Obowiązuje od dnia 23.03.2023

Usługa „Bezpiecznie w Internecie"
– pytania i odpowiedzi

1. Na jakich platformach działa ochrona?

Windows (v19.0)	Mac (v19.0)	Android (v20.0)	iOS (v20.0)
Obsługiwane systemy operacyjne: ▪ Windows 11. ▪ Windows 10, aktualizacja rocznicowa lub nowszy. ▪ Windows 8.1. ▪ Windows 7, dodatek Service Pack 1.	**Obsługiwane systemy operacyjne:** ▪ macOS w wersji 13 „Ventura macOS w wersji 12 „Monterey" ▪ macOS w wersji 11 „Big Sur"	**Obsługiwane systemy operacyjne:** ▪ Android OS 8.0 i nowszy	**Obsługiwane systemy operacyjne:** ▪ iOS 15 – 16
Zalecane wymagania systemowe: ▪ Procesor: 1 gigaherc (GHz) lub szybszy* ▪ Pamięć: 1 gigabajt (GB) ▪ RAM (32-bitowy) lub 2 GB RAM (64-bitowy) ▪ Miejsce na dysku twardym: 600 MB dostępnego miejsca na dysku twardym ▪ Połączenie internetowe jest wymagane do weryfikacji subskrypcji i otrzymywania aktualizacji. *) Procesor ARM nie jest obsługiwany	**Zalecane wymagania systemowe:** ▪ Procesor Intel/Apple Silicon ▪ 250 MB wolnego miejsca na dysku ▪ Zalecane jest 1 GB lub więcej pamięci ▪ Połączenie internetowe jest wymagane do weryfikacji subskrypcji i otrzymywania aktualizacji.	**Zalecane wymagania systemowe:** ▪ Instalacja aplikacji wymaga około 75 MB wolnego miejsca. ▪ Aplikację można zainstalować tylko w pamięci wewnętrznej urządzenia, a nie w pamięci zewnętrznej, takiej jak karta SD. ▪ Połączenie internetowe jest wymagane do weryfikacji subskrypcji i otrzymywania aktualizacji.	**Zalecane wymagania systemowe:** ▪ Instalacja aplikacji klienckiej wymaga około 20-30 MB wolnego miejsca na dysku. ▪ Połączenie internetowe jest wymagane do weryfikacji subskrypcji i otrzymywania aktualizacji.
Obsługiwane przeglądarki przez produkt Fsecure dla systemu Windows w najnowszych wersjach producenta: ▪ Google Chrome ▪ Microsoft Edge (na bazie chromu) ▪ Mozilla Firefox		**Obsługiwane przeglądarki przez produkt Fsecure dla systemu Mac w najnowszych wersjach producenta:** ▪ Apple Safari ▪ Google Chrome ▪ Mozilla Firefox	

2. Jak zainstalować/pobrać Bezpiecznie w Internecie?

Są dwa sposoby zainstalowania Bezpiecznie w Internecie. Można skorzystać z e-maila lub smsa, który został wysłany w dniu zamówienia usługi. Można wyszukać e-maila lub sms korzystając z opcji wyszukaj w skrzynce e-mail lub z wiadomościami poprzez hasło „Bezpiecznie w Internecie". W wiadomości jest link, po którego kliknięciu nastąpi natychmiastowa instalacja rozwiązania. Login to adres e-mail, który Klient podał do banku jako kontaktowy. Hasło jest podane w wiadomości. Następnie hasło (to podane w wiadomości) może zostać zmienione na hasło wykreowane przez Klienta.

Z hasła i loginu można skorzystać w dowolnym momencie, nie jest ono ograniczone czasowo.

3. Jak korzystać z portalu zarządzania online

Produkt zawiera prosty w obsłudze internetowy portal zarządzania, który pozwala instalować produkt na urządzeniach.

Instalowanie produktu na innych urządzeniach

W portalu zarządzania możesz dodawać komputery, smartfony i tablety do konta oraz wysyłać instalator na nowe urządzenia. Gdy zainstalujesz produkt na nowym urządzeniu, zostanie ono uwzględnione w portalu zarządzania.

Zarządzanie ustawieniami funkcji Reguły rodzinne

W portalu zarządzania możesz ustawić ograniczenia dotyczące korzystania z urządzeń przez dzieci. Obejmuje to limity czasu przeglądania Internetu i używania aplikacji oraz określenie dozwolonych typów zawartości, które dzieci mogą wyświetlać na swoich urządzeniach.

Uwaga: Ta funkcja nie jest dostępna we wszystkich wersjach produktu.

4. Jak uzyskać szybki dostęp do ustawień produktu

Dostęp do niektórych ustawień produktu można uzyskać z menu kontekstowego ikony na pasku zadań.

Aby otworzyć menu kontekstowe ikony na pasku zadań, wykonaj te instrukcje:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu Windows.

   Uwaga: Jeśli ikona produktu jest ukryta, najpierw kliknij strzałkę Pokaż ukryte ikony na pasku zadań.

2. Menu kontekstowe zawiera następujące opcje:

Opcja	Opis
Sprawdź dostępność aktualizacji	Sprawdza dostępność aktualizacji i pobiera je.
Wyświetl ostatnie wydarzenia	Wyświetla listę działań wykonanych przez produkt w celu ochrony komputera.
Otwórz ustawienia	Otwiera ustawienia produktu.
Informacje	Pokazuje informacje o wersji produktu.

5. Jak udostępnić licencję?

Licencje pakietu Bezpiecznie w Internecie możesz udostępniać rodzinie i znajomym, zapraszając te osoby do swojej grupy w portalu. Gdy znajomi zaakceptują zaproszenie i utworzą własne konta, będą mogli zainstalować dowolne z aplikacji pakietu Bezpiecznie w Internecie na swoich urządzeniach.

Z licencji korzystają wszyscy członkowie tej samej grupy. W przypadku aplikacji ID PROTECTION obowiązuje też wspólny limit monitorowania adresów e-mail w subskrypcji Bezpiecznie w Internecie.

Zarządzanie subskrypcjami

Na stronie głównej możesz sprawdzić liczbę wolnych licencji.

Aby uzyskać dostęp do informacji dotyczących konta i ustawień powiadomień oraz edytować adres e-mail usługi, na górnym pasku wybierz opcję <Twoja nazwa> > Ustawienia konta.

6. Jak wyświetlić działania podjęte przez produkt?

Ikona stanu ochrony wskazuje, że produkt działa. W polu statystyk ochrony można sprawdzić, w jaki sposób komputer został ochroniony.

Ikony stanu zabezpieczeń

Ikona stanu ochrony pokazuje ogólny stan produktu i jego funkcji.

Ikony stanu ochrony:

Ikona stanu	Nazwa stanu	Opis
	OK	Ten komputer jest chroniony. Funkcje zostały włączone i działają prawidłowo.
	Ostrzeżenie	Komputer nie jest w pełni chroniony. Produkt wymaga uwagi – na przykład długo nie był aktualizowany lub wyłączono funkcję zabezpieczeń.
	Błąd	Komputer nie jest chroniony. Produkt wymaga natychmiastowego działania – na przykład wyłączono krytyczną funkcję lub subskrypcja wygasła.

7. Jak wyświetlić statystyki ochrony

Produkt pokazuje obracający się licznik statystyk ochrony na stronie Subskrypcja.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Subskrypcja.

Możesz zobaczyć, jak produkt chronił zarówno Twoje urządzenie, jak i przeglądanie.

Statystyka	Opis
Pliki do pobrania zostały zweryfikowane jako bezpieczne	Liczba plików przeskanowanych przez produkt w przychodzącym ruchu internetowym, zanim zostaną one zapisane na komputerze. Oprócz plików pobranych za pośrednictwem przeglądarki internetowej uwzględniane są tu również pliki pobrane w tle, na przykład pakiety aktualizacji pobierane automatycznie przez przeglądarkę.
Pliki sprawdzone w tle	Liczba plików przeskanowanych przez produkt. Ta łączna liczba obejmuje statystyki dotyczące wszystkich kont użytkowników na tym komputerze. **Uwaga:** Uwzględniane są też zduplikowane skanowania, więc jeśli na przykład produkt skanuje dwa razy ten sam plik, łączna liczba zwiększy się o dwa.
Zabezpieczone sesje bankowe	Liczba sesji bankowych zabezpieczonych przez produkt. Ta liczba zwiększa się za każdym razem, kiedy aktywowana jest ochrona bankowości podczas uzyskiwania dostępu do strony bankowości internetowej.
Sprawdzone strony internetowe	Liczba odwiedzonych stron internetowych, w przypadku których produkt sprawdził reputację.
Potencjalnie szkodliwe pliki zostały zablokowane	Liczba szkodliwych, potencjalnie niechcianych oraz niechcianych plików zablokowanych przez produkt. W tej liczbie nie są uwzględniane pobrane pliki, które zostały zablokowane przez produkt przed zapisaniem ich na komputerze. Ta łączna liczba obejmuje statystyki dotyczące wszystkich kont użytkowników na tym komputerze. **Uwaga:** Jeśli produkt zablokuje na przykład ten sam plik dwa razy, ta łączna liczba jest zwiększana o dwa.
Zablokowane szkodliwe strony internetowe	Liczba szkodliwych stron internetowych, które zostały zablokowane przez produkt.

