

F-Secure Anti-Virus 2013

Obsah

Kapitola 1: Instalace.....	5
Před první instalací.....	6
První instalace produktu.....	6
Instalace a upgrady aplikací.....	6
Nápověda a podpora.....	7
 Kapitola 2: Základní.....	 9
Používání automatických aktualizací.....	10
Kontrola stavu aktualizace.....	10
Změna nastavení připojení k Internetu.....	10
Kontrola stavu síťové ochrany v reálném čase.....	11
Zobrazení funkcí produktu.....	11
Zobrazení historie oznámení.....	11
Změna nastavení oznámení.....	11
Síťová ochrana v reálném čase.....	12
Co je Síťová ochrana v reálném čase.....	12
Výhody Síťové ochrany v reálném čase.....	12
Jakými daty přispíváte.....	13
Jak chráníme vaše soukromí.....	14
Jak se stát přispěvatelem Síťové ochrany v reálném čase.....	14
Dotazy týkající se Síťové ochrany v reálném čase.....	14
Ověření platnosti předplatného.....	15
Centrum akcí.....	15
Aktivace registrace.....	16
 Kapitola 3: Úvod.....	 17
Zobrazení celkového stavu ochrany.....	18
Zobrazení statistiky produktu.....	18
Práce s aktualizacemi produktu.....	19
Zobrazení verzí databází.....	19
Změna nastavení mobilního širokopásmového připojení.....	19
Co jsou viry a další malware?.....	20
Viry.....	20
Spyware.....	20
Rootkity.....	21
Riskware.....	21

Kapitola 4: Ochrana počítače proti malwaru.....	23
Kontrola počítače.....	24
Automatická kontrola soubor	24
Ruční kontrola soubor	26
Kontrola e-mail	29
Zobrazení výsledků kontroly.....	29
Jak vyloučit soubory z kontroly.....	30
Typy vyloučených soubor	30
Vyloučení soubor podle umístění.....	30
Zobrazení vyloučených aplikací.....	31
Jak využívat karanténu?.....	32
Zobrazení položek v karanténě	32
Obnovení položek uložených v karanténě	32
Co je DeepGuard?.....	33
Zapnutí nebo vypnutí funkce DeepGuard.....	33
Povolení aplikací, které funkce DeepGuard zablokovala.....	33
Použití funkce DeepGuard v režimu kompatibility.....	34
Co dlat při varování na podezřelé chování.....	34

Instalace

Témata:

- *Před první instalací*
- *První instalace produktu*
- *Instalace a upgrady aplikací*
- *Nápověda a podpora*


Před první instalací

Děkujeme, že jste si vybrali společnost F-Secure.

K instalaci produktu potřebujete:

- Instalační disk CD-ROM nebo instalační balíček. Používáte-li netbook bez jednotky CD, můžete si stáhnout instalační balíček z webové stránky www.f-secure.com/netbook.
- Váš registrační klíč
- Připojení k Internetu.

Máte-li k dispozici produkt zabezpečení od jiného prodejce, instalační program se ho automaticky pokusí odstranit. Pokud se tak nestane, odstraněte ho ručně.

 **Poznámka:** Pokud je v počítači více útvarů, přihlaste se před instalací pomocí útvaru s oprávněným správcem.

První instalace produktu

Pokyny k instalaci produktu.

Postupujte podle těchto pokynů k instalaci produktu:

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 poklepnutím na instalační soubor spusťte instalaci.

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 předplatného a stažením nejnovějších aktualizací z Internetu bude možná nutné restartovat počítač. Pokud instalujete z disku CD-ROM, nezapomeňte ho před restartováním počítače vyjmout z jednotky.

Instalace a upravy aplikací

Pokyny k aktivaci registrace.

Podle těchto pokynů postupujte při aktivaci nové registrace nebo při instalaci nové aplikace pomocí hlavního panelu:

 **Poznámka:** Ikony hlavního panelu naleznete na hlavním panelu systému Windows.

1. Přejděte na hlavní panel a klepnutím pravým tlačítkem na ikonu zcela vpravo. Otevře se místní nabídka.
2. Vyberte položku **Zobrazit moje registrace (View my subscriptions)**.
3. V části **Moje registrace (My subscriptions)** přejděte na stránku **Stav registrace (Subscription status)** a klepnutím na tlačítko **Aktivovat registraci (Activate subscription)**. Zobrazí se okno **Aktivovat registraci (Activate subscription)**.
4. Zadejte svůj registrační klíč pro tuto aplikaci a klepnutím na tlačítko **OK**.

