozycję Ochrona Rodzicielska
- 2. Wybierz konto użytkownika, które chcesz edytować. Uwaga: do zmiany ustawień innych kont użytkowników wymagane są uprawnienia administratora.
- 3. Wybierz pozycję Ustawienia.
- 4. Otwórz Ochrona Rodzicielska > Ochrona bankowości.
- 5. Kliknij przełącznik obok opcji **Ochrona bankowości**, aby ja włączyć:
- 6. Wybierz przycisk **OK**.

Ochrona bankowości jest teraz włączona.

Dlaczego przeglądarka działa nieprawidłowo po użyciu Ochrony bankowości?

Najbardziej prawdopodobną przyczyną jest pozostawienie włączonej Ochrony bankowości. Aby otworzyć okno powiadomień Ochrony bankowości, kliknij ikonę oprogramowania zabezpieczającego na pasku zadań systemu operacyjnego, a następnie kliknij polecenie Zakończ w powiadomieniu funkcji Ochrona bankowości. Możesz również zamknąć przeglądarkę i uruchomić nowa sesję. Teraz będzie można bez przeszkód korzystać z Internetu.



Jak zezwolić na korzystanie z innych witryn podczas sesji bankowości online?

Aby umożliwić korzystanie z innych witryn podczas sesji bankowości internetowej, wykonaj następujące czynności:

- 1. Otwórz program Ochrona Rodzicielska
- Wybierz konto użytkownika, które chcesz edytować.
 Uwaga: do zmiany ustawień innych kont użytkowników wymagane są uprawnienia administratora.
- 3. Wybierz Ustawienia.
- 4. Na stronie Ochrona przeglądania wybierz łącze Wyświetl listę dozwolonych i zabronionych witryn internetowych. Zostanie otwarte okno Ograniczenia witryn internetowych.
- 5. Na karcie Dozwolone kliknij przycisk Dodaj. Zostanie otwarte okno Dodaj witrynę.
- 6. Wpisz adres odpowiedniej witryny i kliknij przycisk **OK**.

Jak dodać witrynę banku do listy chronionych witryn banków internetowych?

Jeśli po włączeniu funkcji Ochrona bankowości i rozpoczęciu sesji bankowej u góry ekranu nie jest wyświetlane odpowiednie powiadomienie, dany bank może nie być uwzględniony na liście chronionych witryn banków. Aby konkretna witryna banku została dodana do listy, wyślij na adres bankingprotection@f-secure.com wiadomość e-mail zawierającą następujące informacje:

- nazwa banku lub instytucji finansowej
- adres URL banku

Twój bank zostanie dodany do listy chronionych witryn banków.

TRYB GIER

Co to jest tryb gier?

Włączając tryb gier, możesz zoptymalizować wykorzystanie zasobów systemowych komputera przez produkt. Gry komputerowe często potrzebują dużo zasobów systemowych do płynnego działania.

Tryb gier uwalnia więcej zasobów systemowych na potrzeby gier uruchomionych na komputerze, zmniejszając użycie procesora i sieci przez produkt przy zachowaniu działania najważniejszych funkcji produktu. Na przykład wykonywanie aktualizacji automatycznych i innych operacji zwiększających użycie procesora i sieci jest zawieszone przy włączonym trybie gier.

Ponadto żadne powiadomienia ani okienka centrum akcji nie są wyświetlane przy włączonym trybie gier. Są wyświetlane krytyczne powiadomienia wymagające natychmiastowego działania, ale inne powiadomienia są wyświetlane dopiero po wyjściu z trybu gier. Dotyczy to także innych aplikacji

pełnoekranowych, na przykład prezentacji, pokazów slajdów lub filmów wyświetlanych na pełnym ekranie, nawet przy wyłączonym trybie gier.

Jak włączyć tryb gier dla sytemu Windows?

Aktywując tryb gier, można zoptymalizować działanie komputera pod kątem gier.

Aktywowanie trybu gier:

W panelu głównym wybierz opcje > Tryb gier.



2. Użycie zasobów systemowych przez produkt jest teraz zoptymalizowane, aby gry działały płynnie na komputerze. Gdy tryb gier jest włączony, w menu obok polecenia **Tryb gier** jest widoczny znacznik wyboru .

Wyłączanie trybu gier:

- Ponowne uruchomienie komputera lub wybudzenie go z trybu uśpienia powoduje wyłączenie trybu gier.
- Można też wyłączyć ten tryb w panelu głównym > Tryb gier.