8. Jak wyświetlać aplikacje oraz pliki zablokowane przez produkt?

Możesz wyświetlać aplikacje oraz pliki zablokowane przez produkt oraz zarządzać nimi w widoku Kontrola aplikacji i plików.

Aby otworzyć widok Kontrola aplikacji i plików:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. Wybierz opcję Wirusy i zagrożenia.
3. Wybierz opcję Kontrola aplikacji i plików.

Zostanie otwarty widok Kontrola aplikacji i plików, który zawiera cztery karty:

Poddane kwarantannie

> Kwarantanna to bezpieczne repozytorium dla plików, które mogą być szkodliwe. Kwarantannie można poddać szkodliwe oprogramowanie oraz potencjalnie niechciane aplikacje w celu ich unieszkodliwienia. W razie potrzeby aplikacje i pliki można później przywrócić z kwarantanny. Jeśli element poddany kwarantannie nie jest potrzebny, można go usunąć. Usunięcie elementu z kwarantanny usuwa go bezpowrotnie z komputera.

Zablokowano

> Na tej karcie są wymienione aplikacje zablokowane przez funkcję DeepGuard. Blokuje ona monitorowane aplikacje, gdy wykonują podejrzane działania lub próbują nawiązać połączenie z Internetem.

Wykluczone

> Na tej karcie wyświetlane są aplikacje, pliki i foldery wykluczone ze skanowania. Funkcja DeepGuard nie blokuje działania żadnych wykluczonych aplikacji, a produkt nie skanuje wykluczonych lokalizacji w poszukiwaniu szkodliwych elementów. Wykluczać można zarówno foldery, jak i poszczególne pliki.

Chronione

> Na tej karcie są dostępne informacje o folderach chronionych przed szkodliwym oprogramowaniem, takim jak ransomware. Produkt blokuje wszystkie niebezpieczne aplikacje, uniemożliwiając im wprowadzanie zmian w plikach zapisanych w tych folderach.

9. Jak korzystać z trybu gier

Automatyczny tryb gier wymaga, aby na komputerze działał system Windows 10 o numerze kompilacji 1809 (aktualizacja z października 2018 r.) lub nowszy.

Domyślnie produkt automatycznie włącza tryb gier, gdy wykryje uruchomienie gry na komputerze. Są wtedy zatrzymywane wszelkie zaplanowane skanowania i wstrzymywane aktualizacje produktu oraz baz danych, aby ograniczyć użycie zasobów komputera i sieciowych. Zwolnione zasoby systemowe stają się dostępne dla gier, a podstawowe funkcje produktu nadal działają. Tryb gier jest automatycznie wyłączany, gdy przestajesz grać.

Uwaga: Jeśli na ponad 60 sekund przełączysz się z gry do innej aplikacji otwartej na komputerze (za pomocą klawiszy Alt+Tab), produkt założy, że już nie grasz, i wyłączy tryb gier.

Jeśli nie chcesz, aby tryb gier był automatycznie włączany, wyłącz go w następujący sposób:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Ustawienia > Ustawienia skanowania.
4. Wybierz opcję Edytuj ustawienia.

Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Wyłącz tryb gier.

Teraz tryb gier nie będzie włączany automatycznie.

Uwaga: W widoku Ustawienia możesz sprawdzić, kiedy ostatni raz rozpoczęła się sesja grania.

10. Jak skonfigurować ochronę dla dziecka?

Aby skonfigurować ochronę dla swojego dziecka:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Zarządzaj w polu Osoby i urządzenia.
3. W widoku Osoby i urządzenia i urządzenia wybierz opcję Dodaj urządzenie lub użytkownika.
4. Wybierz Urządzenie mojego dziecka > Kontynuuj.
5. Wybierz, w jaki sposób chcesz dostarczyć łącze instalacyjne do urządzenia, które chcesz chronić, a następnie wybierz Wyślij.
6. Otwórz wiadomość na urządzeniu dziecka i postępuj zgodnie z instrukcjami w wiadomości, aby zainstalować produkt na urządzeniu.
7. Po wyświetleniu okna konfiguracji produktu wybierz Zaakceptuj i kontynuuj jeśli zgadzasz się na Warunki licencji użytkownika końcowego.
8. Po zakończeniu instalacji potwierdź, że konfigurujesz ochronę profilu dziecka, wybierając Kontynuuj:
    a. Wpisz imię swojego dziecka.
    b. Wybierz grupę wiekową, do której należy Twoje dziecko.
    c. Wybierz przycisk Dalej.
    d. Zanim zaczniesz konfigurować Zasady rodzinne ustawienia, przedyskutuj z dzieckiem zasady rodzinne. Wybierz Następny.
9. Włącz Dzienne limity czasowe, aby ustawić maksymalną liczbę godzin, przez które dziecko może korzystać z urządzenia w dni powszednie i weekendy:
    a. Na dni powszednie, użyj suwaka, aby zmienić maksymalny dozwolony czas w ciągu dnia.
    b. Na weekendy, użyj suwaka, aby zmienić maksymalny dozwolony czas w ciągu dnia.

        Uwaga: Jeśli nie chcesz ograniczać czasu, jaki dziecko spędza na urządzeniu każdego dnia, przeciągnij suwak maksymalnie w lewo, aby ustawić dozwoloną liczbę godzin na Nieograniczony.

    c. Wybierz przycisk Dalej.
10. Pora snu uniemożliwi korzystanie z urządzenia w nocy. Możesz ustawić inną porę snu na wieczory szkolne (od niedzieli do czwartku wieczorem) i weekendy (od piątku do soboty) w następujący sposób:
    a. Włącz Noce szkolne:

        Przeciągnij suwak, aby ustawić godzinę rozpoczęcia i zakończenia pory snu.

    b. Włącz Weekendowe noce:

        Przeciągnij suwak, aby ustawić godzinę rozpoczęcia i zakończenia pory snu.

    c. Wybierz przycisk Dalej.
11. Włącz Filtrowanie zawartości, aby zablokować treści internetowe, do których nie chcesz, aby Twoje dzieci miały dostęp:
    a. Z listy kategorii wybierz treści internetowe, które chcesz zablokować we wszystkich przeglądarkach.

b. Wybierz przycisk Dalej.

Skonfigurowałeś teraz ochronę dla swojego dziecka. Aby wyświetlić i zarządzać powyższym profilem dziecka, przejdź do produktu Osoby i urządzenia na własnym urządzeniu lub zaloguj się na swoje konto, aby uzyskać dostęp do portalu zarządzania online.

11. Jak edytować ustawienia kontroli aplikacji?

Dzięki Kontroli Aplikacji możesz wybrać, które aplikacje są zawsze dozwolone, które są ograniczone przez limity czasowe i które są zawsze blokowane na urządzeniach dziecka. Połączenia i wiadomości SMS są zawsze dozwolone.

Jeśli chcesz edytować ustawienia Kontroli aplikacji dla profilu Twojego dziecka, wykonaj następujące czynności:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Zarządzaj w polu Osoby i urządzenia.
3. W widoku Osoby i urządzenia i urządzenia wybierz profil dziecka, który chcesz edytować.
4. W sekcji ZASADY RODZINNE wybierz Kontrola aplikacji.

   Gdyby Kontrola aplikacji jest wyłączony, użyj suwaka, aby ją włączyć.

5. Aby zobaczyć listę aktualnych urządzeń, które mają włączoną funkcję Kontrola aplikacji, wybierz Na jakich urządzeniach działa Kontrola aplikacji.

   Uwaga: Kontrola aplikacji jest obsługiwana tylko przez urządzenia z systemem Android.

6. Pod USTAWIENIA DOMYŚLNE, możesz określić, jak nowo zainstalowana aplikacja jest traktowana przez Kontrolę aplikacji:
   - Ograniczony czasowo - Oznacza to, że korzystanie z aplikacji jest ograniczone przez dzienne limity czasowe i limity pory snu.
   - Zawsze dozwolone - Oznacza to, że korzystanie z aplikacji nie jest ograniczone przez dzienne limity czasu ani limity pory snu.
   - Zawsze zablokowane - Oznacza to, że aplikacja nie może być w ogóle używana.
7. Pod WSZYSTKIE AKTUALNE APLIKACJE, możesz zobaczyć aplikacje, które zostały już zainstalowane na urządzeniu. Dla każdej aplikacji możesz indywidualnie wybrać, czy jest ograniczona czasowo, zawsze dozwolona, czy zawsze zablokowana.
8. Aby zapisać zmiany, wybierz ZAPISZ.

12. Jak edytować ustawienia dziennego limitu czasu?

Możesz kontrolować, kiedy i jak długo dziecko może korzystać z urządzenia.