5. Po ověření a aktivaci registrace klepněte na tlačítko **Zavít (Close)**.
6. V části **Moje registrace (My subscriptions)** přejděte na stránku **Stav instalace (Installation status)**.
Pokud se instalace nespustí automaticky, postupujte podle těchto pokynů:
 - a) Klepněte na tlačítko **Instalovat (Install)**.
Zobrazí se okno instalace.
 - b) Klepněte na tlačítko **Další**.
Aplikace se stáhne a spustí se instalace.
 - c) Po dokončení instalace klepněte na tlačítko **Zavít (Close)**.

Tím byla aktivována nová registrace.

Nápověda a podpora

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

Po zaregistrování licence máte nárok na další služby, jako jsou bezplatné aktualizace a podpora produktu. Registraci lze provést na stránkách www.f-secure.com/register.

Za ináme

Témata:

- *Používání automatických aktualizací*
- *Zobrazení inností produktu*
- *Sí ochrany v reálném ase*
- *Ov ení platnosti p edplatného*

Informace o tom, jak za ít s produktem pracovat.

V této ásti je popsán postup p i zm n spole ných nastavení a správ registrací prost ednictvím hlavního panelu.

Spole ná nastavení jsou ta, která platí pro všechny programy nainstalované na hlavním panelu. Namísto zm n samostatných nastavení v jednotlivých programech m žete jednoduše upravit spole ná nastavení, která jsou pak využívána ve všech nainstalovaných programech.

Mezi spole ná nastavení hlavního panelu pat í:

- Stahování, kde m žete vid t informace o stažených aktualizacích a ru n kontrolovat, zda jsou k dispozici nové aktualizace.
- Nastavení p ipojení, kde lze zm nit zp sob p ipojení po íta e k Internetu.
- Oznámení, kde m žete vid t minulá oznámení a nastavit druh oznámení, která chcete zobrazit.
- Nastavení ochrany osobních dat, kde m žete vybrat, zda se po íta m že p ipojit k síti ochrany v reálném ase.

Pomocí hlavního panelu lze také spravovat registrace nainstalovaných program .

Používání automatických aktualizací

Automatické aktualizace slouží k udržování ochrany v po íta i v aktuálním stavu.

Je-li po íta p ípojen k Internetu, agent automatické aktualizace F-Secure do n j stahuje nejnov jší aktualizace. Zjiš uje p enosy v síti a neomezuje práci s Internetem ani u pomalého p ípojení.


Kontrola stavu aktualizace

Zobrazuje datum a as poslední aktualizace.

Jsou-li zapnuty automatické aktualizace, produkt v dob p ípojení k Internetu automaticky p íjímá nejnov jší aktualizace.

Ov ení instalace nejnov jších aktualizací:



1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo. Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Automatické aktualizace > Stahování**.
4. Klepn te na položku **Ov ít nyní**.
Produkt se p ípojí k Internetu a vyhledá nejnov jší aktualizace. Není-li ochrana aktuální, stáhne nejnov jší aktualizace.

 **Poznamka:** Používáte-li modem nebo máte p ípojení ISDN, je ke kontrole aktualizací pot eba, aby bylo p ípojení aktivní.

Zm na nastavení p ípojení k Internetu

Obvykle není t eba m nit výchozí nastavení, ale m žete nakonfigurovat p ípojení vašeho serveru k internetu tak, abyste mohli p íjímat aktualizace automaticky.

