F-Secure Internet Security 2014

Obsah

Kapitola
1

Instalace

Témata:

1.1 Než zahájíte první instalaci

Děkujeme, že jste si vybrali náš produkt.

K instalaci produktu potřebujete:

- Instalační disk CD nebo instalační balíček.
- Registrační klíč
- Připojení k Internetu

Pokud vlastníte produkt pro zabezpečení od jiného dodavatele, instalační program se ho automaticky pokusí odebrat. Pokud se tak nestane, odeberte ho ručně.

Poznámka: Pokud v počítači existuje více účtů, přihlaste se před instalací pomocí účtu s oprávněními správce.

1.2 První instalace produktu

Pokyny k instalaci produktu

Při instalaci produktu postupujte podle těchto pokynů:

1. Vložte do počítače disk CD-ROM nebo poklepejte na instalační program, který jste si stáhli.

   Pokud se disk CD-ROM nespustí automaticky, přejděte do Průzkumníka Windows, poklepejte na ikonu CD-ROM a spusťte instalaci poklepáním na instalační soubor.

2. Postupujte podle pokynů na obrazovce.

   - Pokud jste produkt zakoupili na CD v obchodě, registrační klíč najdete na obalu Stručného průvodce instalací.
   - Pokud jste produkt stáhli pomocí služby F-Secure eStore, registrační klíč se nachází v potvrzovacím e-mailu objednávky.

   Před ověřením registrace a stažením nejnovějších aktualizací z Internetu bude pravděpodobně nutné restartovat počítač. Pokud instalujete z disku CD-ROM, nezapomeňte před restartováním počítače vyjmout instalační disk.

1.3 Instalace a upgrade aplikací

Pokyny k aktivaci nové registrace

Při aktivaci nové registrace nebo instalaci nové aplikace pomocí hlavního panelu postupujte podle těchto pokynů:

> **Poznámka:** Ikonu hlavního panelu naleznete na hlavním panelu systému Windows.

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Zobrazit moje registrace**.
3. Pod položkou **Moje registrace** přejděte na stránku **Stav registrace** a klepněte na tlačítko **Aktivovat registraci**.
   Otevře se okno **Aktivovat registraci**.
4. Zadejte registrační klíč pro aplikaci a klepněte na tlačítko **OK**.
5. Po ověření a aktivaci registrace klepněte na tlačítko **Zavřít**.
6. Pod položkou **Moje registrace** přejděte na stránku **Stav instalace**. Pokud se instalace nespustí automaticky, postupujte podle těchto pokynů:
   a) Klepněte na tlačítko **Instalovat**.
      Otevře se okno instalace.
   b) Klepněte na tlačítko **Další**.
      Aplikace je stažena a začíná instalace.
   c) Po dokončení instalace klepněte na tlačítko **Zavřít**.

Nová registrace byla aktivována.

1.4 Nápověda a podpora

Přístup k nápovědě produktu online získáte klepnutím na ikonu nápovědy nebo stisknutím klávesy `F1` na kterékoli obrazovce produktu.

Kapitola
2

Začínáme

Témata:

Informace o tom, jak začít s produktem pracovat.

Tato část popisuje, jak lze prostřednictvím hlavního panelu změnit běžná nastavení a spravovat registrace. Nastavení hlavního panelu jsou platná pro všechny programy, které jsou na hlavním panelu nainstalovány.

Mezi společná nastavení hlavního panelu patří:

- Stahování, kde můžete vidět informace o stažených aktualizacích a ručně kontrolovat, zda jsou k dispozici nové aktualizace.
- Nastavení připojení, kde lze změnit způsob připojení počítače k Internetu.
- Oznámení, kde můžete vidět minulá oznámení a nastavit druh oznámení, která chcete zobrazit.
- Registrace pro programy, které jsou nainstalovány prostřednictvím hlavního panelu.

2.1 Kde mohu najít ID svého účtu?

Naše oddělení zákaznické podpory vás může požádat o ID účtu, pokud nás budete chtít kontaktovat.

Zobrazení identifikačních kódů účtu a zařízení:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Zobrazit moje registrace**.
3. Vyberte možnost **Identifikační kódy**.

Na stránce se zobrazují identifikační kódy účtu a aktuálního zařízení, které lze použít ke správě registrací.

2.2 Jak používat centrum akcí

V centru akcí se zobrazují veškerá důležitá upozornění, která vyžadují vaši pozornost.

Pokud jsou v centru akcí čekající akce, budou vám pravidelně připomínány.

2.2.1 Otevření centra akcí

Otevřete centrum akcí, aby se zobrazila všechna upozornění, která vyžadují vaši pozornost.

Postup otevření centra akcí:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Položka **Otevřít centrum akcí** v místní nabídce uvádí, kolik čekajících akcí máte.
2. Vyberte příkaz **Otevřít centrum akcí**.
   V centru akcí se zobrazí seznam všech položek, které je nutné vyřešit.
3. Klepnutím na položku v seznamu zobrazíte další informace, které se jí týkají.
4. Pokud nyní nechcete s nevyřešenou položkou dělat nic, klliknutím na tlačítko **Odložit** můžete položku vyřešit později.

   Poznámka: Pokud centrum akcí obsahuje více položek, kliknutím na tlačítko **Odložit vše** centrum akcí zavřete a budete moci všechny položky vyřešit později.

2.2.2 Instalace aktualizace produktu

Až bude k dispozici bezplatná aktualizace produktu, který jste nainstalovali, bude nutné ji nainstalovat, aby bylo možné začít používat novou verzi.

Postup aktualizace produktu:

1. Otevřete centrum akcí.
   Centrum akcí obsahuje položku **K dispozici je aktualizace produktu**. Pokud centrum akcí obsahuje více položek, kliknutím na položku ji otevřete.
2. Klepněte na tlačítko **Aktualizovat**.

   Poznámka: Aby bylo možné produkt aktualizovat, je třeba přijmout nové licenční podmínky, pokud se změnily.

Po dokončení aktualizace bude pravděpodobně nutné restartovat počítač.

2.2.3 Instalace nového produktu

Pokud byl k vaší registraci přidán nový produkt, můžete ho nainstalovat a začít používat.

Nové produkty je možné přidávat k registraci, dokud je platná.

Postup instalace nového produktu:

1. Otevřete centrum akcí.
   Centrum akcí obsahuje položku **Instalovat nový produkt**. Pokud centrum akcí obsahuje více položek, kliknutím na položku ji otevřete.
2. Klepněte na tlačítko **Instalovat**.

   Poznámka: Pokud produkt instalovat nechcete, klepnutím na ikonu koše v pravém horním rohu připomenutí zavřete a odstraňte je z centra akcí.

3. Při instalaci produktu postupujte podle pokynů v průvodci instalací.

Po dokončení instalace bude pravděpodobně nutné restartovat počítač.

2.2.4 Nahradit produkt s končící platností

Pokud vaší registraci končí platnost a aktuálně nainstalovaný produkt již není k dispozici, nemůžete pokračovat se svou registrací, ale můžete zdarma upgradovat na nový produkt.

Postup aktualizace produktu:

1. Otevřete centrum akcí.
   Centrum akcí obsahuje položku **Aktualizovat produkt**. Pokud centrum akcí obsahuje více položek, kliknutím na ně je otevřete.
2. Klepněte na tlačítko **Aktualizovat**.

Po dokončení aktualizace bude pravděpodobně nutné restartovat počítač.

2.3 Ověření platnosti předplatného

Typ a stav registrace se zobrazuje na stránce **Registrace**.

Když se blíží datum vypršení platnosti registrace nebo již platnost registrace vypršela, v odpovídající ikoně na hlavním panelu se změní celkový stav ochrany programu.

Kontrola platnosti předplatného:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Zobrazit moje registrace**.
3. Vyberte jednu z následujících možností.
   - Výběrem možnosti **Registrace** se zobrazí informace o vašich registracích pro nainstalované programy.
   - Výběrem možnosti **Instalace** můžete zobrazit, jaké programy jsou pro instalaci k dispozici.

Pokud vaše registrace vypršela, musíte ji obnovit, abyste mohli nadále přijímat aktualizace a používat produkt.

2.3.1 Aktivace registrace

Když vlastníte nový registrační klíč nebo kód kampaně pro produkt, musíte ho aktivovat.

Aktivace registrace:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Zobrazit moje registrace**.
3. Klepněte na možnost **Přidat novou registraci**.
4. V dialogovém okně, které se otevře, zadejte nový registrační klíč nebo kód kampaně a klepněte na tlačítko **OK**.

   Tip: Pokud jste obdrželi registrační klíč e-mailem, můžete ho zkopírovat z e-mailové zprávy a vložit ho do tohoto pole.

Po zadání nového registračního klíče se na stránce **Registrace** zobrazí datum platnosti nové registrace.

2.3.2 Obnovení registrace

Pokud se blíží vypršení registrace produktu, je třeba ji obnovit, chcete-li produkt nadále používat.

Postup obnovení registrace:

1. Otevřete centrum akcí.
   Centrum akcí obsahuje položku **Obnovit registraci**. Pokud centrum akcí obsahuje více položek, kliknutím na položku ji otevřete.
2. Obnovení registrace vyžaduje nový registrační klíč.
   - Pokud již máte k dispozici registraci, kterou můžete pro tento počítač použít, kliknutím na možnost **Aktivovat** začněte nové předplatné používat.
   - Pokud jste si již nový registrační klíč zakoupili, klikněte na možnost **Zadat klíč**.

     V dialogovém okně, které se otevře, zadejte nový registrační klíč a klepněte na tlačítko **OK**.
   - V opačném případě klepněte na tlačítko **Obnovit nyní**.

     Registraci můžete obnovit v našem online obchodě. Až registraci obnovíte, obdržíte nový registrační klíč.

Pokud registraci nechcete obnovit, odinstalujte produkt, jehož registrace vypršela.

2.4 Používání automatických aktualizací

Automatické aktualizace zajišťují neustálou ochranu počítače před nejnovějšími hrozbami.

Je-li počítač připojen k Internetu, produkt do něj automaticky stahuje nejnovější aktualizace. Zjišťuje síťové přenosy a neomezuje práci s Internetem ani u pomalého připojení.

2.4.1 Kontrola stavu aktualizace

Zobrazuje datum a čas poslední aktualizace.

Obvykle nemusíte sami kontrolovat aktualizace, protože produkt přijímá nejnovější aktualizace automaticky, když jste připojeni k Internetu a jsou zapnuty automatické aktualizace.

Ověření instalace nejnovějších aktualizací:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **Automatické aktualizaceStahování**.
4. Klepněte na položku **Ověřit nyní**.
   Produkt získává nejnovější aktualizace, pokud jsou k dispozici.

   Poznámka: Pokud chcete zkontrolovat dostupnost nejnovějších aktualizací, musíte mít aktivní připojení k internetu.

2.4.2 Změna nastavení připojení k Internetu

Obvykle není nutné měnit výchozí nastavení, můžete ale nakonfigurovat způsob připojení počítače k Internetu, abyste mohli přijímat aktualizace automaticky.

Změna nastavení připojení k Internetu:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **Automatické aktualizacePřipojení**.
4. V seznamu **Připojení k Internetu** vyberte způsob připojení počítače k Internetu.
   - Máte-li k dispozici nepřetržité síťové připojení, vyberte možnost **Předpokládat nepřetržité připojení**.

     Poznámka: Nemá-li počítač trvalé síťové připojení a je nastaveno vytáčení na vyžádání, výběr možnosti **Předpokládat nepřetržité připojení** může vést k opakovanému vytáčení.
   - Vybráním možnosti **Rozpoznat připojení** se budou aktualizace stahovat, pouze pokud produkt zjistí aktivní síťové připojení.
   - Vybráním možnosti **Rozpoznat přenos** se budou aktualizace stahovat, pouze pokud produkt zjistí jiný síťový přenos.

     Tip: Máte-li neobvyklou hardwarovu konfiguraci, která způsobuje, že nastavení **Rozpoznat připojení** zjistí aktivní přenos v síti, i když žádný přenos neprobíhá, změňte nastavení na možnost **Zjistit přenosy**.
5. V seznamu **Server proxy HTTP** vyberte, zda počítač používá připojení k internetu *server proxy*.
   - Je-li počítač připojen k internetu přímo, klepněte na přepínač **Bez serveru proxy HTTP**.

- Chcete-li nakonfigurovat nastavení *serveru proxy HTTP*, klepněte na přepínač **Ručně konfigurovat server HTTP proxy**.
- Chcete-li použít stejné nastavení *serveru proxy HTTP*, jaké jste nakonfigurovali ve webovém prohlížeči, vyberte možnost **Použít server proxy HTTP mého prohlížeče**.

2.5 Zobrazení činností produktu

Akce, které byly provedeny za účelem ochrany počítače, můžete vidět na stránce **Oznámení**.

Produkt zobrazí oznámení, pokud provede určitou akci, například za účelem ochrany souborů, které jsou uloženy v počítači. Některá oznámení může zasílat také poskytovatel služby, například aby vás informoval o nových službách, které jsou k dispozici.

2.5.1 Zobrazení historie oznámení

Oznámení, která byla zobrazena, můžete vidět v historii oznámení.

Zobrazení historie oznámení:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **JinéOznámení**.
4. Klepněte na položku **Zobrazit historii oznámení**.
   Zobrazí se seznam historie oznámení.

2.5.2 Změna nastavení oznámení

Můžete si vybrat typ oznámení, která má produkt zobrazovat.

Změna nastavení oznámení:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **JinéOznámení**.
4. Výběrem nebo zrušením výběru možnosti **Povolit zprávy programu** zapnete nebo vypnete zprávy programu.

   Po zapnutí tohoto nastavení bude produkt zobrazovat oznámení z nainstalovaných programů.
5. Výběrem nebo zrušením výběru možnosti **Povolit reklamní zprávy** zapnete nebo vypnete reklamní zprávy.
6. Klepněte na tlačítko **OK**.

2.6 Režim hraní her

Zapnutím režimu hraní her můžete optimalizovat využití prostředků počítače produktem.