Jeśli chcesz edytować ustawienia dziennego limitu czasu dla profilu Twojego dziecka, wykonaj następujące czynności:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Zarządzaj w polu Osoby i urządzenia.
3. W widoku Osoby i urządzenia i urządzenia, wybierz profil dziecka, który chcesz edytować.
4. W sekcji ZASADY RODZINNE wybierz Dzienne limity czasu. Gdyby Dzienne limity czasu jest wyłączony, użyj suwaka, aby go włączyć.
5. W widoku Dzienne limity czasu, ustaw maksymalną liczbę godzin, przez które Twoje dziecko może korzystać z urządzenia w dni powszednie i w weekendy:
   a. W dni powszednie, użyj suwaka, aby zmienić maksymalny dozwolony czas w ciągu dnia.
   b. W weekendy, użyj suwaka, aby zmienić maksymalny dozwolony czas w ciągu dnia.

Uwaga: Jeśli nie chcesz ograniczać czasu, przez jaki dziecko korzysta z urządzenia każdego dnia, przeciągnij suwak jak najdalej w lewo, aby ustawić dozwoloną liczbę godzin na Nieograniczony.

6. Aby zapisać zmiany, wybierz ZAPISZ.

13. Jak przywrócić elementy poddane kwarantannie?

Potrzebne elementy można przywracać z kwarantanny.

Jeśli potrzebujesz, możesz przywrócić aplikacje lub pliki z kwarantanny. Nie przywracaj żadnych elementów z kwarantanny, chyba że masz pewność, że nie stanowią zagrożenia. Przywrócone elementy wracają do oryginalnej lokalizacji na komputerze.

Aby przywrócić elementy z kwarantanny:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Poddane kwarantannie.
5. Wybierz element z kwarantanny, który chcesz przywrócić.
6. Kliknij przycisk Zezwalaj.
7. Kliknij przycisk Tak, aby potwierdzić, że chcesz przywrócić element z kwarantanny.

Wybrany element zostanie automatycznie przywrócony do oryginalnej lokalizacji. W zależności od typu infekcji element może zostać wykluczony ze skanowania w przyszłości.

Uwaga: Aby wyświetlić wszystkie wykluczone pliki i aplikacje, wybierz kartę Wykluczone w widoku Kontrola plików i aplikacji.

14. Jak korzystać ze skanowania w czasie rzeczywistym?

Aby usuwać szkodliwe pliki, zanim zdołają wyrządzić szkody na komputerze, skanowanie w czasie rzeczywistym powinno być zawsze włączone.

Zalecamy, aby ochrona przed wirusami była włączona przez cały czas. Możesz również skanować pliki ręcznie, konfigurować zaplanowane skanowanie, aby upewnić się, że na komputerze nie ma szkodliwych plików, a także skanować pliki wyłączone ze skanowania w czasie rzeczywistym.

Aby upewnić się, że skanowanie w czasie rzeczywistym jest włączone:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Włącz funkcję Ochrona antywirusowa.

15. Czy skanowanie w czasie rzeczywistym ma wpływ na wydajność komputera?

Zazwyczaj użytkownik nie dostrzega procesu skanowania, ponieważ trwa on krótko i nie korzysta z wielu zasobów systemowych. Ilość czasu i zasobów systemowych wykorzystywanych podczas skanowania w czasie rzeczywistym zależy między innymi od zawartości, lokalizacji oraz typu pliku.

Skanowanie plików na nośnikach wymiennych, takich jak dyski CD i DVD oraz przenośne dyski USB, trwa dłużej.

Uwaga: Skanowanie w czasie rzeczywistym nie obejmuje plików skompresowanych, na przykład *ZIP*.

Skanowanie w czasie rzeczywistym może spowolnić pracę komputera w następujących przypadkach:

- Komputer użytkownika nie spełnia wymagań systemowych.
- Użytkownik uzyskuje dostęp do wielu plików jednocześnie, na przykład podczas otwierania katalogu zawierającego wiele plików, które należy przeskanować.

16. Jak wykluczyć pliki i foldery ze skanowania?

Gdy wykluczysz pliki i foldery ze skanowania, nie będą one badane w poszukiwaniu szkodliwej zawartości.

Aby wykluczyć pliki lub foldery ze skanowania:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Wykluczone.

   W tym widoku jest wyświetlana lista wykluczonych plików i folderów.

5. Wybierz opcję Dodaj nowy.
6. Wybierz plik lub folder, który chcesz wykluczyć ze skanowania.
7. Wybierz przycisk OK.

Wybrane pliki i foldery nie będą uwzględniane podczas skanowania w przyszłości.

17. Jak ręcznie uruchomić skanowanie w poszukiwaniu wirusów?

Możesz przeskanować cały komputer, aby upewnić się, że nie zawiera szkodliwych plików ani niechcianych aplikacji.

Pełne skanowanie komputera sprawdza wszystkie wewnętrzne i zewnętrzne dyski twarde w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji. Ta funkcja przeprowadza również sprawdzanie pod kątem plików ukrytych przez programy typu „rootkit”. Pełne skanowanie komputera może potrwać dłuższy czas. Możesz też przeskanować tylko obszary systemu zawierające zainstalowane aplikacje, aby bardziej wydajnie znaleźć i usunąć niechciane aplikacje i szkodliwe elementy z komputera.

Aby przeskanować komputer, wykonaj te instrukcje:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.

2. Jeśli chcesz zoptymalizować sposób ręcznego skanowania komputera, wybierz opcję Wirusy i zagrożenia > Ustawienia.
    a. Na ekranie Ustawienia wybierz opcję Ustawienia skanowania.
    b. Jeśli nie chcesz skanować wszystkich plików, wybierz opcję Skanuj tylko pliki tych typów, które często zawierają szkodliwy kod (szybsze).

        Gdy jest wybrana ta opcja, są skanowane między innymi pliki mające te rozszerzenia: com, doc, dot, exe, htm, ini, jar, pdf, scr, wma, xml, zip.

    c. Aby skanować pliki, które znajdują się w skompresowanych archiwach, takich jak pliki ZIP, wybierz opcję Skanuj wewnątrz plików skompresowanych. Skanowanie zawartości plików skompresowanych wymaga więcej czasu. Aby skanować pliki archiwum, ale nie pliki, które się w nim znajdują, pozostaw tę opcję niezaznaczoną,
    d. Wybierz przycisk OK, aby zamknąć okno Ustawienia.
3. W widoku głównym produktu wybierz opcję Wirusy i zagrożenia.
4. W widoku Wirusy i zagrożenia wybierz opcję Szybkie skanowanie lub Pełne skanowanie komputera.
    a. Szybkie skanowanie dotyczy tylko części systemu, w których są instalowane aplikacje, oraz lokalizacji często zawierających wirusy, takich jak foldery dokumentów. Ta funkcja pozwala szybciej wykrywać niechciane aplikacje i szkodliwe elementy oraz usuwać je z komputera.
    b. Pełne skanowanie komputera sprawdza wszystkie wewnętrzne i zewnętrzne dyski twarde w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji. Ta funkcja przeprowadza również sprawdzanie pod kątem plików ukrytych przez programy typu „rootkit”. Pełne skanowanie komputera może potrwać dłuższy czas.

    Rozpoczyna się skanowanie.

5. Jeśli skaner wykryje szkodliwe elementy, wyświetli ich listę.
6. Kliknij wykryty szkodliwy element, aby wybrać, co z nim zrobić.

Opcja	Opis
Wyczyść	Wyczyść pliki automatycznie. Pliki, których nie można wyczyścić, zostaną umieszczone w kwarantannie.
Kwarantanna	Umieść pliki w bezpiecznym miejscu, gdzie nie mogą się rozprzestrzeniać ani uszkodzić komputera.
Usuń	Trwale usuń pliki z komputera.
Pomiń	Nic nie rób i pozostaw pliki na komputerze.
Wyklucz	Zezwól na uruchomienie aplikacji i wyklucz ją ze skanowania w przyszłości.

7. **Uwaga:** Niektóre opcje są niedostępne w przypadku pewnych typów szkodliwych elementów.
8. Wybierz opcję Przetwórz wszystkie, aby uruchomić proces czyszczenia.
9. Skaner wyświetla wyniki obejmujące liczbę szkodliwych elementów, które zostały wyczyszczone.

Uwaga: Skaner może wymagać ponownego uruchomienia komputera w celu ukończenia procesu czyszczenia. Aby ukończyć usuwanie szkodliwych elementów, wybierz opcję Uruchom ponownie i ponownie uruchom komputer.

18. Jak skanować w Eksploratorze Windows?

Skanowanie dysków, folderów i plików w poszukiwaniu szkodliwych plików i niechcianych aplikacji można wykonywać w Eksploratorze Windows.

Jeśli określone pliki na komputerze budzą podejrzenia, możesz przeskanować tylko te pliki lub foldery. Takie skanowanie będzie trwać znacznie krócej niż skanowanie całego komputera. Na przykład po podłączeniu do komputera zewnętrznego dysku twardego lub pamięci USB możesz przeskanować te urządzenia, aby upewnić się, że nie zawierają szkodliwych plików.