Zm na nastavení p ípojení k Internetu:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo. Zobrazí se místní nabídka.
2. Vyberte p íkaz **Otev ít spole ná nastavení**.
3. Klepn te na položku **Automatické aktualizace > P ípojení**.
4. V seznamu **P ípojení k Internetu** vyberte zp sob p ípojení po íta e k Internetu.
 - Máte-li k dispozici nep etržené sí ové p ípojení, vyberte možnost **P edpokládat nep etržené p ípojení**.
 **Poznamka:** Nemá-li po íta trvalé sí ové p ípojení a je nastaveno vytá ení na vyžádání, výb r možnosti **P edpokládat nep etržené p ípojení** m že vést k opakovanému vytá ení.
 - Vybráním možnosti **Rozpoznat p ípojení** se budou aktualizace stahovat, pouze pokud produkt zjistí aktivní sí ové p ípojení.
 - Vybráním možnosti **Rozpoznat p enos** se budou aktualizace stahovat, pouze pokud produkt zjistí jiný sí ový p enos.
 **Tip:** Máte-li neobvyklou hardwarovou konfiguraci, která zp sobuje, že nastavení **Rozpoznat p ípojení** zjistí aktivní p enos v síti, i když žádný p enos neprobíhá, zm te nastavení na možnost **Zjistit p enosy**.

5. V seznamu **Server proxy HTTP** vyberte, zda po íta používá p ípojení k internetu *server proxy*.

- Je-li po íta p ípojen k internetu p ímo, klepn te na p epína [Bez serveru proxy HTTP](#).
- Chcete-li nakonfigurovat nastavení *serveru proxy HTTP*, klepn te na p epína [Ru n konfigurovat server HTTP proxy](#).
- Chcete-li použít stejné nastavení *serveru proxy HTTP*, jaké jste nakonfigurovali ve webovém prohlíže i, vyberte možnost [Použít server proxy HTTP mého prohlíže e](#).

Kontrola stavu síť ochrany v reálném ase

Na p ípojení síť ochrany v reálném ase závisí správná funkce mnoha funkcí produktu.

Jestliže dochází k problém m se sítí nebo pokud brána firewall blokuje p enos síť ochrany v reálném ase, bude stav Odpojeno. Pokud nejsou nainstalovány žádné funkce produktu, které by vyžadovaly p ístup k síti ochrany v reálném ase, bude stav Nepoužíváno.

Kontrola stavu:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo. Zobrazí se místní nabídka.
2. Vyberte p íkaz [Otev ít společná nastavení](#).
3. Klepn te na položku [Automatické aktualizace](#) > [P ípojení](#).

V ásti [Síť ochrany v reálném ase](#) se zobrazí aktuální stav síť ochrany v reálném ase.

Zobrazení inností produktu

Akce, které byly provedeny za ú elem ochrany po íta e, m žete vid t na stránce [Oznámení](#).

Produkt zobrazí oznámení, když provede ur ítou akci, nap . zjistí virus, který zablokuje. N která oznámení m že také zasílat p íslušný poskytovatel služeb, nap . aby vás informoval o dostupnosti nových služeb.

Zobrazení historie oznámení

Oznámení, která byla zobrazena, m žete vid t v historii oznámení.

Zobrazení historie oznámení:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo. Zobrazí se místní nabídka.
2. Vyberte p íkaz [Otev ít společná nastavení](#).
3. Klepn te na položku [Jiné](#) > [Oznámení](#).
4. Klepn te na položku [Zobrazit historii oznámení](#). Zobrazí se seznam historie oznámení.

Zm na nastavení oznámení

M žete si vybrat typ oznámení, která má produkt zobrazovat.

Zm na nastavení oznámení:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo. Zobrazí se místní nabídka.
2. Vyberte p íkaz [Otev ít společná nastavení](#).
3. Klepn te na položku [Jiné](#) > [Oznámení](#).
4. Výb rem nebo zrušením výb ru 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. Klepnutím na tlačítko **OK**.

Sí ochrany v reálném ase

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

Co je Sí ochrany v reálném ase

Sí ochrany v reálném ase je online služba, která poskytuje rychlou odpověď proti internetovým hrozbám.