Počítačové hry často vyžadují pro plynulý chod mnoho prostředků systému. Ostatní aplikace spuštěné na pozadí mohou snížit výkonnost her tím, že způsobují špičky ve spotřebě CPU a aktivitě sítě.

Režim hraní her uvolní větší část systémových prostředků pro účely her, které běží v počítači tím, že sníží dopad produktu na spotřebu CPU počítače a sítě, přičemž zachová základní funkce produktu. Například automatické aktualizace a jiné operace, které mohou způsobit vysokou spotřebu výkonu CPU a sítě, budou po dobu zapnutí režimu hraní her pozastaveny.

Navíc se po dobu zapnutí režimu hraní her nebudou zobrazovat překryvná okna oznámení ani centra akcí. Kritická oznámení se zobrazí, pokud budou vyžadovat okamžitou pozornost nebo interakci, ale ostatní oznámení se zobrazí až povypnutí režimu hraní her. Totéž platí pro všechny ostatní celoobrazovkové aplikace, například když sledujete prezentaci nebo video v režimu celé obrazovky, i když je režim hraní her vypnutý.

2.6.1 Zapnutí režimu hraní her

Zapnutím režimu hraní her zlepšíte výkon her v počítači.

Zapnutí režimu hraní her:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte možnost **Režim hraní her**.
   Využití systémových prostředků produktem je nyní optimalizováno, aby mohly hry v počítači běžet plynule.

Režim hraní her se automaticky vypne, když restartujete počítač nebo když počítač přejde zpět z režimu spánku.

Kapitola
3

Síť ochrany v reálném čase

Témata:

Tento dokument popisuje Síť ochrany v reálném čase, online službu společnosti F-Secure Corporation, která identifikuje čisté aplikace a webové stránky a poskytuje ochranu před škodlivým softwarem a prostředky zneužití webových stránek.

3.1 Co je Síť ochrany v reálném čase

Síť ochrany v reálném čase je online služba, která poskytuje rychlou odpověď proti internetovým hrozbám.

Jako přispěvatel umožňujete Síti ochrany v reálném čase shromažďovat data, která nám pomáhají zintenzivňovat vaši ochranu proti novým a hrozícím nebezpečím. Síť ochrany v reálném čase shromažďuje informace o určitých neznámých, škodlivých nebo podezřelých aplikacích a neklasifikovaných webových stránkách. Tyto informace jsou anonymní a odesílají se společnosti F-Secure Corporation ke kombinované analýze dat. Analyzované informace používáme ke zlepšení vaší ochrany proti nejnovějším hrozbám a škodlivým souborům.

Jak funguje Síť pro ochranu v reálném čase

Síť ochrany v reálném čase shromažďuje informace o neznámých aplikacích a webových stránkách a o škodlivých aplikacích a zneužitích na webových stránkách. Síť ochrany v reálném čase nesleduje vaši webovou aktivitu, neshromažďuje informace o webových stránkách, které již byly analyzovány ani o čistých aplikacích, které jsou nainstalovány na vašem počítači.

Pokud nechcete tato data poskytovat, Síť ochrany v reálném čase údaje o instalovaných aplikacích ani navštívených webových stránkách shromažďovat nebude. Avšak produkt se musí dotazovat serverů F-Secure na pověst aplikací, webových stránek, sdělení a dalších objektů. Dotazy se přenášejí pomocí kryptografického kontrolního součtu, přičemž dotazovaný objekt sám se F-Secure nezasílá. Nesledujeme data podle uživatele, pouze se zvyšuje hodnota počítadla vstupu do souboru nebo na webovou stránku.

Není možné kompletně zastavit veškerou síťovou komunikaci se Sítí ochrany v reálném čase, protože se jedná o nedílnou součást ochrany poskytované produktem.

3.1.1 Kontrola stavu sítě ochrany v reálném čase

Na připojení sítě ochrany v reálném čase závisí správná funkce mnoha funkcí produktu.

Jestliže dochází k problémům se sítí nebo pokud brána firewall blokuje přenos sítě ochrany v reálném čase, bude stav Odpojeno. Pokud nejsou nainstalovány žádné funkce produktu, které by vyžadovaly přístup k síti ochrany v reálném čase, bude stav Nepoužíváno.

Kontrola stavu:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **Automatické aktualizacePřipojení**.

V části **Síť ochrany v reálném čase** se zobrazí aktuální stav sítě ochrany v reálném čase.

3.2 Výhody Sítě ochrany v reálném čase

Se Sítí ochrany v reálném čase získáte rychlejší a přesnější ochranu proti nejnovějším hrozbám a nebudete dostávat zbytečná upozornění na podezřelé aplikace, které nejsou škodlivé.

Jako přispěvatel do Sítě ochrany v reálném čase nám můžete pomoci najít nový a zatím nezjištěný škodlivý software a odstranit možná falešně pozitivní hodnocení.

Všichni účastníci Sítě ochrany v reálném čase si vzájemně pomáhají. Když najde Síť ochrany v reálném čase podezřelou aplikaci, z výsledku analýzy máte užitek stejně, jako kdyby stejnou aplikaci nalezl někdo jiný. Síť ochrany v reálném čase zlepšuje celkový výkon, protože nainstalovaný bezpečnostní produkt již nemusí skenovat aplikace, které byly analyzovány Sítí ochrany v reálném čase a shledány bezpečnými. Podobně se v Síti ochrany v reálném čase šíří také informace o škodlivých webových stránkách a nevyžádaných hromadných sděleních, a proto vám můžeme poskytovat přesnější ochranu před zneužitím webových stránek a nevyžádanými zprávami.

Čím více lidí bude do Sítě ochrany v reálném čase přispívat, tím lépe budou jednotliví účastníci chráněni.

3.3 Jakými daty přispíváte

Jako přispěvatel povolujete Síti ochrany v reálném čase shromažďovat informace o aplikacích, které jste si nainstalovali a o webových stránkách, které navštěvujete, aby Síť ochrany v reálném čase mohla poskytovat lepší ochranu proti nejnovějším škodlivým aplikacím a podezřelým webovým stránkám.

Analýza pověsti souboru

Síť ochrany v reálném čase shromažďuje pouze informace o aplikacích, jejichž pověst není známa a o souborech, které jsou podezřelé nebo se o nich ví, že jsou škodlivé.

Shromažďují se pouze informace o souborech aplikací (spustitelných souborech), nikoli o jiných typech souborů.

V závislosti na produktu mohou shromažďované informace zahrnovat:

- cestu k souboru aplikace (bez jakýchkoli údajů, podle nichž by bylo možné uživatele identifikovat),
- velikost souboru a dobu jeho vytvoření nebo změny,
- atributy a oprávnění souboru,
- informace o podpisu souboru,
- aktuální verzi souboru a společnost, která jej vytvořila,
- původ souboru nebo jeho adresu URL pro stahování (bez jakýchkoli údajů, podle nichž by bylo možné uživatele identifikovat),
- výsledky analýzy aplikace F-Secure DeepGuard a antivirového programu kontrolovaných souborů a
- další podobné informace.

Síť ochrany v reálném čase nikdy neshromažďuje údaje z vašich osobních dokumentů, pokud nejsou infikovány. U všech typů nebezpečných souborů shromažďuje názvy infekcí a stav dezinfekce souborů.

Odeslání souborů k analýze

U některých produktů můžete také odesílat podezřelé aplikace do Sítě ochrany v reálném čase k analýze.

Jednotlivé podezřelé aplikace lze k analýze odeslat ručně, pokud vás k tomu produkt vyzve, nebo můžete zapnout automatické odeslání podezřelých aplikací k analýze v nastavení produktu. Služba Real-time Protection Network nikdy neodesílá informace o vašich osobních dokumentech.

Analýza pověsti webové stránky

Síť ochrany v reálném čase nesleduje vaši webovou aktivitu. Kontroluje při vašem procházení, zda jsou navštěvované webové stránky bezpečné. Když navštívíte webovou stránku, Síť ochrany v reálném čase zkontroluje její bezpečnost a informuje vás o tom, zda je tato stránka vyhodnocena jako podezřelá nebo škodlivá.

Za účelem zlepšení služby a zachování vysoké přesnosti hodnocení může Síť ochrany v reálném čase shromažďovat informace o navštěvovaných webových stránkách. Tyto informace se shromažďují v případě, kdy vámi navštívená stránka obsahuje škodlivý nebo podezřelý obsah nebo známé zneužití, případně tehdy, pokud obsah na stránce zatím nebyl hodnocen nebo kategorizován. Shromážděné informace zahrnují URL a metadata související s návštěvou a s webovou stránkou.

Síť ochrany v reálném čase obsahuje přísné kontroly, které zajišťují, že nebude docházet k odesílání žádných soukromých údajů. Počet shromážděných adres URL je omezen. Všechny odeslané údaje jsou před odesláním filtrovány a ty položky, které by mohly obsahovat informace, které by mohly být s vámi spojovány a mohli byste být na jejich základě identifikováni, jsou odstraněny. Síť ochrany v reálném čase nehodnotí ani neanalyzuje webové stránky na soukromých sítích a nikdy neshromažďuje informace o privátních síťových adresách nebo aliasech.

Analýza systémových informací

Síť ochrany v reálném čase zaznamenává informace o názvu a verzi vašeho operačního systému, o internetovém připojení a o statistikách využívání sítě pro ochranu v reálném čase (například počet dotazů na pověst webové stránky a průměrná doba vrácení výsledku dotazu), abychom mohli službu neustále monitorovat a vylepšovat.

3.4 Jak chráníme vaše soukromí

Všechny informace přenášíme bezpečně a automaticky odstraňujeme veškeré osobní informace, které by mohly být v datech obsaženy.

Shromážděné informace se nezpracovávají individuálně; spojují se s informacemi od ostatních přispěvatelů v sítích ochrany v reálném čase. Veškerá data jsou analyzována statisticky a anonymně, což znamená, že žádná data s vámi nebudou žádným způsobem spojována.

Žádné informace, které by vás mohly identifikovat, se ve shromážděných datech nenacházejí. Síť ochrany v reálném čase neshromažďuje adresy IP ani žádné jiné soukromé informace, jako jsou e-mailové adresy, uživatelská jména a hesla. Ačkoli se snažíme ze získaných informací odstranit veškerá data, která by vás mohla identifikovat, je možné, že zde i přes tuto snahu některá z těchto dat zůstanou. V takových případech nebudeme takto neúmyslně shromážděná data používat k vaší identifikaci.

Uplatňujeme přísná bezpečnostní opatření a fyzické, administrativní a technické ochranné prostředky, abychom ochránili shromážděné informace při přenosu, ukládání a zpracování. Informace se uchovávají v zabezpečených úložištích a na serverech, nad nimiž máme kontrolu a které jsou umístěny buď v našich kancelářích nebo v kancelářích našich subdodavatelů. Ke shromážděným informacím má přístup pouze autorizovaný personál.

F-Secure může shromážděná data sdílet se svými pobočkami, subdodavateli, distributory a partnery, ale pouze v anonymním formátu, aby nemohla sloužit k identifikaci.

3.5 Jak se stát přispěvatelem Sítě ochrany v reálném čase

Můžete nám pomoci vylepšovat provoz Sítě ochrany v reálném čase tak, že budete přispívat informacemi o škodlivých programech a webových stránkách.

Během instalace se můžete rozhodnout, zda se stanete přispěvatelem Sítě ochrany v reálném čase. Přednastaveno je, že se přispěvatelem stanete a budete do Sítě ochrany v reálném čase přispívat svými informacemi. Toto nastavení můžete kdykoliv později změnit.

Chcete-li změnit nastavení Sítě ochrany v reálném čase, postupujte podle následujících pokynů:

1. Přejděte na hlavní panel a klepněte pravým tlačítkem na ikonu zcela vpravo.
   Zobrazí se místní nabídka.
2. Vyberte příkaz **Otevřít společná nastavení**.
3. Klepněte na položku **JinéOchrana osobních dat**.
4. Zatrhněte políčko účastníka a stanete se přispěvatelem Sítě ochrany v reálném čase.

3.6 Dotazy týkající se Sítě ochrany v reálném čase

Kontaktní informace pro jakékoli dotazy týkající se Sítě ochrany v reálném čase.

Máte-li jakékoli dotazy týkající se Sítě ochrany v reálném čase, obraťte se prosím na následující kontakty:

F-Secure Corporation
Tammasaarenkatu 7
PL 24
00181 Helsinki
Finsko
http://www.f-secure.com/en/web/home_global/support/contact

Nejnovější verze těchto zásad je vždy k dispozici na našem webu.

Kapitola
4

Ochrana počítače proti malwaru

Témata:

Kontrola přítomnosti virů a spywaru chrání počítač proti programům, které mohou ukrást osobní údaje, poškodit počítač nebo ho použít k nezákonným účelům.

Program standardně ošetří všechny typy malwaru bezprostředně poté, co jsou nalezeny, takže nemohou nijak uškodit.

Ve výchozím nastavení produkt automaticky kontroluje místní pevné disky, veškerá vyměnitelná média (jako jsou přenosné jednotky nebo kompaktní disky) a stažený obsah.

Produkt lze nastavit tak, aby automaticky kontroloval také e-maily.

Kontrola virů a spywaru také sleduje jakékoliv změny ve vašem počítači indikující *malware*. Pokud jsou nalezeny jakékoliv nebezpečné změny systému (například systémového nastavení nebo pokusy o změnu důležitých systémových procesů), služba DeepGuard zastaví činnost programu jako by to byl *malware*.

4.1 Úvod

Tento produkt chrání váš počítač před viry a dalšími škodlivými aplikacemi.

Tento produkt prověřuje soubory, analyzuje aplikace a provádí automatické aktualizace. Nevyžaduje žádné zásahy uživatele.

4.1.1 Zobrazení celkového stavu ochrany

Na stránce **Stav** je zobrazen celkový stav produktu.

Stránka Stav se otevře, když spustíte produkt. Pokud funkce zabezpečení není aktuální, na stránce se zobrazí návrh řešení tohoto problému. Také se na ní zobrazí čas poslední úspěšné kontroly aktualizací.

Následující ikony udávají stav programu a jeho funkcí zabezpečení.