Aby przeskanować dysk, folder lub plik:

1. Kliknij prawym przyciskiem myszy plik, folder lub dysk, który chcesz przeskanować.
2. W menu wyświetlanym po kliknięciu prawym przyciskiem myszy wybierz polecenie Skanuj w poszukiwaniu wirusów.

   Skanowanie w poszukiwaniu wirusów zostanie uruchomione i sprawdzi wybrany dysk, folder lub plik.

Skanowanie w poszukiwaniu wirusów przeprowadzi użytkownika przez proces oczyszczania, jeśli wykryje szkodliwe pliki lub niechciane aplikacje.

19. Jak zaplanować skanowania?

Możesz skonfigurować automatyczne skanowanie komputera w poszukiwaniu wirusów i innych szkodliwych aplikacji i usuwanie ich, gdy komputer nie jest używany, lub okresowe uruchamianie skanowania, aby mieć pewność, że komputer nie jest zainfekowany.

Aby zaplanować skanowanie:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.
4. Wybierz opcję Ustawienia skanowania.
5. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

6. Włącz opcję Skanowanie zaplanowane.
7. W polu Wykonaj skanowanie wybierz częstotliwość automatycznego skanowania komputera.

Opcja	Opis
Codziennie	Komputer będzie skanowany codziennie.
Co tydzień	Komputer będzie skanowany w wybrane dni tygodnia. Wybierz je z listy.
Co cztery tygodnie	Skanuj komputer w wybrany dzień tygodnia co cztery tygodnie. Wybierz ten dzień z listy. Skanowanie rozpocznie się w najbliższy wybrany dzień tygodnia.

8. W polu Godzina rozpoczęcia określ, kiedy ma się zaczynać zaplanowane skanowanie.

9. Wybierz Uruchom skanowanie z niskim priorytetem aby zaplanowane skanowanie w mniejszym stopniu zakłócało inne działania na komputerze. Uruchomienie skanowania z niskim priorytetem trwa dłużej.
10. Jeśli nie chcesz skanować wszystkich plików, wybierz opcję Skanuj tylko pliki tych typów, które często zawierają szkodliwy kod (szybsze).

    Gdy jest wybrana ta opcja, są skanowane między innymi pliki mające te rozszerzenia: com, doc, dot, exe, htm, ini, jar, pdf, scr, wma, xml, zip.

11. Aby skanować pliki, które znajdują się w skompresowanych archiwach, takich jak pliki ZIP, wybierz opcję Skanuj wewnątrz plików skompresowanych. Skanowanie zawartości plików skompresowanych wymaga więcej czasu. Aby skanować pliki archiwum, ale nie pliki, które się w nim znajdują, pozostaw tę opcję niezaznaczoną,

Uwaga: Zaplanowane skanowania są anulowane po włączeniu trybu gier. Kiedy wyłączysz *tryb gry*, znowu działają zgodnie z harmonogramem.

20. Jak zezwalać na działanie aplikacji zablokowanych przez funkcję DeepGuard?

Aplikacje akceptowane i blokowane przez funkcję DeepGuard można kontrolować.

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, wykonaj następujące czynności:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Zablokowane.

   Ta opcja wyświetla listę aplikacji zablokowanych przez funkcję DeepGuard.

5. Znajdź aplikację, na uruchomienie której chcesz zezwolić, i kliknij przycisk Zezwalaj.
6. Kliknij przycisk Tak, aby potwierdzić, że chcesz zezwolić na używanie aplikacji.

Wybrana aplikacja zostanie dodana do listy Wykluczone, a funkcja DeepGuard zezwoli jej na wprowadzanie zmian w systemie.

21. Co to jest technologia DeepGuard?

Funkcja DeepGuard monitoruje aplikacje w celu wykrycia potencjalnie szkodliwych zmian w systemie.

Funkcja DeepGuard zapewnia, że używasz tylko bezpiecznych aplikacji. Bezpieczeństwo aplikacji jest weryfikowane na podstawie informacji z zaufanej usługi zewnętrznej. Jeśli nie można zweryfikować bezpieczeństwa aplikacji, funkcja DeepGuard zaczyna monitorować jej działanie.

Technologia DeepGuard blokuje nowe i dotychczas niewykryte *konie trojańskie*, *robaki*, *luki w oprogramowaniu* i inne szkodliwe aplikacje, które próbują wprowadzać zmiany na komputerze, a także uniemożliwia podejrzanym aplikacjom dostęp do Internetu.

Potencjalne szkodliwe zmiany w systemie, które są wykrywane przez technologię DeepGuard, obejmują:

- zmiany ustawień systemu (rejestru systemu Windows);
- próby wyłączenia ważnych programów systemowych, na przykład programów zabezpieczających, takich jak niniejszy produkt;
- próby edytowania ważnych plików systemowych.

Aby upewnić się, że funkcja DeepGuard jest aktywna:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień są wymagane uprawnienia administratora.

5. Włącz funkcję DeepGuard.

Gdy funkcja DeepGuard jest włączona, automatycznie blokuje aplikacje, które próbują wprowadzić w systemie potencjalnie szkodliwe zmiany.

22. Jak wyświetlić aplikacje wykluczone?

Aplikacje wykluczone ze skanowania można wyświetlać i usuwać z listy elementów wykluczonych, aby w przyszłości były uwzględniane podczas skanowania.

Jeśli produkt wykryje potencjalnie niechcianą aplikację, ale wiesz, że jest ona bezpieczna, lub jest to oprogramowanie szpiegujące niezbędne do używania innej aplikacji, możesz wykluczyć ją ze skanowania, aby produkt nie wyświetlał więcej ostrzeżeń dotyczących tej aplikacji.

Uwaga: Jeśli aplikacja zachowuje się jak wirus lub inne złośliwe oprogramowanie, nie można jej wykluczyć.

Aby wyświetlić aplikacje wykluczone ze skanowania:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Wykluczone.

   W tym widoku jest wyświetlana lista wykluczonych plików i folderów.

5. Aby ponownie przeskanować wykluczone aplikacje, wykonaj następujące czynności:
   a. Wybierz aplikację, którą chcesz uwzględnić podczas skanowania.
   b. Kliknij przycisk Usuń.

Nowe aplikacje pojawiają się na liście wykluczeń dopiero po dodaniu ich podczas skanowania i nie można dodać ich bezpośrednio do listy wykluczeń

23. Jak korzystać z ochrony przed atakami typu ransomware?

Funkcja Ochrona przed atakami typu ransomware monitoruje wskazany zbiór folderów pod kątem potencjalnie niebezpiecznych zmian, które mogą zostać wprowadzone przez oprogramowanie typu ransomware lub podobne zagrożenia.

Ransomware to szkodliwe oprogramowanie, które może zaszyfrować ważne pliki na komputerze, przez co nie można uzyskać do nich dostępu. Następnie przestępcy żądają okupu w zamian za przywrócenie plików, ale nie ma gwarancji, że uda się odzyskać osobiste pliki nawet po zapłaceniu.

Dostęp do folderów chronionych przez funkcję Ochrona przed atakami typu ransomware mogą uzyskiwać tylko bezpieczne aplikacje. Produkt wyświetla powiadomienie, gdy niebezpieczna aplikacja spróbuje uzyskać dostęp do chronionego folderu. Jeśli znasz taką aplikację i jej ufasz, możesz zezwolić jej na dostęp do folderu. Lista chronionych folderów funkcji Ochrona przed atakami typu ransomware jest też używana przez technologię DeepGuard w celu zapewnienia dodatkowej warstwy zabezpieczeń.

Możesz wybrać foldery wymagające dodatkowej ochrony przed szkodliwym oprogramowaniem, takim jak ransomware.

Uwaga: Musisz włączyć funkcję DeepGuard, aby korzystać z ochrony przed atakami typu ransomware.

Aby zarządzać chronionymi folderami:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.
4. Włącz funkcję Ochrona przed atakami typu ransomware.
5. Wybierz pozycję Wyświetl chronione foldery.
6. Wybierz kartę Chronione.

   Spowoduje to wyświetlenie listy aktualnie chronionych folderów.

7. Dodaj lub usuń foldery według potrzeb.

   Aby dodać nowy chroniony folder:

   a. Kliknij przycisk Dodaj nowe.
   b. Wybierz folder, który chcesz chronić.
   c. Kliknij opcję Wybierz folder.

   Aby usunąć folder:

   d. Wybierz folder na liście.
   e. Kliknij przycisk Usuń.

Wskazówka: Kliknij przycisk Przywróć ustawienia domyślne, jeśli chcesz wycofać wszystkie zmiany, które zostały wprowadzone na liście chronionych folderów od chwili zainstalowania produktu.

24. Jak dodawać i usuwać chronione foldery?

Możesz wybrać foldery wymagające dodatkowej ochrony przed szkodliwym oprogramowaniem, takim jak ransomware.