Jako poskyvatel do Sí ochrany v reálném ase nám můžete pomoci posílit ochranu proti novým hrozbám. Sí ochrany v reálném ase shromažďuje statistiky o určitých neznámých, škodlivých nebo podezřelých aplikacích a o tom, co mohou poškodit vaše počítače. Tyto informace jsou anonymní a jsou zasílány společnosti F-Secure Corporation, která provádí hromadnou analýzu shromážděných dat. Analyzované informace používáme pro vylepšení zabezpečení vašeho počítače proti nejnovějším hrozbám a škodlivým souborům.

Jak funguje Sí ochrany v reálném ase

Jako poskyvatel do Sí ochrany v reálném ase můžete poskytovat informace o neznámých aplikacích a webových stránkách a o škodlivých aplikacích na nich. Sí ochrany v reálném ase nesleduje vaši činnost na webu ani neshromažďuje informace o webových stránkách, které již byly analyzovány. Rovněž neshromažďuje informace o stejných aplikacích, které byly na vašem počítači nainstalovány.

Pokud nechcete tato data poskytovat, Sí ochrany v reálném ase údaje o instalovaných aplikacích ani navštívených webových stránkách shromažďovat nebude. Avšak produkt se musí dotazovat server F-Secure na povolení aplikací, webových stránek, sdílení a dalších objektů. Dotazy se prostřednictvím kryptografického kontrolního součtu, pomocí kterého dotazovaný objekt sám se F-Secure nezasílá. Nesledujeme data podle uživatele, pouze se zvyšuje hodnota počítačového vstupu do souboru nebo na webovou stránku.

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

Výhody Sí ochrany v reálném ase

Se Síťí ochrany v reálném ase získáte rychlejší a přesnější ochranu proti nejnovějším hrozbám a nebudete dostávat zbytečné upozornění na podezřelé aplikace, které nejsou škodlivé.

Jako poskyvatel do Sí ochrany v reálném ase nám můžete pomoci nacházet nový dosud nezjištěný malware a odstraňovat případná falešná pozitiva z naší databáze virů.

Všichni účastníci Sí ochrany v reálném ase si navzájem pomáhají. Když Sí ochrany v reálném ase najde ve vašem zařízení podezřelou aplikaci, můžete využívat výsledky analýzy, pokud již byla stejná aplikace nalezena v jiných zařízeních. Sí ochrany v reálném ase zlepšuje celkový výkon vašeho zařízení, protože nainstalovaný bezpečnostní produkt nemusí kontrolovat aplikace, které již Sí ochrany v reálném ase analyzovala a zjistila, že jsou nezávadné. Podobně jsou prostřednictvím Sí ochrany v reálném ase sdíleny informace o škodlivých webových stránkách a nevyžádaných hromadných zprávách a jsme schopni vám poskytovat účinnější ochranu před prostředky zneužití webových stránek a před nevyžádanými zprávami.

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

Jakými daty p íspíváte

Jako p íspívatel do Sít ochrany v reálném ase poskytujete informace o aplikacích uložených na vašem počítači a webových stránkách, které navštívíte, aby vás Sít ochrany v reálném ase mohla ochránit proti nejnovějším škodlivým aplikacím a podezřelým webovým stránkám.

Analýza pov sti souboru

Sít ochrany v reálném ase shromažďuje pouze informace o aplikacích, jejichž pov st není známa a o souborech, které jsou podezřelé nebo se o nich ví, že jsou škodlivé.

Sít ochrany v reálném ase shromažďuje anonymní informace o nezávadných a podezřelých aplikacích ve vašem zařízení. Sít ochrany v reálném ase shromažďuje pouze informace o spustitelných souborech (jako jsou p enosné spustitelné soubory v platform Windows, které mají p ípony CPL, EXE, DLL, OCX, SYS, SCR a DRV).

Shromážděné informace obsahují:

- cestu k umístění, v níž se nachází aplikace ve vašem zařízení,
- velikost souboru a dobu jeho vytvoření nebo změny,
- atributy a oprávnění souboru,
- informace o podpisu souboru,
- aktuální verzi souboru a společnost, která jej vytvořila,
- p vod souboru nebo adresu URL, odkud byl stažen,
- výsledky analýzy aplikace F-Secure DeepGuard a antivirového programu kontrolovaných souborů a
- další podobné informace.