Ikona stavu	Název stavu	Popis
	OK	Počítač je chráněn. Funkce jsou zapnuty a pracují správně.
	Informace	Produkt vás informuje o zvláštním stavu. Všechny funkce pracují správně, ale produkt například stahuje aktualizace.
	Varování	Váš počítač není plně chráněn. Produkt vyžaduje váš zásah, například již dlouho nepřijal žádné aktualizace.
	Chyba	Váš počítač není chráněn. Například vaše registrace vypršela nebo je vypnuta důležitá funkce.
	Vypnuto	Nekritická funkce je vypnutá.

4.1.2 Zobrazení statistiky produktu

Akce, které produkt od své instalace provedl, jsou uvedeny na stránce **Statistika**.

Zobrazení stránky **Statistika**:

Klikněte na tlačítko **Statistika**.

Na stránce **Statistika** se zobrazí:

- **Kontrola virů a spywaru** zobrazuje kolik souborů produkt od své instalace kontroloval a vyčistil.
- Položka **Aplikace** zobrazuje počet programů, které aplikace DeepGuard od své instalace povolila nebo zablokovala.

4.1.3 Práce s aktualizacemi produktu

Produkt ochranu aktualizuje automaticky.

Zobrazení verzí databází

Časy posledních aktualizací a čísla verzí lze zobrazit na stránce **Verze databáze**.

Otevření stránky **Verze databáze**:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte položky **Jiná nastaveníVerze databáze**.

Na stránce **Verze databáze** je uvedeno datum poslední aktualizace definic virů a spywaru, nástroje DeepGuard a filtrování nevyžádané pošty a phishingu a čísla jejich verzí.

Změna nastavení mobilního širokopásmového připojení

Vyberte, zda chcete stahovat aktualizace zabezpečení, pokud používáte mobilní širokopásmové připojení.

Poznámka: Tato funkce je k dispozici pouze v operačním systému Microsoft Windows 7 a novějších verzích systému Windows.

Standardně jsou aktualizace zabezpečení stahovány vždy v síti domácího operátora. Pokud ale navštívíte síť jiného operátora, aktualizace budou pozastaveny. Důvodem je možnost odlišných cen připojení u různých operátorů, například v různých zemích. Toto nastavení můžete ponechat během své návštěvy beze změny, chcete-li ušetřit šířku pásma a případně i náklady.

Poznámka: Toto nastavení platí pouze pro mobilní širokopásmové připojení. Pokud je počítač připojen k pevné či bezdrátové síti, produkt je automaticky aktualizován.

Chcete-li změnit nastavení:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte položky **Jiná nastaveníMobilní širokopásmovéStáhnout bezpečnostní aktualizace**.
3. Vyberte preferovanou možnost aktualizací pro mobilní připojení:

   - **Pouze v síti mého domovského operátora**

     Aktualizace jsou vždy stahovány v síti domácího operátora. Pokud navštívíte síť jiného operátora, aktualizace budou pozastaveny. Doporučujeme, abyste zvolili tuto možnost, pokud chcete zajistit, aby byl produkt zabezpečení stále aktualizován s očekávanými náklady.
   - **Nikdy**

     Aktualizace nebudou staženy, pokud používáte mobilní širokopásmové připojení.
   - **Vždy**

     Aktualizace jsou stahovány vždy v jakékoliv síti. Vyberte tuto možnost pokud jste si jisti, že chcete mít vždy aktuální zabezpečení počítače bez ohledu na náklady.

4. Chcete-li se samostatně rozhodnout vždy, když opouštíte domácí síť operátora, vyberte možnost **Zobrazit dotaz vždy při opuštění domácí sítě operátora**.

Pozastavené aktualizace zabezpečení

Aktualizace zabezpečení mohou být pozastaveny, pokud použijete mobilní širokopásmové připojení mimo domácí síť vašeho operátora.

V takovém případě se v pravém dolním rohu obrazovky zobrazí oznámení **Pozastaveno**. Aktualizace jsou pozastaveny, protože ceny připojení u různých operátorů, například v různých zemích, se mohou lišit. Toto nastavení můžete ponechat během své návštěvy beze změny, chcete-li ušetřit šířku pásma a případně i náklady. Pokud však chcete nastavení změnit, klepněte na odkaz **Změnit**.

Poznámka: Tato funkce je k dispozici pouze v operačním systému Microsoft Windows 7 a novějších verzích systému Windows.

4.1.4 Co jsou viry a další malware?

Malware jsou programy navržené speciálně za účelem poškození počítače, jeho zneužití k nezákonným aktivitám bez vědomí uživatele nebo krádeže informací z počítače.

Malware může:

- získat kontrolu nad prohlížečem,
- přesměrovat pokusy o vyhledávání,
- zobrazovat nežádoucí reklamy,
- sledovat navštívené weby,
- krást osobní údaje, například bankovní,
- použít počítač k rozesílání nevyžádané pošty,
- použít počítač k útoku na jiné počítače.

Malware také může vést k nestabilitě a snížení výkonu počítače. Pokud je počítač náhle velmi pomalý a často dochází k haváriím, je pravděpodobné, že se v něm nachází *malware*.

Viry

Vir je obvykle program, který se připojí k souborům a dále se síří. Může měnit a přesunovat obsah jiných souborů, a tím poškodit počítač.

Vir je program, který se do počítače obvykle nainstaluje bez vědomí uživatele. Poté se vir snaží dále rozšířit. Viry:

- využívají část systémových prostředků,
- mohou měnit nebo poškodit soubory v počítači,
- pravděpodobně se pokusí nakazit další počítače,
- mohou umožnit zneužití počítače k nezákonným účelům.

Spyware

Spyware jsou programy, které získávají osobní informace uživatelů.

Spyware může shromažďovat například následující osobní údaje:

- navštívené internetové servery,
- e-mailové adresy uložené v počítači,
- hesla,
- čísla platebních karet.

Spyware se téměř vždy instaluje bez výslovného souhlasu uživatele. Spyware může být nainstalován spolu s užitečným programem, nebo když podvodně přiměje ke klepnutí na volbu v zavádějícím překryvném okně.

Rootkity

Rootkity jsou programy znesnadňující nalezení *malwaru*.

Rootkity skrývají soubory a procesy, obecně proto aby skryly škodlivé aktivity v počítači. Když rootkit skrývá *malware*, je těžké jej v počítači odhalit.

Tento produkt obsahuje speciální kontrolu přítomnosti rootkitů, *malware* se tedy nemůže skrývat.

Riskware

Riskware není navržen výslovně pro poškození počítače, může ho však ohrozit v případě zneužití.

Riskware není přesně totéž co malware. Programy označené jako riskware provádějí některé užitečné, avšak potenciálně nebezpečné funkce.

Příklady riskwaru mohou být následující:

- programy rychlého zasílání zpráv, například IRC (Internet relay chat),
- programy pro přenos souborů z jednoho počítače do druhého prostřednictvím Internetu,
- programy pro telefonování prostřednictvím Internetu, např. protokol VoIP (*Voice Over Internet Protocol*).
- software pro vzdálený přístup, například VNC,
- scareware, který může jednotlivce hrozbou nebo podvodem přimět k nákupu falešného bezpečnostního softwaru nebo
- software navržený k obejití kontrol CD nebo ochran proti kopírování.

Pokud jste program nainstalovali sami a správně nastavili, snižuje se pravděpodobnost, že bude v počítači škodit.

Pokud byl riskware nainstalován bez vašeho vědomí, byl pravděpodobně nainstalován se škodlivými úmysly a měl by být odstraněn.

4.2 Kontrola počítače

Pokud je zapnuta funkce hledání virů a spywaru, počítač bude automaticky zkontrolován na škodlivé soubory. Nebo můžete soubory zkontrolovat ručně a nastavit naplánované kontroly.

Doporučujeme nechat funkci hledání virů a spywaru vždy zapnutou. Soubory zkontrolujte ručně, chcete-li se ujistit, že se v počítači nenachází žádné škodlivé soubory, nebo pokud chcete zkontrolovat soubory, které jste vyloučili z kontroly v reálném čase.

Při nastavení naplánované kontroly budou při hledání virů a spywaru odstraněny z počítače škodlivé soubory v každém zadaném čase.

4.2.1 Automatická kontrola souborů

Kontrola v reálném čase chrání počítač tím, že při přístupu kontroluje všechny soubory a blokuje přístup k souborům obsahujícím *malware*.

Když se počítač pokouší o přístup k souboru, kontrola v reálném čase nejprve zjistí, zda soubor neobsahuje malware, teprve pak počítači povolí přístup.

Pokud kontrola v reálném čase zjistí škodlivý obsah, umístí soubor do karantény dříve, než by mohl způsobit škodu.

Má kontrola v reálném čase vliv na výkon počítače?

Obvykle si kontroly nevšimnete, protože trvá krátce a nevyužívá mnoho systémových prostředků. Množství času a systémových prostředků využité kontrolou v reálném čase závisí například na obsahu, umístění a typu souboru.

Soubory, jejichž kontrola trvá déle:

- Soubory na vyměnitelných médiích, jako jsou disky CD a DVD a přenosné jednotky USB.
- Komprimované soubory, například soubory *ZIP*.

> **Poznámka:** Komprimované soubory nejsou ve výchozím nastavení kontrolovány.

Kontrola v reálném čase může počítač zpomalit v následujících případech:

- máte počítač, který nesplňuje systémové požadavky, nebo
- přistupujete současně k velkému množství souborů; například při otevření adresáře, který obsahuje mnoho souborů, které je třeba zkontrolovat.

Zapnutí nebo vypnutí kontroly v reálném čase

Ponechte funkci kontroly v reálném čase zapnutou, aby mohla zabránit *malwaru* v poškození počítače.

Zapnutí nebo vypnutí kontroly v reálném čase:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   > **Poznámka:** Změna těchto nastavení vyžaduje oprávnění správce.

2. Zapněte nebo vypněte **kontrolu virů a spywaru**.
3. Klepněte na položku **Zavřít**.

Automatické řešení škodlivých souborů

Kontrola v reálném čase může vyřešit škodlivé soubory automaticky bez jakýchkoli otázek.

Povolení automatického řešení škodlivých souborů při kontrole v reálném čase:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Vyberte možnost **Automaticky vyřešit škodlivé soubory**.

Pokud vyberete, že se škodlivé soubory nemají řešit automaticky, kontrola v reálném čase se vás zeptá, co chcete při zjištění škodlivého souboru dělat.

Řešení spywaru

Hledání virů a spywaru blokuje spyware ihned, když se pokusí o spuštění.

Než se spywarová aplikace spustí, produkt ji zablokuje a umožní vám rozhodnout se, co chcete udělat.

Vyberte jednu z následujících akcí při zjištění spywaru:

Zvolená akce	Akce provedená se spywarem
Zpracovat automaticky	Nechte produkt rozhodnout, jaká je nejvhodnější akce pro zjištěný spyware.
Uložit položku do karantény	Přesuňte spyware do karantény, kde nemůže počítač poškodit.
Odstranit spyware	Odstraňte z počítače všechny spywarové soubory.
Blokovat pouze spyware	Zablokujte přístup ke spywaru, ale ponechte jej v počítači.
Vyloučit spyware z kontroly	Umožňuje spuštění spywaru a jeho vyloučení z kontrol v budoucnu.

Řešení riskwaru

Hledání virů a spywaru blokuje riskware ihned, když se pokusí o spuštění.

Než se riskwarová aplikace spustí, produkt ji zablokuje a umožní vám rozhodnout se, co chcete udělat.

Vyberte jednu z následujících akcí při zjištění riskwaru:

Zvolená akce	Akce provedená s riskwarem
Blokovat pouze riskware	Zablokujte přístup k riskwaru, ale ponechte jej v počítači.
Uložit riskware do karantény	Přesuňte riskware do karantény, kde nemůže počítač poškodit.
Odstranit riskware	Odstraňte z počítače všechny riskwarové soubory.
Vyloučit riskware z kontroly	Umožňuje spuštění riskwaru a jeho vyloučení z kontrol v budoucnu.

Automatické odstranění stopovacích souborů cookie

Odstraněním stopovacích souborů cookie zabráníte webovým stránkám sledovat stránky, které na internetu navštívíte.

Stopovací soubory cookie jsou malé soubory, které umožňují webovým stránkám zaznamenávat webové stránky, které navštívíte. Podle těchto pokynů vypněte stopovací soubory cookie v počítači.

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Vyberte možnost **Odstranit stopovací soubory cookie**.
4. Klepněte na tlačítko **OK**.

4.2.2 Ruční kontrola souborů

Soubory lze zkontrolovat ručně, například pokud chcete k počítači připojit externí zařízení, abyste se ujistili, že neobsahují malware.

Spuštění ruční kontroly

Můžete zkontrolovat celý počítač, přítomnost konkrétního typu *malwaru* nebo konkrétní umístění.

Pokud máte podezření na výskyt konkrétního typu *malwaru*, můžete zkontrolovat pouze přítomnost tohoto typu. Máte-li podezření na konkrétní umístění, můžete zkontrolovat pouze tuto část počítače. Tyto kontroly budou provedeny mnohem rychleji než kontrola celého počítače.

Spuštění ruční kontroly počítače:

Poznámka: Chcete-li rychle zkontrolovat počítač, klikněte na položku **Kontrolovat** na stránce Stav.

1. Na stránce Nástroje klikněte na šipku vedle položky **Rozšířená kontrola**.
   Zobrazí se možnosti kontroly.
2. Vyberte typ kontroly.
   Výběrem možnosti **Změnit nastavení kontroly** optimalizujte ruční kontrolu počítače pro hledání virů a dalších škodlivých aplikací.
3. Poku vyberete možnost **Vybrat položku ke kontrole**, zobrazí se okno, ve kterém můžete vybrat umístění, které se bude kontrolovat.
   Otevře se **Průvodce kontrolou**.

Typy kontroly

Můžete zkontrolovat celý počítač, přítomnost konkrétního typu malwaru nebo konkrétní umístění.