Ochrona przed atakami typu ransomware blokuje wszystkie niebezpieczne próby uzyskania dostępu o chronionych folderów.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Chronione.

   Spowoduje to wyświetlenie listy aktualnie chronionych folderów.

5. Dodaj lub usuń foldery według potrzeb.

   Aby dodać nowy chroniony folder:

   a. Kliknij przycisk Dodaj nowe.
   b. Wybierz folder, który chcesz chronić.
   c. Kliknij opcję Wybierz folder.

   Wskazówka: Musisz oddzielnie zezwolić poszczególnym aplikacjom na dostęp do chronionego folderu, dlatego nie zalecamy dodawania folderów zawierających zainstalowane gry lub aplikacje (na przykład folderów biblioteki Steam). Jeśli to zrobisz, te aplikacje mogą przestać działać.

   Aby usunąć folder:

   d. Wybierz folder na liście.
   e. Kliknij przycisk Usuń.

Wskazówka: Kliknij przycisk Przywróć ustawienia domyślne, jeśli chcesz wycofać wszystkie zmiany, które zostały wprowadzone na liście chronionych folderów od chwili zainstalowania produktu.

25. Jak korzystać z ochrony sabotażowej?

Ochrona przed manipulacją uniemożliwia szkodliwym aplikacjom zamknięcie podstawowych procesów bezpieczeństwa produktu.

Ochrona przed manipulacją chroni zainstalowany produkt zabezpieczający i jego usługi, procesy, pliki i wpisy rejestru przed zmianami lub wszelkimi próbami kontroli.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.

26. W jaki sposób zapobiegać pobieraniu szkodliwych plików przez aplikacje?

Możesz zapobiec 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. Zaawansowane zabezpieczenia sieciowe umożliwiają zapobieganie pobieraniu szkodliwych plików przez aplikacje, zanim takie pliki dotrą na komputer.

Aby zablokować aplikacjom możliwość pobierania szkodliwych plików, wykonaj następujące czynności:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Włącz funkcję Skanowanie ruchu internetowego.

Uwaga: To ustawienie działa nawet po wyłączeniu zapory.

27. Jak wyświetlić elementy poddane kwarantannie?

Są dostępne dodatkowe informacje na temat elementów umieszczonych w kwarantannie.

Kwarantanna to bezpieczne repozytorium plików, które mogą być szkodliwe. W kwarantannie można umieścić szkodliwe oprogramowanie oraz potencjalnie niechciane aplikacje w celu ich unieszkodliwienia. W razie potrzeby aplikacje i pliki można później przywrócić z kwarantanny. Jeśli element umieszczony w kwarantannie nie jest potrzebny, można go usunąć. Usunięcie elementu z kwarantanny usuwa go bezpowrotnie z komputera.

Aby wyświetlić szczegółowe informacje na temat elementów w kwarantannie:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Kontrola aplikacji i plików.

   Uwaga: Aby mieć dostęp do tych ustawień, musisz mieć uprawnienia administratora.

4. Wybierz kartę Poddane kwarantannie.

   Na liście znajduje się nazwa, data wykrycia i typ infekcji każdego elementu poddanego kwarantannie.

5. Kliknij dwukrotnie element poddany kwarantannie, aby zobaczyć więcej informacji.

   W przypadku pojedynczych elementów wyświetlana jest oryginalna lokalizacja elementu poddanego kwarantannie.

28. Co to jest szkodliwa zawartość?

Szkodliwe aplikacje i pliki mogą próbować uszkodzić dane lub uzyskać nieautoryzowany dostęp do systemu komputera w celu kradzieży prywatnych informacji.

29. Jak blokować szkodliwe witryny?

Włączenie funkcji Ochrona przeglądania powoduje blokowanie dostępu do szkodliwych witryn internetowych.

Aby włączyć funkcję Ochrona przeglądania:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Ochrona przeglądania i bankowości.
3. W widoku Ochrona przeglądania i bankowości wybierz opcję Ustawienia.

4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Włącz funkcję Ochrona przeglądania.
6. Jeśli przeglądarka jest otwarta, uruchom ją ponownie w celu zastosowania zmienionych ustawień.

Uwaga: Ochrona przeglądania wymaga, aby w używanej przeglądarce było włączone rozszerzenie Ochrona przeglądania.

30. Jak blokować podejrzane i zabronione witryny internetowe?

Funkcja Ochrona przeglądania pozwala zapobiegać przypadkowemu otwieraniu witryn internetowych, które są podejrzane lub zawierają zabronione treści.

Czasami możesz otworzyć witrynę internetową zawierającą podejrzane, szkodliwe lub zabronione treści. Taka witryna może być na przykład fałszywą kopią innej, być znanym źródłem spamu, zawierać potencjalnie niechciane programy albo treści, które są niedozwolone w świetle obowiązującego prawa.

Korzystając z funkcji Ochrona przeglądania, możesz zapobiec przypadkowemu odwiedzaniu takich witryn.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Ochrona przeglądania i bankowości.
3. W widoku Ochrona przeglądania i bankowości wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Upewnij się, że jest włączona funkcja Ochrona przeglądania.
6. Jeśli chcesz, aby oprócz witryn uznanych za niebezpieczne, były też blokowane witryny podejrzane, wybierz opcję Blokuj podejrzane witryny.
7. Jeśli chcesz zablokować witryny zawierające zabronione materiały, wybierz opcję Blokuj podejrzane witryny.
8. Jeśli przeglądarka jest otwarta, uruchom ją ponownie w celu zastosowania zmienionych ustawień.

Uwaga: Ochrona przeglądania wymaga, aby w używanej przeglądarce było włączone rozszerzenie Ochrona przeglądania.

31. Co oznaczają poszczególne ikony reputacji?

Funkcja Ochrona przeglądania wyświetla ocenę bezpieczeństwa witryn na stronie wyników w wyszukiwarkach Google, Bing, Yahoo i DuckDuckGo.

Kolorowe ikony wskazują klasyfikację bezpieczeństwa bieżącej witryny. Klasyfikacja bezpieczeństwa łączy w wynikach wyszukiwarki jest wyświetlana przy użyciu takich samych ikon:

	Według naszych informacji dana witryna jest bezpieczna. Nie wykryliśmy w niej żadnych podejrzanych elementów.
	Ta witryna jest podejrzana. Zalecamy zachowanie ostrożności podczas jej odwiedzania. Unikaj pobierania jakichkolwiek plików i podawania danych osobowych.

	Ta witryna jest szkodliwa. Zalecamy unikanie jej odwiedzania.
	Nie przeanalizowaliśmy jeszcze tej witryny lub obecnie nie są dostępne żadne informacje na jej temat.
	Administrator pozwolił na otwarcie tej witryny.
	Administrator zablokował tę stronę internetową, dlatego nie możesz jej otworzyć.

Aby ikony reputacji były wyświetlane na stronie wyników wyszukiwania:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Ochrona przeglądania i bankowości.
3. W widoku Ochrona przeglądania i bankowości wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Upewnij się, że jest włączona funkcja Ochrona przeglądania.
6. Wybierz opcję Pokazuj klasyfikację reputacji witryn w wynikach wyszukiwania.
7. Jeśli przeglądarka jest otwarta, uruchom ją ponownie w celu zastosowania zmienionych ustawień.

Uwaga: Ochrona przeglądania wymaga, aby w używanej przeglądarce było włączone rozszerzenie Ochrona przeglądania

32. Co zrobić, gdy witryna sieci Web jest zablokowana?

Przy próbie uzyskania dostępu do witryny sklasyfikowanej jako szkodliwa jest wyświetlana strona blokowania funkcji ochrony przeglądania.

Gdy pojawi się strona blokowania funkcji ochrony przeglądania:

1. Aby otworzyć witrynę, wybierz opcję Dopuść witrynę na tym komputerze. Zezwalanie na otwieranie zablokowanych witryn wymaga uprawnień administratora.

   Zostanie wyświetlone okno Dodaj dozwoloną witrynę z adresem, który chcesz dodać do dozwolonych.

2. Wybierz przycisk OK.

Zablokowana witryna zostanie otwarta, a produkt doda ją do listy dozwolonych witryn.

Uwaga: Jeśli strona blokowania nie jest wyświetlana, upewnij się, że w używanej przez Ciebie przeglądarce jest włączone rozszerzenie ochrony przeglądania

33. Jak włączyć funkcję Ochrona bankowości?

Po włączeniu funkcji Ochrona bankowości sesje i transakcje bankowe będą chronione.

Podczas korzystania z witryny internetowej banku lub realizowania płatności online funkcja Ochrona bankowości blokuje wszystkie połączenia, które nie są niezbędne do przeprowadzenia operacji bankowych, aby nie mogły wpływać na poufne transakcje.