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

Prostřednictvím Sít ochrany v reálném ase můžete rovněž odesílat podezřelé aplikace k analýze. Aplikace, které zašlete, musí být výhradně typu p enosného spustitelného souboru. Sít ochrany v reálném ase nikdy neshromažďuje informace o vašich osobních dokumentech a rovněž je nikdy automaticky nezasílá k analýze.

Odeslání souborů k analýze

Pomocí sít ochrany v reálném ase můžete také odesílat podezřelé aplikace k analýze.


Jednotlivé podezřelé aplikace můžete odeslat ručně, když vás k tomu produkt vyzve. Odesílat lze pouze p enosné spustitelné soubory. Sít ochrany v reálném ase v žádném případě nenahrává osobní dokumenty.

Analýza pov sti webové stránky

Sít ochrany v reálném ase nesleduje vaši webovou aktivitu ani neshromažďuje informace o webových stránkách, které již byly analyzovány. Kontroluje, zda jsou vámi navštívené webové stránky bezpečné. Když navštívíte webovou stránku, zkontroluje Sít ochrany v reálném ase její bezpečnost a upozorní vás, když je tato stránka hodnocena jako podezřelá nebo škodlivá.

Pokud webová stránka, kterou navštívíte, obsahuje škodlivý nebo podezřelý obsah nebo je známa jako prostředek ke zneužití, Sít ochrany v reálném ase zaznamená celou URL adresu stránky, aby bylo možno analyzovat její obsah.

Pokud navštívíte stránku, která zatím nebyla hodnocena, Sít ochrany v reálném ase zaznamená názvy domén a poddomén a v níž kterých p ípadech i cestu k navštívené stránce, aby bylo možno ji analyzovat a vyhodnotit. Všechny parametry URL, které by mohly obsahovat informace, které by mohly být jakýmkoli způsobem spojovány s vámi a mohly by vás osobně identifikovat, budou pro ochranu vašeho soukromí odstraněny.

 **Poznámka:** Sí ochrany v reálném ase nehodnotí ani neanalyzuje webové stránky v soukromých sítích, takže nikdy nebude zaznamenávat žádné informace z IP adres v soukromých sítích (například v podnikových intranetech).

Analýza systémových informací

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

Jak chráníme vaše soukromí

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

Sí ochrany v reálném ase odstraní identifikační údaje před odesláním do F-Secure a šifruje všechny shromážděné informace pro přenos, aby je chránila před neoprávněným přístupem. Shromážděné informace se nezpracovávají individuálně, spojují se s informacemi od jiných poskytovatelů Sí ochrany v reálném ase. Všechna data jsou analyzována statisticky a anonymně, což znamená, že podle žádných dat nebude možno identifikovat vaši osobu.

Žádné informace, které by vás mohly identifikovat, se ve shromážděných datech nenacházejí. Sí ochrany v reálném ase neshromažďuje adresy IP ani žádné jiné soukromé informace, jako jsou e-mailové adresy, uživatelská jména a hesla. A když 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 zstanou. V takových případech nebudeme takto neúmyslně shromážděná data používat k vaší identifikaci.

Uplatníme přísná bezpečnostní opatření a fyzické, administrativní a technické ochranné prostředky, abychom ochránili shromážděné informace před 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 partnery, subdodavateli, distributory a partnery, ale pouze v anonymním formátu, aby nemohla sloužit k identifikaci.

Jak se stát poskytovatelem Sí ochrany v reálném ase

Můžete nám pomoci vylepšovat provoz Sí ochrany v reálném ase tak, že budete poskytovat informacemi o škodlivých programech a webových stránkách.

Během instalace se můžete rozhodnout, zda se stanete poskytovatelem Sí ochrany v reálném ase.

Přednastaveno je, že se poskytovatelem stanete a budete do Sí ochrany v reálném ase poskytovat svými informacemi. Toto nastavení můžete kdykoliv později změnit.

Chcete-li změnit nastavení Sí ochrany v reálném ase, 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 **Jiné > Ochrana osobních dat**.
4. Zatrhněte políčko uastníka a stanete se poskytovatelem Sí ochrany v reálném ase.

Dotazy týkající se Sí ochrany v reálném ase

Kontaktní informace pro jakékoli dotazy týkající se Sí ochrany v reálném ase.