Následuje seznam různých typů kontroly:

Typ kontroly	Co je kontrolováno?	Kdy použít tento typ?
Kontrola přítomnosti virů a spywaru	Části počítače, zda neobsahují viry, spyware nebo riskware.	Tento typ kontroly je daleko rychlejší než úplná kontrola. Prohledává pouze části systému, které obsahují soubory instalovaných programů. Tento typ kontroly se doporučuje, pokud chcete rychle zkontrolovat, zda je počítač čistý, protože umožňuje efektivně najít a odstranit jakýkoliv aktivní malware z vašeho počítače.
Kontrola celého počítače	Celý počítač (interní i externí pevné disky), zda neobsahuje viry, spyware nebo riskware.	Pokud si chcete být zcela jistí, že se v počítači nenachází malware ani riskware. Tento typ kontroly zabírá nejvíce času. Kombinuje rychlou kontrolu malwaru a kontrolu pevného disku. Rovněž kontroluje položky, které by mohly být skryté rootkitem.
Vyberte položky, které se mají kontrolovat	Určitý soubor, složka nebo jednotka, zda neobsahuje viry, spyware nebo riskware.	Máte-li podezření, že se malware nachází v určité části počítače, například se zde nachází soubory stažené z potencionálně nebezpečných zdrojů, jako jsou sítě P2P (peer-to-peer). Časová náročnost kontroly bude záviset na velikosti cíle, který kontrolujete. Kontrola proběhne rychle, pokud například kontrolujte složku, která obsahuje pouze malé množství menších souborů.

Kontrola v programu Průzkumník Windows

V Průzkumníkovi Windows lze zkontrolovat, zda disk, složka nebo soubor neobsahuje *virů*, *spywaru* a *riskwaru*.

Kontrola disku, složky nebo souboru:

1. Umístěte ukazatel myši na disk, složku nebo soubor, který chcete zkontrolovat, a klepněte na něj pravým tlačítkem.
2. V nabídce zobrazené pravým klepnutím vyberte příkaz **Zkontrolovat přítomnost virů ve složkách**. (Název příkazu závisí na tom, zda je zvolena kontrola disku, složky nebo souboru.) Otevře se okno **Průvodce kontrolou** a spustí se kontrola.

Pokud je nalezen *vir* nebo *spyware*, **Průvodce kontrolou** vás provede procesem odstranění viru.

Výběr souborů ke kontrole

Vyberte typy souborů, v nichž chcete kontrolovat přítomnost *virů* a *spywaru* při ručních a plánovaných kontrolách.

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte položky **Jiná nastaveníRuční kontrola**.
3. Pod položkou **Možnosti kontroly** zvolte jedno z následujících nastavení:

Zkontrolovat pouze známé typy souborů	Chcete-li zkontrolovat pouze typy souborů, u nichž je nejvyšší pravděpodobnost infekce, například spustitelné soubory. Výběrem této možnosti rovněž zrychlíte kontrolu. Kontrolují se soubory s následujícími příponami: `ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, htm, html, htt, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, td0, vbe, vbs, vxd, wbk, wma, wmv, wmf, wsc, wsf, wsh, wri, xls, xlt, xml, zip, jar, arj, lzh, tar, tgz, gz, cab, rar, bz2, hqx`.
Zkontroloval obsah komprimovaných souborů	Kontrola archivovaných souborů a složek.
Použít pokročilo heuristiku	Použití veškeré dostupné heuristiky během kontroly pro lepší nalezení nového nebo neznámého malwaru. **Poznámka:** Vyberete-li tuto možnost, kontrola trvá déle a může vést k více falešným pozitivním výsledkům (neškodné soubory jsou nahlášeny jako podezřelé).

4. Klepněte na tlačítko **OK**.

Poznámka: Vyloučené soubory v seznamech vyloučených položek nebudou zkontrolovány, ani když zde vyberete, aby zkontrolovány byly.

Co dělat při zjištění škodlivých souborů

Vyberte, jak chcete naložit se zjištěnými škodlivými soubory.

Chcete-li vybrat akci, která má být provedena při zjištění škodlivého obsahu během ručního prověřování:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte položky **Jiná nastaveníRuční kontrola**.
3. V dialogu **Při zjištění virů nebo spywaru** vyberte jednu z následujících možností:

Možnost	Popis
Vždy se dotázat (výchozí)	Můžete vybrat akci, která má být provedena, pro všechny položky zjištěné během ručního prověřování.
Vyléčit soubory	Produkt se pokusí o automatické vyléčení nakažených souborů nalezených při ruční kontrole. **Poznámka:** Pokud produkt nemůže nakažený soubor vyléčit, bude uložen do karantény (kromě případů, kdy se soubor nachází v síti nebo na vyměnitelném disku),aby nemohl počítač poškodit.
Umístit soubory do karantény	Produkt přesune všechny škodlivé soubory nalezené během ruční kontroly do karantény, v níž nemohou počítač poškodit.
Odstranit soubory	Produkt odstraní všechny škodlivé soubory nalezené během ručního prověřování.
Pouze ohlásit	Produkt ponechá beze změny všechny škodlivé soubory, které byly nalezeny během ručního prověřování, protože zaznamenávají výsledky ve zprávě z kontroly. **Poznámka:** Pokud vyberete tuto možnost a kontrola v reálném čase je vypnutá, případný malware může poškodit počítač.

Poznámka: Při zjištění škodlivých souborů během naplánované kontroly budou automaticky vyléčeny.

Plánování kontroly

Nastavte v počítači automatické hledání a odstranění virů a dalších škodlivých aplikací, i když jej nepoužíváte, nebo nastavte pravidelné hledání, abyste zajistili, že počítač bude chráněn.

Postup plánování kontroly:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte položky **Jiná nastaveníPlánovaná kontrola**.
3. Zapněte možnost **Naplánovaná kontrola**.
4. Vyberte, kdy se má hledání spustit.

Možnost	Popis
Denně	Hledání se bude opakovat každý den.
Týdně	Počítač bude prověřován ve vybrané dny v týdnu. Vybetre dny ze seznamu.
Měsíčně	Počítač bude prověřován ve vybrané dny v měsíci. Chcete-li vybrat dny: 1. Vyberte jednu z možností **Den**. 2. Den v měsíci vyberte v seznamu vedle vybraného dne.

5. Vyberte kdy chcete spustit kontrolu vybraných dnů.

Možnost	Popis
Čas spuštění	Hledání se spustí ve vybraný čas.
Po nečinnosti počítače po dobu	Hledání se spustí po určité době nečinnosti počítače.

Naplánovaná kontrola používá nastavení ručního prověřování při kontrole počítače, ale vždy prověřuje také archivy a automaticky čistí škodlivé soubory.

4.2.3 Kontrola e-mailů

Kontrola e-mailů vás chrání před škodlivými e-maily, které jsou vám zaslány.

Hledání virů a spywaru musí být zapnuto, aby byly e-maily prověřovány na viry.

Postup zapnutí kontroly e-mailu:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Vyberte možnost **Odstranit škodlivé e-mailové přílohy**.
4. Klepněte na tlačítko **OK**.

Kdy jsou e-mailové zprávy a přílohy kontrolovány?

Kontrola virů a spywaru může odstranit nebezpečný obsah z e-mailů, které přijímáte.

Kontrola virů a spywaru odstraňuje nebezpečné e-mailové zprávy, které přijímají e-mailové programy, jako například Microsoft Outlook a Outlook Express, Microsoft Mail nebo Mozilla Thunderbird. Prověřuje nešifrované e-mailové zprávy a přílohy, vždy když je e-mailový program obdrží z poštovního serveru pomocí protokolu POP3.

Funkce hledání virů a spywaru nemůže zkontrolovat e-mailové zprávy ve webové poště, které zahrnují e-mailové aplikace, které běží ve webovém prohlížeči, jako například Hotmail, Yahoo! mail nebo Gmail. Stále budete chráněni před *viry*, i když neodstraníte škodlivé přílohy nebo používáte webovou poštu. Když e-mailovou přílohu otevřete, kontrola v reálném čase odstraní jakékoli škodlivé přílohy, než způsobí jakoukoli škodu.

Poznámka: Kontrola v reálném čase chrání pouze váš počítač, ale ne vaše přátele. Kontrola v reálném čase neprověřuje připojené soubory, pokud přílohu neotevřete. To znamená, že pokud používáte webovou poštu a zprávu přepošlete před otevřením této přílohy, můžete přátelům přeposlat nakažený e-mail.

4.2.4 Zobrazení výsledků kontroly

V historii virů a spywaru se zobrazují všechny škodlivé soubory, které produkt zjistil.

Někdy produkt nemůže provést akci, kterou jste vybrali při zjištění škodlivých položek. Například pokud vyberete, že chcete soubory vyléčit, a není možné je vyléčit, produkt je přesune do karantény. Tyto informace najdete v historii virů a spywaru.

Zobrazení historie:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Klepněte na možnost **Zobrazit historii odstranění**.

V historii virů a spywaru jsou uvedeny následující informace:

- datum a čas zjištění škodlivého souboru,
- název malwaru a jeho umístění v počítači,
- provedená akce.

4.3 Jak vyloučit soubory z kontroly

Někdy možná budete chtít vyloučit některé soubory nebo aplikace z kontroly. Vyloučené položky nebudou zkontrolovány, dokud je neodstraníte ze seznamu vyloučených položek.

Poznámka: Seznamy vyloučených položek lze samostatně zkontrolovat v reálném čase nebo ručně. Pokud například vyloučíte soubor z kontroly v reálném čase, bude zkontrolován během ruční kontroly, pokud je z ruční kontroly taktéž nevyloučíte.

4.3.1 Typy vyloučených souborů

Když soubory vyloučíte dle typu, soubory s vybranými příponami nebudou prověřeny na škodlivý obsah.

Přidání nebo odstranění souborů určitého typu, které chcete vyloučit:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte, zda chcete vyloučit soubory určitého typu z kontroly v reálném čase nebo z ruční kontroly:
   - Výběrem položek **Zabezpečení počítačeHledání virů a spywaru** lze z kontroly v reálném čase vyloučit určitý typ souborů.
   - Výběrem položek **Jiná nastaveníRuční kontrola** lze z kontroly v reálném čase vyloučit určitý typ souborů.
3. Klěpnete na možnost **Vyloučit soubory z kontroly**.
4. Postup vyloučení typu souboru:
   a) Přejděte na kartu **Typy souborů**.
   b) Vyberte volbu **Vyloučit soubory s těmito příponami**.
   c) Napište do pole vedle tlačítka **Přidat** příponu, která představuje typ souborů, které chcete vyloučit.

      Chcete-li zadat soubory, které nemají příponu, napište „.“. Můžete použít zástupný znak „?“, který představuje jakýkoliv samostatný znak nebo „*“, který představuje libovolný počet znaků.

      Chcete-li například vyloučit spustitelné soubory, napište do pole `exe`.
   d) Klepněte na tlačítko **Přidat**.
5. Opakujte předchozí krok pro jakékoliv soubory s danou příponou, které chcete z kontroly přítomnosti virů vyloučit.
6. Klepnutím na tlačítko **OK** zavřete dialog **Vyloučit z kontroly**.
7. Chcte-li použít nové nastavení, klepněte na tlačítko **OK**.

Vybrané typy souborů budou vyloučeny z příštích kontrol.

4.3.2 Vyloučení souborů podle umístění

Když soubory vyloučíte dle umístění, nebudou soubory ve vybraných jednotkách nebo složkách prověřeny na škodlivý obsah.

Přidání nebo odstranění umístění souborů, které chcete vyloučit:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte, zda chcete vyloučit umístění z kontroly v reálném čase nebo z ruční kontroly:
   - Výběrem položek **PočítačKontrola virů a spywaru** vyloučíte umístění z kontroly v reálném čase.

- Výběrem položek **PočítačRuční kontrola** vyloučíte umístění z ruční kontroly.

3. Klepněte na možnost **Vyloučit soubory z kontroly**.
4. Postup vyloučení souboru, jednotky nebo složky:
   a) Přejděte na kartu **Objekty**.
   b) Vyberte položku **Vyloučit objekty (soubory, složky, ...)**.
   c) Klepněte na tlačítko **Přidat**.
   d) Vyberte soubor, jednotku nebo složku, které chcete vyloučit z kontroly výskytu virů.

      Poznámka: Některé jednotky mohou být vyměnitelné, například CD, DVD nebo síťové jednotky. Síťové jednotky a prázdné vyměnitelné jednotky nemohou být vyloučeny.

   e) Klepněte na tlačítko **OK**.
5. Opakujte předchozí krok pro vyloučení dalších souborů, jednotek nebo složek z kontroly výskytu virů.
6. Klepnutím na tlačítko **OK** zavřete dialog **Vyloučit z kontroly**.
7. Klepnutím na tlačítko **OK** použijte nová nastavení.

Vybrané soubory, jednotky nebo složky budou z kontrol v budoucnu vyloučeny.

4.3.3 Zobrazení vyloučených aplikací

Můžete zobrazit aplikace, které jste vyloučili z kontroly, a odstranit je ze seznamu vyloučených položek, pokud je budete chtít zkontrolovat v budoucnu.

Pokud kontrola v reálném čase nebo ruční kontrola zjistí aplikaci, která se chová jako spyware nebo riskware, ale víte, že se jedná o bezpečnou aplikaci, můžete ji vyloučit z kontroly, aby vás produkt před touto aplikací již nevaroval.

Poznámka: Pokud se aplikace chová jako virus nebo jiný škodlivý software, nelze ji vyloučit.

Není možné vyloučit aplikace přímo. Nové aplikace se zobrazí v seznamu vyloučených položek, pouze když je vyloučíte během kontroly.

Postup zobrazení aplikací, které byly z kontroly vyloučeny:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte, zda chcete zobrazit aplikace, které byly vyloučeny z kontroly v reálném čase nebo ruční kontroly:
   - Výběrem položek **PočítačKontrola virů a spywaru** zobrazíte aplikace, které byly z kontroly v reálném čase vyloučeny.
   - Výběrem položek **PočítačRuční kontrola** zobrazíte aplikace, které byly z ruční kontroly vyloučeny.
3. Klepněte na možnost **Vyloučit soubory z kontroly**.
4. Klepněte na kartu **Aplikace**.