Włącz funkcję Ochrona bankowości.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Ochrona przeglądania i bankowości.
3. W widoku Ochrona przeglądania i bankowości wybierz opcję Ustawienia.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Włącz funkcję Ochrona bankowości.
6. Aby dostosować ustawienia funkcji Ochrona bankowości:
   - Jeśli funkcja Ochrona bankowości ma pozostawiać otwarte wcześniej połączenia, usuń zaznaczenie opcji Rozłącz niezaufane aplikacje. Gdy to ustawienie jest zaznaczone, po włączeniu funkcji Ochrona bankowości są zamykane wszystkie aktywne połączenia internetowe z wyjątkiem połączeń zaufanych aplikacji.
   - Jeśli musisz używać narzędzia zewnętrznego, które jest blokowane podczas sesji funkcji Ochrona bankowości, usuń zaznaczenie opcji Rozłączaj narzędzia wiersza poleceń i skryptowe.

     Uwaga: Zalecamy pozostawienie tego ustawienia zaznaczonego, jeśli tylko to możliwe. Niektóre ataki złośliwego oprogramowania są oparte na wbudowanych składnikach systemu Windows, takich jak narzędzie PowerShell, przy użyciu których złośliwe oprogramowanie uzyskuje dostęp do poświadczeń bankowych i danych osobowych.

   - Wybierz sposób obsługi danych skopiowanych do schowka przez funkcję Ochrona bankowości. Domyślnie jest zaznaczona opcja Wyczyść schowek – funkcja Ochrona bankowości czyści wszystkie dane ze schowka po zakończeniu sesji.

     Jeśli funkcja Ochrona bankowości nie ma czyścić schowka, usuń zaznaczenie tego ustawienia.

   - Domyślnie podczas sesji bankowości jest zablokowany zdalny dostęp do urządzenia. Transakcje bankowe są zawsze prywatne i poufne. Nigdy nie loguj się do banku internetowego, jeśli ktoś ma zdalny dostęp do używanego urządzenia.

     Ważne: Nie usuwaj zaznaczenia ustawienia Blokuj dostęp zdalny podczas sesji bankowej na czyjąkolwiek prośbę, chyba że znasz zarówno osobę żądającą dostępu, jak i dokładny cel takiego żądania.

Uwaga: Ochrona bankowości wymaga, aby w używanej przeglądarce było włączone rozszerzenie Ochrona przeglądania.

34. Jak przeglądać i zarządzać monitorowanymi adresami e-mail?

Możesz monitorować swoje adresy e-mail i otrzymywać wskazówki, co zrobić, jeśli Twoje dane osobowe zostały ujawnione w wyniku naruszenia danych.

Uwaga: Ma to zastosowanie tylko wtedy, gdy Twoja subskrypcja obejmuje licencję na aplikację do ochrony tożsamości i menedżera haseł.

Monitorowanie tożsamości pomaga chronić Twoje dane osobowe, powiadamiając Cię o wszelkich naruszonych usługach online, z których możesz korzystać, oraz udzielając szczegółowych instrukcji dotyczących sposobu naprawy po incydencie przy minimalnych szkodach.

Wiadomość e-mail z powiadomieniem zawiera informacje o tym, jakie dane osobowe (PII) zostały powiązane z naruszeniem; czym było naruszenie; jaka firma lub podmiot został naruszony; kiedy doszło do naruszenia; oraz jakie inne informacje umożliwiające identyfikację osoby zostały powiązane z monitorowanym adresem e-mail, takie jak hasła, numery kart kredytowych, adres pocztowy i tak dalej.

Aby rozpocząć monitorowanie adresu e-mail:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Monitorowanie tożsamości.
3. Wybierz + Dodaj monitorowany przedmiot.
4. Wpisz adres e-mail i wybierz Dodaj.

   Ważne: Na podany adres e-mail wyślemy wiadomość z linkiem potwierdzającym.

5. Wybierz przycisk OK.

   Aplikacja natychmiast sprawdza istniejące naruszenia danych, aby sprawdzić, czy Twój adres e-mail jest wymieniony w którymkolwiek z nich. Jeśli Twój adres e-mail pojawia się w którymkolwiek ze znanych naruszeń danych, naruszenia są wymienione w widoku Monitorowanie. Aby móc zobaczyć bardziej szczegółowe informacje o wyciekających danych i zalecanych działaniach, musisz najpierw potwierdzić swój adres e-mail.

6. Otwórz wiadomość e-mail z potwierdzeniem i wybierz Potwierdź adres email aby potwierdzić, że to jest Twój adres e-mail.

   Ten adres e-mail staje się automatycznie Twoim kontaktowym adresem e-mail. Jeśli chcesz, możesz później zmienić go na inny adres e-mail.

7. Aby zobaczyć szczegóły ujawnionych danych osobowych i co należy zrobić, dotknij konkretnego naruszenia wymienionego w Monitorowanie pogląd.
8. Jeśli chcesz monitorować więcej adresów e-mail, wybierz Monitorowane przedmioty w Monitorowanie wyświetl i powtórz powyższe kroki, zaczynając od kroku 3.

Ważne: Aby wyeliminować ryzyko niewłaściwego wykorzystania Twoich informacji, zachęcamy Cię do jak najszybszego wykonania zalecanych działań.

35. Jak zezwalać na otwieranie określonych stron internetowych i je blokować?

Na liście wyjątków witryn internetowych znajdują się dozwolone i zablokowane witryny.

Możesz ręcznie blokować określone witryny internetowe, które uważasz za szkodliwe, lub zezwalać na automatyczne blokowanie witryn, jeśli masz pewność, że są one bezpieczne.

Aby wyświetlić i edytować listę wyjątków stron internetowych:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Ochrona przeglądania i bankowości.
3. W widoku Ochrona przeglądania i bankowości wybierz opcję Zarządzaj zablokowanymi i dozwolonymi witrynami.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

4. Aby dodać nową witrynę internetową do jednej z list:

a. Kliknij kartę Dozwolone, jeśli chcesz zezwolić na dostęp do witryny, lub kartę Zablokowane, jeśli chcesz zablokować witrynę.
b. Aby dodać nową witrynę do listy, kliknij przycisk Dodaj nową.
c. Wprowadź adres witryny internetowej, którą chcesz dodać, i kliknij przycisk OK.

Witryna jest teraz wymieniona jako dozwolona lub zablokowana witryna internetowa.

Aby usunąć dozwoloną lub zablokowaną witrynę z listy, najpierw wybierz witrynę, którą chcesz usunąć, a następnie wybierz Usunąć.

36. Co oznaczają poszczególne kategorie treści?

Możesz zablokować dostęp do kilku rodzajów treści.


Materiały dla dorosłych

Witryny przeznaczone dla pełnoletniej widowni zawierające treści o jednoznacznie seksualnym charakterze lub podteksty seksualne. Na przykład strony sex-shopów lub prezentujące nagość w kontekście seksualnym.


Niepokojące treści

Witryny internetowe zawierające obrazy, treści lub gry wideo, które mogą zaniepokoić użytkownika. Ta kategoria obejmuje informacje, zdjęcia i filmy o odrażającym, wstrząsającym lub przerażającym charakterze, które potencjalnie mogą zaniepokoić młodsze dzieci.


Narkotyki

Witryny internetowe zachęcające do zażywania narkotyków. Na przykład strony z informacjami dotyczącymi kupowania, uprawiania lub sprzedawania takich substancji w dowolnej postaci.


Hazard

Witryny internetowe, w których można prowadzić zakłady o prawdziwe pieniądze lub dowolną formę środków. Na przykład strony kasyn i loterii online oraz blogi i fora zawierające informacje o hazardzie, zarówno internetowym, jak i rzeczywistym.


Alkohol i tytoń

Witryny internetowe prezentujące lub promujące napoje alkoholowe bądź wyroby tytoniowe, w tym strony producentów, takich jak gorzelnie, winnice i browary. Na przykład witryny promujące festiwale piwa i strony barów lub klubów nocnych.


Treści nielegalne

Witryny zawierające obrazy lub informacje zabronione na mocy prawa.


Nielegalne pliki do pobierania

Witryny umożliwiające nieautoryzowane pobieranie plików lub zapewniające nielegalny dostęp do oprogramowania. Na przykład strony podmiotów tworzących i rozpowszechniających programy, które mogą posłużyć do naruszania zabezpieczeń sieci i systemów.


Przemoc

Witryny internetowe, których treść może nakłaniać do przemocy, albo zawierające obrazy lub filmy o brutalnym bądź szokującym charakterze. Na przykład strony z informacjami o gwałtach, dokuczaniu, prześladowaniu, bombach, atakach, morderstwach lub samobójstwach.


Nienawiść

Witryny internetowe szerzące uprzedzenia wobec określonych religii, ras, narodowości, płci, grup wiekowych, niepełnosprawności lub orientacji seksualnych. Na przykład strony promujące działanie na szkodę osób, zwierząt lub instytucji albo zawierające opisy i obrazy przedstawiające przemoc fizyczną w stosunku do nich.