Máte-li jakékoli dotazy týkající se Sí ochrany v reálném ase, 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

Nejnov jší verze t chto zásad je vždy k dispozici na našem webu.

Ov ení platnosti p edplatného


Typ a stav vaší registrace se zobrazí na stránce **Stav registrace**.

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

Kontrola platnosti p edplatného:

1. P ejd te na hlavní panel a klepn te pravým tla ítkem na ikonu zcela vpravo.
Zobrazí se místní nabídka.
2. Vyberte p íkaz **Zobrazit moje registrace**.
3. Klepnutím na položku **Stav registrace** zobrazíte informace o registracích nainstalovaných program .
4. Výb rem možnosti **Stav instalace** zobrazíte programy, které jsou k dispozici pro instalaci.

Stav registrace a datum vypršení platnosti se zobrazí také na stránce **Statistika** p íslušného programu. Pokud platnost registrace vypršela, bude nutné registraci obnovit, aby bylo možné i nadále získávat aktualizace a používat produkt.


 **Poznámka:** Ikona stavu produktu na hlavním panelu po vypršení platnosti p edplatného bliká.

Centrum akcí

V centru akcí se zobrazují veškerá d ležitá upozorn ní, která vyžadují vaši pozornost.

Pokud vypršela nebo brzy vyprší platnost vaší registrace, centrum akcí vás na to upozorní. Barva pozadí a obsah zprávy centra akcí závisí na typu a stavu registrace:


- Jestliže se blíží konec platnosti vaší registrace a jsou k dispozici bezplatné registrace, zpráva má bílé pozadí a obsahuje tla ítko **Aktivovat (Activate)**.
- Jestliže se blíží konec platnosti vaší registrace a nejsou k dispozici bezplatné registrace, zpráva má žluté pozadí a obsahuje tla ítko **Koupit (Buy)** a **Zadat klí (Enter key)**. Pokud jste již zakoupili novou registraci, m žete klepnout na tla ítko **Zadat klí (Enter key)**, zadat registra ní klí a novou registraci aktivovat.
- Pokud vypršela platnost vaší registrace a jsou k dispozici bezplatné registrace, zpráva má červené pozadí a obsahuje tla ítko **Aktivovat (Activate)**.
- Jestliže vypršela platnost vaší registrace a nejsou k dispozici bezplatné registrace, zpráva má červené pozadí a obsahuje tla ítko **Koupit (Buy)** a **Zadat klí (Enter key)**. Pokud jste již zakoupili novou registraci, m žete klepnout na tla ítko **Zadat klí (Enter key)**, zadat registra ní klí a novou registraci aktivovat.

 **Poznámka:** Klepnutím na odkaz **Zobrazit historii upozorn ní (Show notification history)** v centru akcí zobrazíte seznam upozorn ní produktu, nikoli d ív jší zprávy centra akcí.

Aktivace registrace

Když vlastníte nový registra ní klí nebo kód kampan pro produkt, musíte ho aktivovat.

Aktivace registrace:

1. P ejd te na hlavní panel a klepn te pravým tlačítkem na ikonu zcela vpravo.
Zobrazí se místní nabídka.
2. Vyberte p íkaz **Zobrazit moje registrace**.
3. Vyberte jednu z možností:
 - Klepn te na položku **Aktivovat registraci**.
 - Klepn te na položku **Aktivovat kód kampan**.
4. V dialogovém okně, které se otev ě, zadejte nový registra ní klí nebo kód kampan a klepn te na tlačítko **OK**.
 **Tip:** Pokud jste obdrželi registra ní klí e-mailem, můžete ho zkopírovat z e-mailové zprávy a vložit ho do tohoto pole.

Po zadání nového registra ního klí e se na stránce **Stav registrace** zobrazí nové datum platnosti registrace.

Úvod

Témata:

- *Zobrazení celkového stavu ochrany*
- *Zobrazení statistiky produktu*
- *Práce s aktualizacemi produktu*
- *Co jsou viry a další malware?*

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

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

Zobrazení celkového stavu ochrany






Stránka **Stav** zobrazuje rychlý přehled funkcí instalovaného produktu a jejich aktuální stav.