   Poznámka: Vyloučit lze pouze spyware a riskware nikoliv viry.

5. Pokud chcete vyloučené aplikace znovu prověřit:
   a) Vyberte aplikaci, kterou chcete zahrnout do kontroly.
   b) Klepněte na tlačítko **Odstranit**.
6. Klepnutím na tlačítko **OK** dialog **Vyloučit z kontroly** zavřete.
7. Klepnutím na tlačítko **OK** dialog zavřete.

4.4 Jak využívat karanténu?

Karanténa slouží jako úložiště potencionálně nebezpečných souborů.

Soubory umístěné v karanténě se nemohou šířit ani poškodit počítač.

Položky *malwaru*, *spywaru* a *riskwaru* můžete uložit do karantény, pak budou neškodné. V případě potřeby je možné aplikace a soubory umístěné v karanténě později obnovit.

Pokud soubor umístěný v karanténě nepotřebujete, můžete jej odstranit. Odstraněním položky umístěné v karanténě dojde k jejímu trvalému odstranění z počítače.

- Obecně je možné odstranit *malware* umístěný v karanténě.
- Ve většině případů je možné odstranit *spyware* umístěný v karanténě. *Spyware* umístěný v karanténě může být součástí skutečného softwarového programu a program nemusí po jeho odstranění fungovat správně. Chcete-li program v počítači ponechat, můžete *spyware* umístěný v karanténě obnovit.
- *Riskware* umístěný v karanténě může fungovat jako skutečný softwarový program. Pokud jste program nainstalovali a nastavili sami, můžete jej obnovit. Pokud byl *riskware* nainstalován bez vašeho vědomí, pravděpodobně tak bylo učiněno se škodlivými úmysly a měl by být smazán.

4.4.1 Zobrazení položek v karanténě

Můžete zobrazit další informace o položkách v karanténě.

Zobrazení podrobných informací o položkách v karanténě:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Klikněte na možnost **Zobrazit karanténu**.
   Na stránce **Karanténa** se zobrazuje celkový počet položek, které jsou uloženy v karanténě.
4. Chcete-li zobrazit detailní informace o položkách v karanténě, klepněte na položku **Detaily**.

   Obsah můžete třídit buď podle názvu malwaru nebo podle cesty k souboru.

   Zobrazí se seznam prvních 100 položek spolu s typy položek v karanténě, názvy a cestami, kam byly soubory nainstalovány.
5. Chcete-li zobrazit více informací o určité položce v karanténě, klepněte na ikonu ⓘ vedle položky ve sloupci **Stav**.

4.4.2 Obnovení položek uložených v karanténě

Položky umístěné v karanténě lze v případě potřeby obnovit.

V případě potřeby lze obnovit aplikace a soubory z karantény. Neobnovujte položky z karantény, pokud jsi nejste zcela jisti, že nejsou nebezpečné. Obnovené položky budou přesunuty do původního umístění v počítači.

Obnovení položek uložených v karanténě

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeHledání virů a spywaru**.
3. Klikněte na možnost **Zobrazit karanténu**.
4. Vyberte položku karantény, kterou chcete obnovit.

5. Klepněte na položku **Obnovit**.

Kapitola

5

Co je DeepGuard?

Témata:

Funkce DeepGuard monitoruje aplikace, aby zjistila potenciálně škodlivé změny systému.

Funkce DeepGuard zajistí, že budete používat pouze bezpečné aplikace. Bezpečnost aplikací ověřuje důvěryhodná služba cloudu. Pokud bezpečnost některé aplikace nelze ověřit, DeepGuard začne monitorovat její chování.

Funkce DeepGuard blokuje nové a nezjištěné *trojské koně*, *červy*, *prostředky zneužití* a jiné nebezpečné aplikace, které se pokoušejí provádět změny ve vašem počítači, a znemožňuje podezřelým aplikacím přístup k Internetu.

Mezi potenciálně škodlivé změny systému, které funkce DeepGuard zjišťuje, patří následující:

- změny nastavení systému (registrů systému Windows),
- pokusy o vypnutí důležitých programů systému, například programů zabezpečení jako je tento produkt,
- pokusy o úpravu důležitých systémových souborů.

5.1 Výběr položek, které budou monitorovány funkcí DeepGuard

Funkce DeepGuard monitoruje důležitá nastavení systému, soubory a pokusy o vypnutí důležitých aplikací, například tohoto zabezpečovacího produktu.

Výběr položek, které bude funkce DeepGuard monitorovat:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeDeepGuard**.
3. Přesvědčte se, že je funkce **DeepGuard** zapnutá.
4. Vyberte nastavení funkce DeepGuard:

Upozornit na podezřelé chování	Toto nastavení ponechte zapnuté, chcete-li být upozorňováni na podezřelé chování aplikací. Pokud je vypnete, DeepGuard přestane monitorovat podezřelé chování, čímž se sníží zabezpečení.
Upozornit na zneužívání aplikace	Toto nastavení ponechte zapnuté, chcete-li být upozorňováni na potenciální pokusy o zneužití. Pokud je vypnete, škodlivé webové stránky a dokumenty budou moci zneužívat vaše aplikace, čímž se sníží zabezpečení. Doporučujeme, abyste toto nastavení nevypínali.
Vyžádat si mé svolení k vytvoření internetového připojení	Toto nastavení ponechte zapnuté, pokud chcete, aby vás funkce DeepGuard upozorňovala na pokusy neznámých aplikací o připojení k Internetu.
Použít režim kompatibility (snížení zabezpečení)	Aby byla zajištěna maximální ochrana, funkce DeepGuard dočasně změní spuštěné programy. Některé programy kontrolují, zda nejsou poškozeny nebo změněny, a nemusí být s touto funkcí kompatibilní. Například online hry s anti-cheatingovými nástroji kontrolují, zda nebyly nijak upraveny, při jejich spuštění. V těchto případech můžete zapnout režim kompatibility.

5. Klepněte na tlačítko **OK**.

5.1.1 Povolení aplikací, které funkce DeepGuard zablokovala

Je možné řídit, které aplikace funkce DeepGuard povolí a které zablokuje.

Některy může funkce DeepGuard zablokovat spuštění bezpečné aplikace, i když chcete aplikaci použít a když víte, že je bezpečná. To se stává, protože aplikace se pokouší provést změny systému, které by mohly být škodlivé. Také můžete aplikaci zablokovat neúmyslně, když se zobrazí vyskakovací okno funkce DeepGuard.

Povolení aplikací, které funkce DeepGuard zablokovala:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeDeepGuard**.
3. Klikněte na položku **Změnit oprávnění aplikací**.
   Zobrazí se seznam **Monitorované aplikace**.
4. Vyhledejte aplikaci, kterou chcete povolit, a klikněte na položku **Podrobnosti**.

   Poznámka: Klepnutím na záhlaví sloupce můžete položky v seznamu seřadit. Například klepnutím na sloupec **Povolení** můžete položky v seznamu seřadit do skupin povolených a zamítnutých programů.

5. Vyberte možnost **Povolit**.
6. Klepněte na tlačítko **OK**.
7. Klepněte na položku **Zavřít**.

Funkce DeepGuard umožní aplikaci znovu provést změny systému.

5.2 Co dělat při varování na podezřelé chování

DeepGuard blokuje monitorované aplikace, když se chovají podezřele nebo se pokoušejí o připojení k Internetu.

Podle toho, co se děje, se můžete rozhodnout, zda aplikaci dovolíte pokračovat.

5.2.1 Funkce DeepGuard blokuje nebezpečnou aplikaci

Funkce DeepGuard vás upozorní, když zjistí a zablokuje nebezpečnou aplikaci.

Když se zobrazí upozornění:

Klepnutím na možnost **Podrobnosti** zobrazíte další informace o aplikaci.
V podrobnostech jsou uvedeny tyto informace:

- umístění aplikace,
- reputace aplikace v cloudu zabezpečení,
- jak je běžná a
- název zjištěného malwaru.

Vzorek aplikace můžete odeslat k analýze.

5.2.2 Funkce DeepGuard blokuje podezřelou aplikaci

Když je v nastavení funkce DeepGuard zapnutá možnost **Upozornit na podezřelé chování**, DeepGuard oznámí zjištění aplikace, která se chová podezřele. Pokud aplikaci věříte, můžete povolit pokračování jejího běhu.

Chcete-li se rozhodnout, co provedete s aplikací zablokovanou funkcí DeepGuard:

1. Klepnutím na možnost **Podrobnosti** zobrazíte další informace o aplikaci.
   V podrobnostech jsou uvedeny následující informace:
   - umístění aplikace,
   - reputace aplikace v cloudu zabezpečení,
   - jak je běžná a
   - název malwaru.
2. Rozhodněte se, zda je možné aplikaci, kterou funkce DeepGuard zablokovala, věřit:
   - Vyberte možnost **Aplikaci věřím. Je možné pokračovat.**, pokud nechcete aplikaci blokovat.

     Aplikace je pravděpodobně bezpečná, pokud:

     - Funkce DeepGuard aplikaci zablokovala po určité vaší akci.
     - Aplikaci znáte.
     - Získali jste aplikaci z důvěryhodného zdroje.
   - Vyberte možnost **Aplikace nevěřím. Je třeba ji ponechat blokovanou.**, chcete-li aplikaci nadále blokovat.

     Aplikace je pravděpodobně nebezpečná, pokud:

     - Aplikace není příliš častá.
     - Pověst aplikace není známa.
     - Aplikaci neznáte.

Vzorek podezřelé aplikace můžete odeslat k analýze.

5.2.3 Neznámá aplikace se pokouší o připojení k Internetu

Když je v nastavení funkce DeepGuard zapnutá možnost **Vyžádat si mé svolení k vytvoření internetového připojení**, DeepGuard vás upozorní na pokus neznámé aplikace o připojení k Internetu. Pokud této aplikaci důvěřujete, můžete jí dovolit, aby pokračovala.

Chcete-li se rozhodnout, co provedete s aplikací zablokovanou funkcí DeepGuard:

1. Klepnutím na možnost **Podrobnosti** zobrazíte další informace o aplikaci.
   V podrobnostech jsou uvedeny následující informace:
   - umístění aplikace,
   - reputace aplikace v cloudu zabezpečení,
   - jak běžná je tato aplikace,
   - co se pokusila provést a
   - k čemu se pokusila připojit.
2. Rozhodněte se, zda je možné aplikaci, kterou funkce DeepGuard zablokovala, věřit:
   - Vyberte možnost **Aplikaci věřím. Je možné pokračovat.**, pokud nechcete aplikaci blokovat.

     Aplikace je pravděpodobně bezpečná, pokud:
     - Funkce DeepGuard aplikaci zablokovala po určité vaší akci.
     - Aplikaci znáte.
     - Získali jste aplikaci z důvěryhodného zdroje.
   - Pokud chcete aplikaci ponechat zablokovanou, vyberte možnost **Nedůvěřuji této aplikaci. Trvale zablokovat.**

     Aplikace je pravděpodobně nebezpečná, pokud:
     - Aplikace není příliš častá.
     - Pověst aplikace není známa.
     - Aplikaci neznáte.

Vzorek podezřelé aplikace můžete odeslat k analýze.

5.2.4 Funkce DeepGuard zjistí možné zneužití

Když je v nastavení funkce DeepGuard zapnutá možnost **Upozornit na zneužívání aplikace**, funkce DeepGuard zobrazí upozornění, pokud po otevření škodlivé webové stránky nebo dokumentu zjistí podezřelé chování některé aplikace.

Chcete-li se rozhodnout, co provedete s aplikací zablokovanou funkcí DeepGuard:

1. Klepnutím na možnost **Podrobnosti** zobrazíte další informace o aplikaci.
   V podrobnostech jsou uvedeny následující informace:
   - název malwaru a
   - zdroj prostředku zneužití (škodlivá webová stránka nebo dokument), pokud je znám.
2. Rozhodněte se, zda je možné aplikaci, kterou funkce DeepGuard zablokovala, věřit:
   - Pokud nechcete aplikaci ukončit, vyberte možnost **Ponechat aplikaci spuštěnou (může ohrozit vaše zařízení)**.

     Může být vhodné nechat aplikaci běžet v případě, že by ukončení bez uložení dat v daném okamžiku způsobilo potíže.
   - Výběrem možnosti **Ukončit aplikaci, aby nedošlo k zneužití** ukončíte aplikaci a zajistíte, aby zařízení nebylo ohroženo.

Doporučujeme ukončení aplikace, aby vaše zařízení nebylo vystaveno riziku.

Pokud bude identifikován zdroj zneužití, můžete odeslat vzorek k analýze.

5.3 Odeslání podezřelé aplikace k analýze

Můžete nám pomoci vylepšovat ochranu, jestliže předáte podezřelé aplikace k analýze.

Vzorek doporučujeme odeslat v následujících případech:

- Funkce DeepGuard zablokuje aplikaci, o které víte, že je bezpečná, nebo
- Máte podezření, že se může jednat o *malwarovou* aplikaci.

Odeslání vzorku k analýze:

1. V upozornění funkce DeepGuard klepněte na položku **Nahlásit aplikaci společnosti F-Secure**. Produkt zobrazí podmínky odeslání.
2. Klepněte na možnost **Přijmout**, pokud s podmínkami souhlasíte a chcete vzorek odeslat.

Kapitola
6

Co je brána firewall?

Témata:

Brána *firewall* brání narušitelům a škodlivým aplikacím v přístupu k vašemu počítači z Internetu.

Brána firewall povoluje pouze bezpečná připojení k Internetu z vašeho počítače a blokuje útoky z Internetu.

6.1 Zapnutí nebo vypnutí brány firewall

Bránu firewall ponechte zapnutou, aby blokovala přístup narušitelů k vašemu počítači.

Zapnutí nebo vypnutí brány firewall:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Zapněte nebo vypněte **bránu firewall**.

   Poznámka: Váš počítač nebude plně chráněn, pokud funkce zabezpečení vypnete.

3. Klepněte na tlačítko **OK**.

Doporučujeme *bránu firewall* nevypínat. Pokud tak učiníte, počítač nebude nijak chráněn proti všem síťovým útokům. Jestliže aplikace přestane pracovat, neboť není připojena k Internetu, místo vypnutí *brány firewall* změňte *nastavení brány firewall*.