Broń

Witryny internetowe zawierające informacje, ilustracje, zdjęcia lub filmy związane z tematyką broni lub jakimikolwiek przedmiotami, które mogą być używane jako broń lub służyć do wyrządzenia krzywdy ludziom bądź zwierzętom. Obejmuje to strony organizacji, które promują używanie broni, na przykład kół myśliwskich i klubów strzeleckich. Do tej kategorii należą zabawki i repliki broni, takie jak markery paintballowe, broń airsoftowa i wiatrówki.


Randki

Witryny internetowe umożliwiające znajdowanie partnerów życiowych lub seksualnych. Na przykład usługi randkowe i strony z ogłoszeniami matrymonialnymi.


Zakupy i aukcje

Witryny, w których można kupować jakiekolwiek produkty i usługi. Obejmuje to między innymi witryny z katalogami przedmiotów, które ułatwiają zamawianie i kupowanie online, a także witryny zawierające informacje o zamawianiu i kupowaniu przedmiotów online.


Sieci społecznościowe

Portale społecznościowe umożliwiające użytkownikom ogólną komunikację lub zapewniające kontakt z określoną grupą osób w celach towarzyskich, biznesowych itp. Na przykład strony, na których można utworzyć profil członka, aby dzielić się osobistymi lub służbowymi zainteresowaniami. Obejmuje to media społecznościowe, takie jak serwis Twitter.


Narzędzia do zapewniania anonimowości

Witryny internetowe umożliwiające pomijanie filtrów sieciowych albo udostępniające instrukcje dotyczące takich czynności, w tym internetowe usługi tłumaczeniowe, które pozwalają wykonywać takie działania. Na przykład strony z listami publicznych serwerów proxy, których można używać do pomijania filtrów sieciowych.


Nieznane

Witryny internetowe, które nie zostały skategoryzowane. Przy użyciu tej kategorii można zablokować nieznane treści.

37. Co to jest zapora?

Zapora uniemożliwia intruzom i szkodliwym aplikacjom dostęp do komputera z Internetu.

Zapora umożliwia nawiązywanie tylko bezpiecznych połączeń internetowych z komputera i blokuje włamania z Internetu.

38. Jak zmienić ustawienia zapory systemu Windows?

Gdy zapora jest włączona, ogranicza dostęp do i z komputera. Niektóre aplikacje do prawidłowego działania mogą wymagać zezwolenia na dostęp przez zaporę.

W celu ochrony komputera produkt korzysta z Zapory systemu Windows.

Aby zmienić ustawienia zapory systemu Windows, wykonaj następujące czynności:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. Wybierz pozycję Ustawienia zapory systemu Windows.

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

39. Jak korzystać z aktualizacji automatycznych?

Aktualizacje automatyczne pozwalają chronić komputer przed najnowszymi zagrożeniami.

Kiedy jest dostępne połączenie z Internetem, produkt automatycznie pobiera na komputer najnowsze aktualizacje. Oprogramowanie wykrywa ruch sieciowy i nie przeszkadza w korzystaniu z Internetu w innych celach nawet w przypadku wolnego połączenia sieciowego.

40. Jak sprawdź dostępność aktualizacji?

Możliwe jest wyświetlenie daty i godziny ostatniej aktualizacji.

Gdy aktualizacje automatyczne są włączone i jest dostępne połączenie z Internetem, produkt automatycznie otrzymuje najnowsze aktualizacje.

Aby sprawdzić dostępność aktualizacji dla zainstalowanych produktów:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Sprawdź aktualizacje.

4. W obszarze Historia aktualizacji zostaną wyświetlone szczegóły ostatnich aktualizacji.
5. Aby ręcznie sprawdzić dostępność aktualizacji, wybierz opcję Sprawdź teraz.

   Produkt automatycznie instaluje najnowsze aktualizacje, jeśli są dostępne.

   Uwaga: Aby było można sprawdzić dostępność aktualizacji, musi być aktywne połączenie internetowe.

41. Jak zmienić ustawienia połączenia z Internetem?

Instrukcje dotyczące wybierania, jak Twój komputer łączy się z Internetem i jak traktować aktualizacje podczas korzystania z sieci komórkowej.

Dostawca usług internetowych może zasugerować lub wymagać używania serwera proxy, który pełni rolę pośrednika pomiędzy komputerem i Internetem. Taki serwer przejmuje wszystkie żądania wysyłane do Internetu i sprawdza, czy może je obsłużyć, korzystając ze swojej pamięci podręcznej. Serwery proxy są używane do zwiększania wydajności, filtrowania żądań i ukrywania komputera w Internecie w celu poprawy bezpieczeństwa.

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz opcję Wirusy i zagrożenia.
3. W widoku Wirusy i zagrożenia wybierz opcję Sprawdź aktualizacje.
4. W polu Ręczna konfiguracja serwera proxy określ, czy komputer korzysta z serwera proxy do nawiązywania połączenia z Internetem.
   - Jeśli komputer jest bezpośrednio połączony z Internetem, wybierz opcję Nie używaj.
   - Aby zastosować ustawienia serwera proxy HTTP skonfigurowane w domyślnej przeglądarce internetowej, wybierz opcję Użyj ustawień przeglądarki.
   - Aby ręcznie skonfigurować ustawienia serwera proxy HTTP, wybierz opcję Adres niestandardowy i dodaj adres serwera oraz numer portu.

42. Jak włączyć funkcję ulepszanie produktu?

Możesz nam pomóc w ulepszaniu produktów przez wysyłanie danych dotyczących użycia.

Aby wysyłać dane dotyczące użycia:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Ustawienia.
4. Otwórz stronę ustawień Prywatność.
5. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

6. W obszarze Ulepszanie produktu wybierz opcję Wysyłaj niespersonalizowane dane dotyczące użycia.

43. Gdzie znajdę mój identyfikator konta?

W przypadku kontaktu z pomocą techniczną może być konieczne podanie kodów tożsamości.

Aby wyświetlić swoje kody tożsamości:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.

2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Pomoc techniczna.
4. Znajdź swój identyfikator konta w obszarze Kod tożsamości.

44. Gdzie można znaleźć informacje o wersji produktu?

W przypadku kontaktu z pomocą techniczną może być konieczne podanie wersji produktu.

Aby wyświetlić informacje o bieżącej wersji:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Pomoc techniczna.
4. Informacje o zainstalowanym obecnie produkcie są dostępne w obszarze Informacje o wersji.

45. Jak uruchomić narzędzia pomocy technicznej?

Zanim skontaktujesz się z pomocą techniczną, uruchom narzędzie pomocy technicznej, aby zebrać podstawowe informacje o sprzęcie, systemie operacyjnym, konfiguracji sieci i zainstalowanym oprogramowaniu.

Aby uruchomić narzędzie pomocy technicznej:

1. Otwórz produkt, korzystając z menu Start w systemie Windows.
2. W widoku głównym wybierz przycisk menu ☰.
3. Wybierz opcję Pomoc techniczna.
4. Wybierz opcję Edytuj ustawienia.

   Uwaga: Do zmiany tych ustawień wymagane są uprawnienia administratora.

5. Wybierz Uruchom narzędzie wsparcia.
6. Wybierz opcję Uruchom diagnostykę w oknie Narzędzie pomocy technicznej.

   Zostanie uruchomione narzędzie pomocy technicznej i zostanie w nim wyświetlony postęp zbierania danych.

Po zakończeniu działania narzędzia zapisuje ono zgromadzone dane w archiwum na komputerze. Te dane (plik diagnostyczny) można przesłać, kontaktując się z działem obsługi klienta.

46. Co to są oszustwa telefoniczne?

Połączenia telefoniczne mogą być albo inicjowane przez oszustów, gdy dzwonią sami, albo mogą być efektem wyświetlenia reklamy lub łącza, które powoduje pokazanie okienka wyskakującego na komputerze. Takie okienka zawierają informacje o konieczności pilnego zadzwonienia pod wskazany numer pomocy technicznej. Mogą się pojawiać zupełnie niespodziewanie i niełatwo się ich pozbyć.

47. Jak rozpoznać oszustwo telefoniczne?

Tego rodzaju połączenia mają zwykle ustalony przebieg: oszuści zazwyczaj informują, że wystąpił problem z Twoim komputerem, na przykład jest na nim wirus, choć tak naprawdę go nie ma, i namawiają do zapłacenia za usługę, która także nie istnieje. Działają z zaskoczenia i grają na emocjach. Oto podstawowy scenariusz:

- Oszuści telefoniczni twierdzą, że pochodzą od znanej firmy, takiej jak Microsoft, Twój bank, a nawet operator sieci. Ponieważ używają renomowanej nazwy, zapewnia to większą swobodę. Wydają się również posiadać wiedzę i używają terminów technicznych, co sprawia, że wydają się uzasadnione i wiarygodne.

- Ryzyko wydaje się realne, więc bojąc się możliwych wirusów komputerowych, udzielasz oszustom dostępu do swojego komputera. Oni przekonują Cię do zainstalowania aplikacji, która daje im dostęp do Twojego komputera za pomocą narzędzi do uzyskiwania zdalnego dostępu.