Otevření stránky **Stav**:

Přejďte na hlavní stránku a klepněte na položku **Stav**.

Otevře se stránka **Stav**.

Ikony zobrazují stav programu a jeho bezpečnostních funkcí.

Ikona stavu	Název stavu	Popis
	OK	Váš počítač je chráněn. Funkce je zapnutá a pracuje správně.
	Informace	Produkt vás informuje o zvláštním stavu funkce. Například probíhá aktualizace funkce.
	Varování	Váš počítač není plně chráněn. Například je možné, že produkt nebyl delší dobu aktualizován nebo stav funkce vyžaduje vaši pozornost.
	Chyba	Váš počítač není chráněn. Například vaše registrace vypršela nebo je vypnuta důležitá funkce.
	Vypnuto	Nekritická funkce je vypnutá.

Zobrazení statistiky produktu

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

Zobrazení stránky **Statistika**:

Přejďte na hlavní stránku a klepněte na položku **Statistika**.

Zobrazí se stránka **Statistika**.

- **Poslední úspěšná kontrola aktualizace** zobrazuje čas poslední aktualizace.
- **Kontrola virů a spywaru** zobrazuje kolik souborů produkt od své instalace kontroloval a vyistil.
- Položka **Aplikace** zobrazuje počet programů, které aplikace DeepGuard od své instalace povolila nebo zablokovala.
- V části **Připojení brány firewall** je uveden počet povolených a blokových připojení od instalace.

- část **Filtrování nevyžádané pošty a phishingu** uvádí, kolik e-mailových zpráv produkt označil jako platné e-mailové zprávy a kolik jako nevyžádanou poštu.

Práce s aktualizacemi produktu

Produkt ochranu aktualizuje automaticky.

Zobrazení verzí databází

čas a číslo verze poslední aktualizace se zobrazuje na stránce **Aktualizace databáze**.

Otevření stránky **Aktualizace databáze**:

1. Klepnutím na hlavní stránce na možnost **Nastavení**.


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

2. Vyberte položky **Jiná nastavení** > **Verze 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 možnost je dostupná pouze v operačním systému Microsoft Windows 7.

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

 **Poznámka:** Toto nastavení platí pouze pro mobilní širokopásmové připojení. Pokud je pořízeno připojení k pevné i bezdrátové síti, produkt je automaticky aktualizován.

Chcete-li změnit nastavení:

1. Klepnutím na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte položky **Jiná nastavení** > **Mobilní širokopásmové** > **Stáhnout bezpevnostní aktualizace**.
3. Vyberte preferovanou možnost aktualizací pro mobilní připojení:

- **Pouze v domácí síti 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 pořízené 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 určitých operátorů, například v různých zemích, se mohou lišit. Toto nastavení můžete ponechat, abyste své návštěvy bez zbytečných, chcete-li ušetřit šířku pásma a případně náklady. Pokud však chcete nastavení změnit, klepněte na odkaz **Změnit**.



Poznámka:

Tato možnost je dostupná pouze v operačním systému Microsoft Windows 7.

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 šíří. Může mít například 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 mít 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 uživatele.

Spyware může shromažďovat například následující osobní údaje:

- navštívené internetové servery,
- e-mailové adresy uložené v počítači,
- hesla,

- ísla platebních karet.

Spyware se téměř vždy instaluje bez výslovného souhlasu uživatele. Spyware může být nainstalován spolu s užitečným programem, nebo když podvodník vám je ke klepnutí na volbu v zavádějícím 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 rootkitu, *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, například 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.

Ochrana počítače proti malwaru

Témata:

- [Kontrola počítače](#)
- [Jak vyloučit soubory z kontroly](#)
- [Jak využívat karanténu?](#)
- [Co je DeepGuard?](#)

Kontrola virů a spywaru chrání počítač před programy, které mohou ukrást osobní informace, poškodit váš počítač nebo ho použít k nezákonným účelům.

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

Dle výchozího nastavení prohledává kontrola virů a spywaru vaše lokální disky, všechna výmenná média (jako jsou přenosné jednotky a kompaktní disky) a stažený obsah automaticky. Můžete také nastavit automatickou kontrolu e-mailů.