6.2 Změna nastavení brány firewall

Pokud je brána firewall zapnuta, omezuje přístup k vašemu počítači a z něj. Některé aplikace mohou vyžadovat, abyste je v bráně firewall povolili, aby fungovaly správně.

Produkt používá k ochraně vašeho počítače bránu firewall systému Windows.

Změna nastavení brány firewall systému Windows:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeBrána firewall**.
3. Klepněte na nastavení **Změnit bránu firewall systému Windows**.

   Poznámka: Úprava nastavení vyžaduje oprávnění správce.

Další informace o bráně firewall systému Windows najdete v dokumentaci k systému Microsoft Windows.

6.3 Bránit aplikacím ve stahování nebezpečných souborů

Aplikacím v počítači lze zabránit ve stahování nebezpečných souborů z Internetu.

Některé webové stránky obsahují zneužívající a jinak nebezpečné soubory, které mohou počítač poškodit. Díky pokročilé ochraně sítě můžete jakékoli aplikaci zabránit ve stahování nebezpečných souborů dříve, než se dostanou do počítače.

Blokování aplikací před stahováním nebezpečných souborů:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeBrána firewall**.
3. Vyberte možnost **Nedovolit aplikacím stahovat nebezpečné soubory**.

Poznámka: Toto nastavení bude účinné, i když vypnete bránu firewall.

6.4 Používání osobních bran firewall

Tento produkt je navržen pro spolupráci s bránou Windows Firewall. Jiné osobní brány firewall potřebují ke spolupráci s tímto produktem dodatečné nastavení.

Produkt používá bránu Windows Firewall k výkonu základních funkcí brány firewall, jako je řízení příchozích síťových přenosů a oddělení vnitřní sítě od veřejného Internetu. Funkce DeepGuard kromě toho monitoruje nainstalované aplikace a znemožňuje přístup podezřelých aplikací k Internetu bez svolení uživatele.

Pokud nahradíte bránu Windows Firewall osobní bránou firewall, zajistěte, aby umožňovala příchozí a odchozí síťové přenosy všech procesů softwaru F-Secure, a povolte všechny procesy softwaru F-Secure, když vás k tomu tato osobní brána firewall vyzve.

Tip: Pokud u vaší osobní brány firewall existuje režim ručního filtrování, použijte ho k povolení všech procesů softwaru F-Secure.

Kapitola

7

Blokování nevyžádané pošty

Témata:

Filtrování nevyžádaných zpráv a phishingu lze použít k zachycení nevyžádané pošty a phishingových zpráv a jejich odstranění ze složky doručených zpráv.

Nevyžádaná pošta a *phishingové* zprávy často zabírají místo pro žádoucí e-mailové zprávy.

E-mailová zpráva je považována za *nevyžádanou poštu*, pokud byla odeslána v rámci větší kolekce zpráv s téměř totožným obsahem a pokud jste neudělili povolení pro zasílání takových zpráv na vaši adresu.

Phishingové zprávy se pokouší odcizit vaše osobní údaje. Tyto skutečně vypadající zprávy mají vyvolat dojem, že pochází z ověřených zdrojů, a jejich cílem je vás zmást, abyste poskytli své osobní údaje, jako například čísla bankovních účtů, hesla a čísla platebních karet nebo sociálního pojištění. Nevěřte obsahu žádných e-mailových zpráv, které budou zjištěny při filtrování nevyžádané pošty a phishingu.

7.1 Zapnutí a vypnutí filtrování nevyžádaných zpráv a phishingu

Ponechejte filtrování nevyžádaných zpráv a phishingu zapnuté, aby bylo možné odstraňovat nevyžádané a phishingové zprávy ze složky doručených zpráv.

Zapnutí a vypnutí filtrování nevyžádaných zpráv a phishingu:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Zapněte a vypněte **filtrování nevyžádaných zpráv a phishingu**.
3. Klepněte na tlačítko **OK**.

Tip: V e-mailovém programu vytvořte pravidlo filtrování, chcete-li automaticky přesunovat hromadné reklamy a podvodné e-maily do složky nevyžádané pošty.

7.2 Označit nevyžádané zprávy štítkem

Filtrování nevyžádané pošty a phishingu může označit pole předmětu nevyžádaných zpráv štítkem.

Přidání textu [SPAM] do nevyžádaných a phishingových zpráv:

1. Na stránce Stav klikněte na tlačítko **Nastavení**.

   Poznámka: Změna těchto nastavení vyžaduje oprávnění správce.

2. Vyberte možnost **Zabezpečení počítačeFiltrování nevyžádané pošty**.
3. Vyberte možnost **Označit nevyžádanou poštu předponou [SPAM] v poli předmětu e-mailu (Mark spam with [SPAM] in the e-mail subject field)**.
4. Klepněte na tlačítko **OK**.

Když obdržíte nevyžádaný nebo phishingový e-mail, funkce filtrování nevyžádané pošty a phishingu přidá text `[SPAM]` do pole předmětu e-mailové zprávy.

7.3 Nastavení e-mailových programů pro filtrování nevyžádané pošty

V e-mailovém programu lze vytvořit pravidla filtrování *nevyžádané pošty* a *phishingu*, chcete-li automaticky přesunout nežádoucí zprávy do samostatné složky.

Filtrování nevyžádané pošty a phishingu označí všechny nevyžádané a phishingové e-maily, které najde, předponou [SPAM] v poli předmětu e-mailové zprávy. Chcete-li automaticky přesunout tyto zprávy ze složky doručených zpráv, je třeba v e-mailovém programu vytvořit složku nevyžádané pošty a pravidla filtrování. Pokud máte více e-mailových účtů, je třeba vytvořit pravidla filtrování pro každý e-mailový účet samostatně.

Tato část obsahuje pokyny k vytvoření složky nevyžádané pošty a pravidel filtrování pro aplikace Windows Mail, Microsoft Outlook, Mozilla Thunderbird, Eudora a Opera. Tyto pokyny lze použít také pro vytvoření podobných pravidel filtrování v jiných e-mailových programech.

Poznámka: Filtrování *nevyžádané pošty* a *phishingu* podporuje pouze protokol POP3. E-mailové programy nebo jiné protokoly nejsou podporovány.

7.3.1 Blokování nevyžádané pošty v programu Windows Mail

Chcete-li filtrovat *nevyžádané* a phishingové e-mailové zprávy, je třeba vytvořit složku nevyžádané pošty a pravidlo filtrování.

Chcete-li filtrování nevyžádaných a phishingových zpráv používat s aplikací Windows Mail, zkontrolujte, že je možnost **Označit nevyžádanou poštu předponou [SPAM] v poli předmětu e-mailu (Mark spam with [SPAM] in the e-mail subject field)** v nastavení **Filtrování nevyžádané pošty (Spam filtering)** zapnutá.

Vytvoření pravidla filtrování *nevyžádané pošty*:

1. V nabídce **Windows Mail** vyberte položku **SložkyPravidla pro zprávy**.

   Poznámka: Pokud se automaticky nezobrazí okno **Nové pravidlo pro poštu**, klepněte na tlačítko **Nový** na kartě **Pravidla e-mailu**.

2. V okně **Nové pravidlo pro poštu** vytvořte pravidlo pro přemísťování e-mailových zpráv do složky *Nevyžádaná pošta*:
   a) V poli s podmínkami vyberte možnost **Kde řádek Předmět obsahuje určitá slova**.
   b) V poli s akcemi vyberte možnost **Přesunout zprávu do určené složky**.
3. V poli obsahujícím popis pravidla klepněte na odkaz **obsahuje určitá slova**.
   a) V okně **Zadat určitá slova** zadejte řetězec `[SPAM]` a klepněte na tlačítko **Přidat**.
   b) Klepnutím na tlačítko **OK** zavřete okno **Zadat určitá slova**.
4. V poli obsahujícím popis pravidla klepněte na odkaz na **určenou** složku.
   a) V okně **Přesunout** klepněte na položku **Nová složka**.
   b) Jako název nové složky zadejte text `Nevyžádaná pošta` a klepněte na tlačítko **OK**.
   c) Klepnutím na tlačítko **OK** zavřete okno **Přesunout**.
5. Do pole pro název pravidla zadejte text `Nevyžádaná pošta`.
6. Klepnutím na tlačítko **Uložit pravidlo** zavřete okno **Nové pravidlo pro poštu**.
   Otevře se okno **Pravidla**.
7. Klepnutím na tlačítko OK zavřete okno **Pravidla**.

   Pokud chcete toto nové pravidlo použít na e-mailové zprávy, které již jsou ve složce s doručenou poštou, vyberte pravidlo **Nevyžádaná pošta** a klepněte na tlačítko **Použít nyní**.

Vytvořili jste pravidlo filtrování *nevyžádané pošty*. Od tohoto okamžiku bude *Nevyžádaná pošta* filtrována do složky *nevyžádané pošty*.

7.3.2 Blokování nevyžádané pošty v aplikaci Microsoft Outlook

Chcete-li filtrovat *nevyžádané* a phishingové e-mailové zprávy, je třeba vytvořit složku nevyžádané pošty a pravidlo filtrování.

Chcete-li filtrování nevyžádaných a phishingových zpráv používat s aplikací Microsoft Outlook, zkontrolujte, že je možnost **Označit nevyžádanou poštu předponou [SPAM] v poli předmětu e-mailu (Mark spam with [SPAM] in the e-mail subject field)** v nastavení **Filtrování nevyžádané pošty (Spam filtering)** zapnutá.

Poznámka: Uvedené kroky platí pro aplikaci Microsoft Outlook 2007. Kroky pro jiné verze se mohou poněkud lišit.

Vytvoření pravidla filtrování *nevyžádané pošty*:

1. V nabídce **Nástroje** vyberte položku **Pravidla a oznámení**.
2. Na kartě **Pravidla e-mailu** klepněte na tlačítko **Nové pravidlo**.
3. V seznamu **Třídit zprávy** vyberte šablonu **Přesunout zprávy s určitými slovy v předmětu do složky**.
4. Klepněte na tlačítko **Další**.
5. V podokně **Krok 2: Upravte popis pravidla** klepněte na odkaz **určitá slova**.
   a) V poli **Zadejte slovo nebo spojení, které chcete vyhledat v poli předmětu** zadejte text `[SPAM]` a klepněte na tlačítko **Přidat**.
   b) Klepnutím na tlačítko **OK** zavřete okno **Zadat určitá slova**.
6. V podokně **Krok 2: Upravte popis pravidla** klepněte na odkaz **zadaná** složka.
   a) V okně **Pravidla a oznámení** klepněte na tlačítko **Nové**.
   b) Jako název nové složky zadejte text `Nevyžádaná pošta` a klepněte na tlačítko **OK**.
   c) Klepnutím na tlačítko **OK** zavřete okno **Pravidla a oznámení**.
7. Klepněte na tlačítko **Dokončit**.
8. Klepněte na tlačítko **OK**.

   Pokud chcete toto nové pravidlo použít na e-mailové zprávy, které již jsou ve složce s doručenou poštou, před zavřením okna Pravidla a oznámení klepněte na tlačítko **Spustit pravidla**.

Vytvořili jste pravidlo filtrování *nevyžádané pošty*. Od tohoto okamžiku bude *Nevyžádaná pošta* filtrována do složky *nevyžádané pošty*.

7.3.3 Blokování nevyžádané pošty v aplikaci Mozilla Thunderbird a Eudora OSE

Chcete-li filtrovat *nevyžádané* a phishingové e-mailové zprávy, je třeba vytvořit složku nevyžádané pošty a pravidlo filtrování.

Chcete-li vytvořit filtrovací pravidlo pro *nevyžádanou poštu*:

1. Vytvoření nové složky pro nevyžádanou poštu a phishingové zprávy:
   a) Klikněte pravým tlačítkem na název svého e-mailového účtu a vyberte příkaz **Nová složka (New Folder)**.
   b) Jako název složky zadejte `nevyžádaná pošta`.
   c) Klikněte na položku **Vytvořit složku (Create Folder)**.
2. Přesvědčte se, že je vybrán název vašeho účtu a klikněte na položku **Spravovat filtry zpráv (Manage message filters)** v seznamu **Pokročilé funkce (Advanced Features)**.
3. Klepněte na položku **Nový**.
4. Jako **název filtru** zadejte `Nevyžádaná pošta`.

5. Vytvoření přizpůsobeného záznamu záhlaví:
   a) V seznamu **Porovnat všechny následující položky (Match all of the following)** otevřete první rozevírací nabídku, v níž je ve výchozím nastavení vybrána možnost **Předmět (Subject)**.
   b) Z prvního rozevíracího seznamu vyberte položku **Vlastní (Customize)**.
   c) V dialogovém okně Vlastní nastavení záhlaví zadejte řetězec X-Spam-Flag jako záhlaví nové zprávy a klepněte na položku Přidat (Add).
   d) Klepnutím na tlačítko **OK** zavřete dialogové okno **Vlastní nastavení záhlaví (Customize Headers)**.
6. Vytvoření pravidla pro filtrování nevyžádaných zpráv:
   a) V seznamu **Porovnat všechny následující položky (Match all of the following)** otevřete první rozevírací nabídku a vyberte položku **X-Spam-Flag**, kterou jste vytvořili v předchozím kroku.
   b) Ve druhé rozevírací nabídce vyberte možnost **obsahuje (contains)**.
   c) Jako text, který chcete porovnat s posledním textovým polem na řádku, zadejte `Ano`.
7. Vytvořte akci, která přesune nevyžádanou zprávu do složky nevyžádané pošty:
   a) V seznamu **Provést tyto akce (Perform these actions)** vyberte položku **Přesunout zprávu do (Move Message to)**.
   b) Ve druhém rozevíracím seznamu vyberte složku `nevyžádané pošty`.
8. Klepnutím na tlačítko **OK** uložte změny.
9. Zavřete dialogové okno **Třídící filtry zpráv**.

Vytvořili jste pravidlo filtrování *nevyžádané pošty*. Od tohoto okamžiku bude *Nevyžádaná pošta* filtrována do složky *nevyžádané pošty*.