- Gdy oszuści mają już dostęp do komputera, udają, że usuwają wirusa. Mogą też zapytać o Twoje osobiste poświadczenia. Gdy oszuści „usuną" problem, poproszą o zalogowanie się do banku online lub wypełnienie formularza z danymi karty kredytowej. Oszuści obciążą Cię opłatą za fikcyjną usługę, która będzie znacznie wyższa niż Ci się wydawało. Tak naprawdę nie wiadomo, jaka będzie kwota obciążenia.

48. Rzeczy do zapamiętania na temat niepożądanych połączeń telefonicznych

- Jeśli nadejdzie tego rodzaju połączenie, zastanów się, czy rozmówca dzwoni na Twoją prośbę.

  Uwaga: Zwykle obsługa klienta dzwoni do Ciebie, jeśli już się z nimi skontaktowałeś i utworzyłeś zgłoszenie do pomocy technicznej.

- Zdalne sesje są często wykorzystywane przy udzielaniu pomocy technicznej jako sposób asystowania przy rozwiązywaniu problemów.

  Zapamiętaj: Zezwalaj tylko na zdalne sesje z osobami lub firmami, które znasz i którym ufasz. Zezwalaj na sesje zdalne tylko wtedy, gdy wcześniej skontaktowałeś się z usługodawcą i masz ważne zgłoszenie do pomocy technicznej. Ponadto chroń swoje dane dostępu zdalnego, tak jak chroń każde inne hasło.

- Nigdy nie dawaj dostępu do swojego urządzenia osobom, których nie znasz. Udzielenie oszustom zdalnego dostępu oznacza w rezultacie przyznanie praw administratora do komputera. Nawet jeśli masz zainstalowanie oprogramowanie antywirusowe, nie będzie ono w stanie Ciebie chronić, ponieważ to oszuści będą mieli kontrolę nad komputerem.

- Firma Microsoft poinformowała użytkowników, że nigdy nie umieszcza numerów telefonów w komunikatach o błędach i komunikatach ostrzegawczych.

- Nigdy lekkomyślnie nie udostępniaj żadnych osobistych poświadczeń ani danych karty kredytowej.

- Natychmiast zakończ połączenie.

- Tego rodzaju połączenia telefoniczne są niezgodne z prawem. W razie wątpliwości zwróć się do organów zajmujących się oszustwami i zgłoś je.

49. Co zrobić, gdy uważa się, że padło się ofiarą oszustwa

Jeśli uważasz, że ktoś próbuje Cię oszukać, i rozpoznajesz scenariusz opisany przez nas powyżej, wykonaj następujące czynności:

- Działaj natychmiast: zadzwoń na dedykowany numer.

- Natychmiast skontaktuj się z emitentem karty kredytowej lub bankiem, zgłoś oszustwo i unieważnij wszelkie karty bankowe i kredytowe. Jeśli się pospieszysz, może się nawet udać zatrzymać transakcję i cofnąć obciążenia.
- Zgłoś oszustwo do odpowiedniego organu.
- Zmień wszystkie hasła do witryn i usług, które Twoim zdaniem mogą być zagrożone.
- Odinstaluj wszelkie nieznane oprogramowanie innych firm.
- Uruchom pełne skanowanie na komputerze: Otwórz produkt zabezpieczający, a następnie wybierz Wirusy i zagrożenia > Pełne skanowanie komputera.

50. Co to jest Cyber Pomoc

Zadzwoń na dedykowany numer Cyber Pomocy aby:

- Mieć bezpośredni kontakt z firmą F-Secure w przypadku pytań/problemów związanych z kluczowymi kompetencjami firmy F-Secure w zakresie cyberbezpieczeństwa: odpowiadanie na pytania związane z ID Monitoring (alarmy o naruszeniach i instrukcje dotyczące naruszeń)
- uzyskać wskazówki w przypadku narażenia danych osobowych
- uzyskać wskazówki w przypadku phishingu
- uzyskać wskazówki w przypadku ataków złośliwego oprogramowania i hackingu
- uzyskać wskazówki dotyczących serii incydentów offline (na przykład: kradzież paszportu, kradzież portfela)
- uzyskać wskazówki, jak być bezpiecznym w sieci
- Pomoc prawna, pełnomocnictwo, remediacja i całkowite przywrócenie do stanu pierwotnego jest poza zakresem usług.

51. Ochrona przeglądania

Ochrona przeglądania to usługa reputacji, która traktuje strony internetowe jako bezpieczne lub niebezpieczne. Niebezpieczne strony są zwykle znane jako strony wyłudzające informacje i zawierające złośliwe oprogramowanie. Reputacja stron jest sprawdzana bezgłośnie w tle podczas przeglądania Internetu. Zapytania o reputację są optymalizowane w celu zapewnienia najlepszych wrażeń z przeglądania. Dostęp do bezpiecznych witryn odbywa się normalnie, bez żadnych zakłóceń. Dostęp do niebezpiecznych witryn jest po prostu blokowany za pomocą okna dialogowego. Ochrona przeglądania chroni również Twoich klientów przed oszustwami za pośrednictwem poczty elektronicznej lub wiadomości SMS kierujących na przykład do fałszywych witryn bankowych, o ile korzystają oni z przeglądarek zabezpieczonych przez funkcję ochrony przeglądania.

Złośliwe oprogramowanie i strony wyłudzające informacje często przetwarzają i wprowadzają nowe domeny, aby ominąć ochronę. Ze względu na ograniczoną dostępność adresów IP zmieniają się one rzadziej. Zastosowanie technologii VPN umożliwia uniemożliwienie dostępu do znanych złośliwych adresów IP, nawet jeśli odwiedzana przez użytkownika domena jest nowa. Ocena adresów IP umożliwia również uniemożliwienie dostępu do grupy złych witryn internetowych zarejestrowanych w tej samej domenie. Firma F-Secure może również utworzyć białą listę domen pod tym samym adresem IP, aby zapobiec fałszywym pozytywom. Rozwiązanie F-Secure TOTAL for Windows może obsługiwać to na urządzeniu nawet bez filtrowania na poziomie bramy VPN.

52. Ochrona bankowości

Ochrona bankowości dodaje kolejną warstwę zabezpieczeń do ochrony przeglądania i ochrony przed wirusami. Ochrona przeglądania uniemożliwia dostęp do niebezpiecznych witryn internetowych, takich jak znane fałszywe witryny bankowe lub witryny wyłudzające informacje, natomiast ochrona bankowości poprawia widoczność i bezpieczeństwo podczas wchodzenia na bezpieczną witrynę bankową. Ochrona przeglądania zapewnia bezpieczeństwo w tle, nie powoduj zakłócania normalnego przeglądania. Ochrona bankowości została zaprojektowana tak, aby bezpieczeństwo było bardziej widoczne i namacalne.

Ochrona bankowości pokazuje użytkownikowi wskaźnik (baner lub toast) w kontekście przeglądarki, gdy wchodzi na bezpieczną stronę bankową, a połączenie ze stroną jest zabezpieczone (https). Część ochrony przeglądania automatycznie zapobiega dostępowi do znanych fałszywych witryn bankowych lub wyłudzających informacje.

Ochrona bankowości F-Secure for Windows zapobiega również innym połączeniom podczas przebywania w bezpiecznej witrynie bankowej. Tylko zaufane aplikacje mogą otwierać nowe połączenia. W praktyce wygląda to tak, że po uruchomieniu sesji ochrony bankowości wszystkie połączenia internetowe niezaufanych procesów są odcinane. Sprawdzane są również wszystkie połączenia zaufanych procesów. Jeśli zaufane procesy łączą się z niezaufanymi lub nieznanymi adresami IP, połączenia te są automatycznie blokowane. Ochrona bankowa pozwala nowym zaufanym procesom na komunikację z Internetem.

Możliwość blokowania niezaufanych połączeń zapobiega porwaniu sesji bankowych - pieniądze użytkownika są bezpieczne. Aplikacja zamyka Ochronę bankowości automatycznie po zakończeniu sesji bankowej przez użytkownika. Ochrona bankowości zostanie uruchomiona ponownie po wejściu na inną stronę bankową. Remote Access Protection for PC zapobiega wykorzystywaniu przez oszustów telefonicznych oprogramowania zdalnego dostępu do dokonywania kradzieży online

53. GEOLOKALIZACJA VPN

Program Bezpiecznie w Internecie jest wyposażony w zintegrowaną technologię VPN.

Firma F-Secure wykorzystuje technologię VPN w celu zwiększenia bezpieczeństwa i prywatności użytkowników. Ze względu na charakter technologii VPN zaszyfrowany tunel wychodzący z urządzenia klienta musi gdzieś wejść do publicznego Internetu. Firma F-Secure posiada już kilka geograficznie rozmieszczonych węzłów wyjściowych.

Kluczowe korzyści

- Oferowane jako usługa dla operatora
- Szybkie wdrożenie produkcji i wejście na rynek
- Brak integracji z infrastrukturą operatora
- Elastyczność dzięki węzłom VPN