7.3.4 Blokování nevyžádané pošty v aplikaci Opera

Chcete-li filtrovat *nevyžádané* a phishingové e-mailové zprávy, je třeba vytvořit složku nevyžádané pošty a pravidlo filtrování.

Poznámka: Kroky uvedené výše platí pro aplikaci Opera verze 12. Kroky pro jiné verze se mohou poněkud lišit.

Vytvoření pravidla filtrování *nevyžádané pošty*:

1. Přepněte aplikaci do zobrazení **Pošta aplikace Opera**.
2. Pravým tlačítkem klepněte na složku *Nevyžádaná pošta* a vyberte možnost **Vlastnosti**.
3. Klepněte na položku **Přidat pravidlo**.
4. Vytvořte pravidlo pro přesunutí e-mailové zprávy do složky nevyžádané pošty:
   a) V prvním seznamu vyberte položku **Libovolná hlavička (Any header)**.
   b) Z druhého seznamu vyberte položku **obsahuje**.
   c) Do textového pole jako text, který chcete porovnávat, zadejte `X-Spam-Flag: Yes`.

   Zkontrolujte, zda je mezi dvojtečkou a slovem `Yes` mezera.
5. Klepnutím na tlačítko **Zavřít** potvrďte nové pravidlo pro filtrování *nevyžádané* pošty.

Vytvořili jste pravidlo filtrování *nevyžádané pošty*. Od tohoto okamžiku bude *nevyžádaná pošta* filtrována do složky *nevyžádané pošty*.

Kapitola

8

Bezpečné používání Internetu

Témata:

Informace o tom, jak začít s produktem pracovat.

Tento produkt vám pomáhá bezpečně procházet web. Kromě ochrany proti škodlivému softwaru a webovým stránkám můžete rovněž omezit typ obsahu, který mohou jednotlivé uživatelské účty zobrazit.

Tento produkt využívá k řízení nastavení pro jednotlivé osoby, které používají váš počítač, uživatelské účty systému Windows. Změny nastavení produktu pro jednotlivé uživatelské účty systému Windows může provádět pouze uživatel s oprávněním pro přístup správce. Doporučujeme pro každou osobu, která používá váš počítač, vytvořit samostatný uživatelský účet systému Windows. Například uživatelé typu guest (host) by neměli mít pro své uživatelské účty oprávnění pro přístup správce.

8.1 Jak chránit různé uživatelské účty

Aby se vám dostalo nejlepší ochrany proti online hrozbám, měli byste používat samostatný uživatelský účet systému Windows pro každou osobu, která používá váš počítač.

Tento produkt umožňuje použití různých nastavení pro jednotlivé uživatelské účty systému Windows, které jste vytvořili v počítači. Pouze uživatelé s přístupem správce mohou měnit nastavení produktu pro jiné uživatelské účty. Všichni ostatní uživatelé s výjimkou správců by měli mít pouze normální přístupová práva, aby nemohli měnit nastavení, která jste jim nadefinovali.

8.1.1 Vytváření uživatelských účtů systému Windows

Prostřednictvím tohoto produktu lze vytvářet uživatelské účty systému Windows.

Vytváření uživatelských účtů systému Windows:

1. Na hlavní stránce klikněte na položku **Vytvořit nový**.
   Tímto postupem otevřete nastavení uživatelského účtu v systému Windows.
2. Zadejte potřebné údaje a vytvořte nebo upravte příslušný uživatelský účet.

8.1.2 Prohlížení statistik

Na stránce **Statistiky** můžete zobrazovat webové stránky, které byly procházeny a blokovány.

Produkt shromažďuje informace o navštívených a blokovaných webových serverech. Tyto informace jsou u jednotlivých uživatelských účtů systému Windows specifické pro uživatele.

Blokované webové servery jsou rozděleny na servery, které jsou blokovány filtrováním webových stránek, a na ty, které jsou blokovány ochranou procházení. Můžete tak vidět, zda blokovaný server má obsah, který jste záměrně zablokovali, nebo zda byl produkt označen jako potenciálně škodlivý.

8.2 Ochrana procházení Internetu

Ochrana procházení Internetu usnadňuje hodnocení zabezpečení webů, které navštěvujete, a zabraňuje neúmyslnému přístupu k nebezpečným webům.

Ochrana procházení zobrazuje hodnocení zabezpečení webových stránek uvedených ve výsledcích vyhledávače. Identifikací webových stránek, které obsahují bezpečnostní hrozby, jako například malware (viry, červy, trojské koně) a podvodné zprávy, hodnocení zabezpečení v rámci ochrany procházení vám pomáhají vyhýbat se nejnovějším internetovým hrozbám, které tradiční antivirové programy ještě neznají.

Existují čtyři možná hodnocení zabezpečení pro webové stránky; bezpečná, podezřelá, škodlivá a neznámá. Tato hodnocení zabezpečení jsou založena na informacích z několika zdrojů, například od analytiků malwaru ze společnosti F-Secure a partnerů společnosti F-Secure.

8.2.1 Zapnutí a vypnutí ochrany procházení Internetu

Po zapnutí ochrany procházení Internetu bude zablokován přístup ke škodlivým webům.

Zapnutí nebo vypnutí ochrany procházení Internetu:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyOchrana procházení**.
3. Klikněte na přepínač v pravém horním rohu.
4. Pokud je prohlížeč spuštěn, restartujte jej, aby byla použita změněná nastavení.

Tento produkt zajišťuje pomocí rozšíření prohlížeče plnou podporu ochrany procházení na zabezpečených webech (HTTPS). Prohlížeč by měl toto rozšíření automaticky zjistit a zapnout, ale v některých případech je nutné ho zapnout ručně. Zapnutí rozšíření prohlížeče:

- V prohlížeči Firefox vyberte v nabídce položku **NástrojeDoplňky** a klikněte na tlačítko **Povolit** vedle rozšíření.
- V prohlížeči Chrome vyberte v nabídce položku **Nastavení**, klikněte na položku **Rozšíření** a vyberte možnost **Povolit** vedle rozšíření.
- V prohlížeči Internet Explorer vyberte položku **NástrojeSpravovat doplňky**, vyberte rozšíření prohlížeče a klikněte na tlačítko **Povolit**.

Poznámka: Pokud musíte rozšíření zapnout ručně, je nutné ho zapnout zvlášť pro každý uživatelský účet v počítači.

8.2.2 Hodnocení zabezpečení ochrany procházení Internetu

Ochrana procházení Internetu zobrazuje hodnocení bezpečnosti webových stránek ve výsledcích vyhledávače.

Barevně odlišené ikony udávají hodnocení bezpečnosti aktuálního webu. Hodnocení bezpečnosti jednotlivých odkazů ve výsledcích hledání je také vyznačeno stejnými ikonami:

Zelená barva udává, že pokud je nám známo, je tento server bezpečný. Na tomto webovém serveru jsme nenašli nic podezřelého.

Žlutá barva udává, že je server podezřelý. Doporučujeme, abyste byli při jeho návštěvě opatrní, nestahovali žádné soubory a neuváděli žádné osobní údaje.

Červená barva znamená, že je server škodlivý. Doporučujeme, abyste tento webový server nenavštěvovali.

Šedá barva udává, že webový server dosud nebyl analyzován a momentálně o něm nejsou k dispozici žádné informace.

Hodnocení zabezpečení jsou dostupná na těchto vyhledávacích webech:

- Google
- Bing
- Yahoo

V závislosti na nastaveních ochrany procházení Internetu můžete navštěvovat weby, které byly vyhodnoceny jako nebezpečné. Webové servery jsou buďto automatickly blokovány, nebo se pouze zobrazí upozornění na možné riziko.

Zobrazení hodnocení webových odkazů

Když nastavíte funkci Ochrana procházení, aby zobrazovala hodnocení, ve výsledcích vyhledávačů (Google, Yahoo a Bing) se zobrazí hodnocení zabezpečení webů.

Zobrazení hodnocení webů:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyOchrana procházení**.
3. Vyberte možnost **Zobrazit hodnocení reputace webových serverů ve výsledcích vyhledávání**.
4. Klepněte na tlačítko **OK**.

Když prohledáváte web vyhledávacím strojem, ochrana procházení zobrazuje hodnocení zabezpečení nalezených webů.

8.2.3 Postup v případě zablokování webu

Při pokusu o přístup k webu, který byl vyhodnocen jako škodlivý, se zobrazí upozornění ochrany procházení Internetu na blokování stránky.

Zobrazí-li se upozornění ochrany procházení Internetu na blokování stránky:

1. Klepněte na možnost **Domovská stránka** a přejděte na domovskou stránku, aniž byste na nebezpečný web vstoupili.

   Tuto akci důrazně doporučujeme.
2. Pokud přesto chcete na stránku přejít, klikněte na položku **Povolit web**.

8.3 Bezpečné používání online bankovnictví

Ochrana bankovnictví chrání před nebezpečnými činnostmi při přístupu k online bankovnictví nebo provádění transakcí online.

Ochrana bankovnictví automaticky vyhledává bezpečná připojení k webům online bankovnictví a blokuje všechna připojení, která nevedou k požadovaným stránkám. Když otevřete web online bankovnictví, budou povolena pouze připojení na weby online bankovnictví nebo na weby, které jsou pro online bankovnictví považovány za bezpečné.

Ochrana bankovnictví nyní podporuje následující prohlížeče:

- Internet Explorer 9 nebo novější
- Firefox 13 nebo novější
- Google Chrome

Poznámka: Tato funkce není k dispozici ve všech verzích produktu.

8.3.1 Zapnutí ochrany bankovnictví

Je-li ochrana bankovnictví zapnuta, relace a transakce online bankovnictví jsou chráněny.

Zapnutí ochrany bankovnictví:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyOchrana bankovních operací**.
3. Klikněte na přepínač v pravém horním rohu.

8.3.2 Používání ochrany bankovnictví

Je-li ochrana bankovnictví zapnuta, automaticky zjišťuje přístupy k webu online bankovnictví.

Když otevřete webovou stránku online bankovnictví v prohlížeči, v horní části obrazovky se objeví oznámení **Ochrana bankovnictví**. Dokud bude spuštěna relace ochrany bankovnictví, všechna ostatní připojení budou blokována.

Tip: Klikněte na tlačítko **Změnit nastavení** v oznámení, chcete-li změnit nastavení produktu pro váš uživatelský účet.

Ukončení relace ochrany bankovnictví a obnovení ostatních připojení:

Klikněte na tlačítko **Konec** v oznámení **Ochrana bankovnictví**.

8.4 Bezpečné procházení

Před mnohými hrozbami internetu se můžete ochránit monitorováním všech uživatelských účtů systému Windows na vašem počítači.

Na internetu se nachází mnoho zajímavých webů, ale také zde na uživatele číhá mnoho rizik. Mnoho webů obsahuje materiály, které můžete považovat za nevhodné. Uživatelé mohou být vystaveni nevhodnému obsahu nebo mohou obdržet obtěžující zprávy prostřednictvím e-mailu nebo konverzace. Mohou omylem stáhnout soubory obsahující *viry*, které by mohly poškodit počítač.

Poznámka: Omezením přístupu k obsahu online ochráníte svoje uživatelské účty před konverzačními a e-mailovými programy, které běží ve webovém prohlížeči.

Můžete omezit weby, které lze zobrazit, a naplánovat dobu, kterou je možné strávit na internetu. Dále je možné blokovat odkazy na obsah pro dospělé uvedené ve výsledcích vyhledávače. Protože jsou tato omezení použita na uživatelské účty systému Windows, jsou v platnosti vždy, když se někdo přihlásí pomocí vlastního uživatelského účtu.

8.4.1 Omezení přístupu k obsahu na webu

Můžete vybrat typ filtrování, který chcete používat pro různé uživatelské účty systému Windows.

Filtrování webů blokuje přístup buď na všechny webové stránky, které jste nepovolili, nebo na všechny webové stránky, které obsahují blokovaný obsah.

Povolení webových stránek

Můžete povolit přístup jen k těm webovým serverům a stránkám, jimž důvěřujete, a to přidáním do seznamu povolených webových stránek.

Povolení přístupu na konkrétní webové stránky:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyBlokování obsahu**.
3. Klikněte na přepínač v pravém horním rohu.
4. Vyberte možnost **Povolit pouze vybrané weby**.
5. Klepnutím na tlačítko **Přidat** weby přidáte do seznamu **Povolené weby**.
6. Až budou přidány všechny webové servery, které chcete povolit, klikněte na tlačítko **OK**.

Po přihlášení k vašemu počítači mohou všichni uživatelé účtů systému Windows, které jste upravili, nyní přistupovat pouze na ty webové stránky, které jste přidali do seznamu povolených webových stránek.

Blokování webových stránek podle jejich obsahu

Je možné zablokovat přístup k webovým serverům a stránkám s nevhodným obsahem.

Výběr typů webového obsahu, které se mají blokovat:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyBlokování obsahu**.
3. Klikněte na přepínač v pravém horním rohu.
4. Vyberte možnost **Blokovat webový obsah**.
5. Vyberte typy obsahu, které chcete blokovat.

6. Až budou vybrány všechny typy obsahu, které chcete blokovat, klikněte na tlačítko **OK**.

Po přihlášení k vašemu počítači nebudou moci uživatelé účtů systému Windows, které jste upravili, přistupovat na ty webové stránky, které obsahují typ obsahu, který jste zablokovali.

Úpravy povolených a blokovaných webových stránek

Je možné povolit konkrétní weby, které jsou blokovány, a také zablokovat jednotlivé weby, které nejsou zahrnuty v žádném typu obsahu.

Můžete například usoudit, že je webová stránka bezpečná, i když jinak necháváte ostatní webové stránky se stejným typem obsahu zablokovat. Můžete rovněž zablokovat konkrétní webovou stránku, ačkoli ostatní webové stránky daného typu obsahu jsou povoleny.

Povolení nebo zablokování webu:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyBlokování obsahu**.
3. Klikněte na položku **Zobrazit povolené a zakázané webové servery**.

   Pokud je již webová stránka, kterou chcete upravit, uvedena jako povolená nebo zakázaná, a chcete ji přesunout z jednoho seznamu do druhého:

   a) Podle toho, který seznam webových stránek chcete upravit, klepněte na kartu **Povolené** nebo **Zakázané**.
   b) Klepněte pravým tlačítkem na webovou stránku v seznamu a vyberte příkaz **Povolit** nebo **Zakázat**.

   Pokud webová stránka není uvedena v žádném seznamu:

   a) Klepněte na kartu **Povolené**, chcete-li povolit webovou stránku, nebo **Zakázané**, chcete-li webovou stránku zablokovat.
   b) Klepnutím na tlačítko **Přidat** přidáte novou webovou stránku do seznamu.
   c) V dialogu **Přidat webovou stránku** zadejte adresu webu, který chcete přidat, a klepněte na tlačítko **OK**.
4. Kliknutím na tlačítko **OK** se vrátíte na hlavní stránku.

Chcete-li změnit adresu povolené nebo blokované webové stránky, klepněte pravým tlačítkem na webovou stránku v seznamu a vyberte příkaz **Upravit**.

Chcete-li odstranit povolenou nebo blokovanou webovou stránku ze seznamu, vyberte ji a klepněte na tlačítko **Odebrat**.

8.4.2 Používání funkce SafeSearch

Google, Bing a Yahoo používají filtry SafeSearch k blokování neslušného obsahu ve výsledcích vyhledávání.

Přestože funkce SafeSearch nemůže zabránit zobrazení veškerého nevhodného a neslušného obsahu ve výsledcích vyhledávání, pomůže vám vyhnout se většině tohoto materiálu.

Pomocí nastavení funkce SafeSearch v tomto produktu můžete zajistit, aby se pro podporované vyhledávače vždy používala nejpřísnější možná úroveň filtrování.

8.5 Jak naplánovat čas procházení?

Můžete stanovit čas, který uživatelé vašeho počítače mohou strávit procházením internetu.

Pro jednotlivé uživatelské účty systému Windows v počítači můžete nastavit různá omezení. Můžete řídit tyto položky:

- Kdy má uživatel povoleno procházet internet. Můžete například povolit procházení internetu pouze před 8. hodinou večer.
- Jak dlouho má uživatel povoleno procházet internet. Můžete například povolit procházení internetu pouze jednu hodinu denně.

Poznámka: Pokud odstraníte časová omezení, je procházení internetu povoleno bez jakýchkoli časových omezení.

8.5.1 Povolit procházení internetu pouze v určitých hodinách

Můžete omezit dobu, kdy je dovoleno procházet internet, nastavením doby procházení pro jednotlivé uživatelské účty systému Windows.

Nastavení dovolené doby procházení:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyČasové limity procházení webu**.
3. Klikněte na přepínač v pravém horním rohu.
4. V tabulce **Hodiny procházení** vyberte časy, kdy bude v jednotlivých dnech v týdnu povoleno procházení.
5. Vyberte počet hodin povoleného procházení ve všedních dnech a o víkendech.
   Pokud nechcete dobu dovolenou pro procházení internetu omezit, ujistěte se, že je doba procházení pro všední dny i víkendy nastavena na hodnotu **Max**.
6. Klepněte na tlačítko **OK**.

Po přihlášení k vašemu počítači mohou všichni uživatelé účtů systému Windows, které jste upravili, nyní procházet internet pouze v povolených hodinách.

8.5.2 Denní omezení doby procházení Internetu

V počítači můžete během dne nastavit různá omezení přístupu k internetu.

Pro jednotlivé uživatelské účty systému Windows v počítači můžete během dne nastavit různá omezení.

Nastavení časových omezení:

1. Na hlavní stránce vyberte uživatelský účet systému Windows, který chcete upravit, a klikněte na tlačítko **Nastavení**.
   Otevře se dialog **Nastavení**.
2. Vyberte položku **Online SafetyČasové limity procházení webu**.
3. Klikněte na přepínač v pravém horním rohu.
4. V tabulce **Hodiny procházení** vyberte časy, kdy bude v jednotlivých dnech v týdnu povoleno procházení.
   Pokud nechcete omezit procházení webu na určitou dobu, ujistěte se, že jsou zaškrtnuty všechny buňky v tabulce **Doba procházení**.
5. Vyberte počet hodin povoleného procházení ve všedních dnech a o víkendech a klikněte na tlačítko **OK**.

Po přihlášení k vašemu počítači mohou všichni uživatelé účtů systému Windows, které jste upravili, nyní procházet internet pouze v povolených hodinách.

Kapitola

9

Co je Safe Search

Témata:

Nástroj Safe Search zobrazuje zabezpečení webových serverů ve výsledcích hledání a zabraňuje neúmyslnému přístupu ke škodlivým webům.

Nástroj Safe Search zjišťuje webové servery, které obsahují hrozby zabezpečení, jako je malware (viry, červi, trojští koně), nebo se pokoušejí ukrást vaše citlivé údaje, například uživatelská jména a hesla.

9.1 Co jsou hodnocení zabezpečení

Hodnocení zabezpečení ve výsledcích hledání vám pomohou vyhnout se internetovým hrozbám.

Existují čtyři možná hodnocení zabezpečení pro webové stránky – bezpečné, podezřelé, škodlivé a neznámé. Jsou založena na informacích z několika zdrojů, například od analytiků malwaru ze společnosti F-Secure a partnerů společnosti F-Secure.

Barevně odlišené ikony udávají hodnocení bezpečnosti aktuálního webu. Hodnocení bezpečnosti jednotlivých odkazů ve výsledcích hledání je také vyznačeno stejnými ikonami:

Zelená barva udává, že pokud je nám známo, je tento server bezpečný. Na tomto webovém serveru jsme nenašli nic podezřelého.

Žlutá barva udává, že je server podezřelý. Doporučujeme, abyste byli při jeho návštěvě opatrní, nestahovali žádné soubory a neuváděli žádné osobní údaje.

Červená barva znamená, že je server škodlivý. Doporučujeme, abyste tento webový server nenavštěvovali.

Šedá barva udává, že webový server dosud nebyl analyzován a momentálně o něm nejsou k dispozici žádné informace.

9.2 Nastavení nástroje Safe Search pro webový prohlížeč

Safe Search můžete nastavit jako svůj výchozí vyhledávací nástroj ve webovém prohlížeči během instalace produktu.

Safe Search podporuje následující webové prohlížeče:

- Internet Explorer 8 pro Windows XP SP3
- Internet Explorer, dvě naposledy vydané verze pro systém Windows Vista, Windows 7 a Windows 8
- Firefox, dvě naposledy vydané verze
- Google Chrome, dvě naposledy vydané verze

9.2.1 Použití nástroje Safe Search s aplikací Internet Explorer

Nástroj Safe Search můžete nastavit jako svoji výchozí domovskou stránku a zprostředkovatele hledání a nainstalovat panel nástrojů pro vyhledávání při použití aplikace Internet Explorer.

Chcete-li používat Safe Search s aplikací Internet Explorer, postupujte podle těchto pokynů:

1. Spusťte aplikaci Internet Explorer.
2. Až Internet Explorer zobrazí zprávu, že určitý program požaduje změnu vašeho zprostředkovatele hledání, klikněte na položku **Změnit**.

   Poznámka: Tuto zprávu neuvidíte, pokud jste během instalace nevybrali jako výchozího zprostředkovatele hledání nástroj Safe Search.

3. Když se v aplikaci Internet Explorer zobrazí zpráva, že je doplněk panelu nástrojů připraven k použití, klikněte na tlačítko **Povolit**. Pokud se ale zobrazí dialog **Několik doplňků je připraveno k použití**, klikněte nejprve na tlačítko **Vybrat doplňky**.

   Poznámka: V aplikaci Internet Explorer 8 bude panel nástrojů připraven k použití automaticky.

   Poznámka: Tuto zprávu neuvidíte, pokud jste během instalace nezvolili možnost instalace panelu nástrojů pro vyhledávání.

9.2.2 Používání nástroje Safe Search s prohlížečem Firefox

Nástroj Safe Search můžete nastavit jako výchozí domovskou stránku a zprostředkovatele hledání a nainstalovat panel nástrojů pro vyhledávání při použití aplikace Firefox.

Poznámka: Pokud konfigurace prohlížeče Firefox znemožňuje změnu domovské stránky nebo zprostředkovatele hledání, nástroj Safe Search tato nastavení nemůže změnit.

Chcete-li po instalaci produktu používat panel nástrojů Safe Search s prohlížečem Firefox, postupujte podle těchto pokynů:

1. Spusťte aplikaci Firefox.
2. Otevřete kartu **Instalovat doplněk**.
3. Přesvědčte se, že je doplňkem určeným k instalaci nástroj *Safe Search*.
4. Zaškrtněte políčko **Povolit tuto instalaci**.
5. Klikněte na tlačítko **Pokračovat**.
6. Klikněte na tlačítko **Restartovat Firefox**.

9.2.3 Používání nástroje Safe Search s prohlížečem Chrome

Nástroj Safe Search můžete nastavit jako svoji výchozí domovskou stránku a zprostředkovatele hledání a nainstalovat panel nástrojů pro vyhledávání při použití aplikace Chrome.

Pokud budete používat Chrome jako výchozí prohlížeč, při instalaci produktu lze nainstalovat panel nástrojů pro vyhledávání a automaticky změnit domovskou stránku a zprostředkovatele hledání.

9.3 Odstranění nástroje Safe Search

9.3.1 Odstranění nástroje Safe Search z prohlížeče Internet Explorer

Chcete-li nástroj Safe Search v prohlížeči Internet Explorer přestat používat, postupujte podle těchto pokynů:

1. Otevřete ovládací panely systému Windows.
2. Otevřete nabídku **Síť a InternetMožnosti Internetu**.
   Zobrazí se okno **Internet – vlastnosti**.
3. Chcete-li zrušit nastavení nástroje Safe Search jako výchozí domovské stránky, postupujte podle těchto pokynů:
   a) V okně **Internet vlastnosti** otevřete kartu **Obecné**.
   b) V nabídce **Domovská stránka** klikněte na možnost **Použít výchozí**.
4. V okně **Internet – vlastnosti** otevřete kartu **Programy**.
5. Klikněte na možnost **Spravovat doplňky**.
   Otevře se okno **Spravovat doplňky**.
6. Chcete-li nástroj Safe Search přestat používat jako poskytovatele hledání, postupujte podle těchto pokynů:
   a) V okně **Spravovat doplňky** vyberte možnost **Poskytovatelé vyhledávání**.
   b) Vyberte možnost *Safe Search*.
   c) Klikněte na tlačítko **Odebrat**.
7. Chcete-li odstranit panel nástrojů Safe Search, postupujte podle těchto pokynů:
   a) V okně **Spravovat doplňky** vyberte možnost **Panely nástrojů a rozšíření**.
   b) Vyberte možnost *Safe Search*.
   c) Klikněte na možnost **Zakázat**.

Poznámka: Pokud nástroj Safe Search odinstalujete, dojde také k úplnému odsstranění vyhledávače a panelu nástrojů Safe Search.

9.3.2 Odstranění nástroje Safe Search z prohlížeče Firefox

Chcete-li nástroj Safe Search v prohlížeči Firefox přestat používat, postupujte podle těchto pokynů.

1. Chcete-li zrušit nastavení nástroje Safe Search jako výchozí domovské stránky, postupujte podle těchto pokynů:
   a) Přejděte do nabídky **NástrojeMožnosti**.
   a) V okně **Možnosti** otevřete kartu **Obecné**.
   b) Klikněte na možnost **Obnovit výchozí** pod polem **Domovská stránka**.
2. Chcete-li nástroj Safe Search přestat používat jako poskytovatele hledání, postupujte podle těchto pokynů:
   a) Kliknutím na ikonu poskytovatele hledání v poli hledání otevřete nabídku vyhledávače.
   b) Klikněte na možnost **Spravovat vyhledávače**.
   c) Vyberte možnost *Safe Search* ze seznamu a klikněte na možnost **Odebrat**.
   d) Klikněte na tlačítko **OK**.
3. Chcete-li odstranit panel nástrojů Safe Search, postupujte podle těchto pokynů:
   a) Přejděte do nabídky **NástrojeDoplňky**.
   b) V okně **Správce doplňků** otevřete kartu **Rozšíření**.
   c) Klikněte na tlačítko **Zakázat** na řádku rozšíření Safe Search.
   d) Odstranění panelu nástrojů se projeví až po restartu prohlížeče.

Poznámka: Pokud nástroj Safe Search odinstalujete, dojde také k úplnému odsstranění vyhledávače a panelu nástrojů Safe Search.

9.3.3 Odstranění nástroje Safe Search z prohlížeče Chrome

Chcete-li nástroj Safe Search v prohlížeči Chrome přestat používat, postupujte podle těchto pokynů.

1. Chcete-li zrušit nastavení nástroje Safe Search jako výchozí domovské stránky, postupujte podle těchto pokynů:
   a) Otevřete možnost **Nastavení** v nabídce prohlížeče Chrome.
   b) Vyhledejte nastavení **Při spuštění**.
   c) Klikněte na odkaz **Nastavit stránky** vedle možnosti **Otevřít konkrétní stránku nebo skupinu stránek**.
   d) Klikněte na znak **X** na konci řádku Safe Search.
2. Chcete-li nástroj Safe Search přestat používat jako poskytovatele hledání, postupujte podle těchto pokynů:
   a) Otevřete možnost **Nastavení** v nabídce prohlížeče Chrome.
   b) Vyhledejte nastavení **Vyhledávání**.
   c) Klikněte na možnost **Spravovat vyhledávače**.
   d) Klikněte na znak **X** na konci řádku Safe Search.
3. Chcete-li odstranit panel nástrojů Safe Search, postupujte podle těchto pokynů:
   a) Pravým tlačítkem myši klikněte na ikonu panelu nástrojů Safe Search.
   b) Vyberte možnost **Odstranit z prohlížeče Chrome**.

Poznámka: Pokud nástroj Safe Search odinstalujete, dojde také k úplnému odsstranění vyhledávače a panelu nástrojů Safe Search.