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*.

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.

Doporučíme 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.

Automatická kontrola souborů

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


Pokud se počítač pokusí o přístup k souboru, kontrola v reálném čase soubor zkontroluje na malware, než počítač umožní přístup k souboru. Pokud funkce kontroly v reálném čase zjistí jakýkoli škodlivý obsah, uložit soubor do karantény, aby nemohl způsobit žádné škody.

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 využitých 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 souasně 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. Přejděte na hlavní stránku a klepněte na položku **Stav**.
2. Klepněte na položku **Změnit nastavení na této stránce**.

 **Poznámka:** Vypnutí bezpečnostních funkcí vyžaduje oprávnění správce.

3. Zapněte nebo vypněte **kontrolu virů a spywaru**.
4. Klepněte na položku **Zavít**.

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. Klepněte na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte možnost **Zabezpečení počítače > Hledání virů a spywaru**.
3. Vyberte možnost **Automaticky vyšetřovat škodlivé soubory**.

Pokud vyberete, že se škodlivé soubory nemají vyšetřovat automaticky, kontrola v reálném čase se vás zeptá, co chcete dělat s každým škodlivým souborem.

vyšetřování 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 pro vyšetřování spywaru:

Zvolená akce	Akce provedená se spywarem
Zpracovat automaticky	Nechte produkt rozhodnout, jaká je nejvhodnější akce pro vyšetřování 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	Umožněte spuštění spywaru a jeho vyloučení z kontrol v budoucnu.

vyšetřování 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 pro vyšetřování 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	Umožněte 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 vypnete stopovací soubory cookie v počítači.

1. Klepněte na hlavní stránce na možnost **Nastavení**.

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

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

Ruční kontrola souborů

Soubory lze zkontrolovat ručně, například pokud chcete pokračovat v instalaci a 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:

1. Na hlavní stránce klepněte na šipku pod položkou **Kontrola**.
Zobrazí se možnosti kontroly.
2. Vyberte typ kontroly.
Výběrem možnosti **Zmírnit nastavení kontroly** optimalizujete ruční kontrolu počítače pro hledání virů a dalších škodlivých aplikací.
3. Pokud 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 umožní 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 potenciálně nebezpečných zdrojů, jako jsou sítě P2P (peer-to-peer). Úspornost kontroly bude záviset na velikosti cíle, který kontrolujete. Kontrola proběhne rychle, pokud například kontrolujete složku, která obsahuje pouze malé množství menších souborů.
Kontrola přítomnosti rootkitu	Důležitá část systému, v nichž by podezřelá položka mohla způsobit bezpečnostní problémy. Kontroluje skryté soubory, složky, jednotky nebo procesy	Máte-li podezření, že je ve vašem počítači nainstalován rootkit. Pokud byl například nedávno v počítači zjištěn malware a chcete se ujistit, že nenainstaloval žádný rootkit.

Kontrola v programu Průzkumník Windows

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

Kontrola disku, složky nebo souboru:

1. Umístíte ukazatel myši na disk, složku nebo soubor, který chcete zkontrolovat, a klepnete 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 souboru ke kontrole

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

1. Klepnete na hlavní stránce na možnost **Nastavení**.

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

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

Zkontrolovat pouze známé typy souborů


Kontrola pouze těchto typů souborů, u nichž je nejvyšší pravděpodobnost infekce, například spustitelných souborů. Výběrem této možnosti kontrolu také zrychlí. Kontrolují se soubory s těmito 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 a .hqx.

Zkontrolovat obsah komprimovaných souborů


Kontrola archivovaných souborů a složek.

Použít pokročilou 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. Klepnete na tlačítko **OK**.

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

Co dále zjistit škodlivých souborů



Vyberte, jak chcete naložit se zjištěnými škodlivými soubory.


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

1. Klepnete na hlavní stránce na možnost **Nastavení**.

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

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

Možnost	Popis
Dotázat se (výchozí)	Můžete vybrat akci, která má být provedena, pro všechny položky zjištěné během ručního prověření.
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 prověření.
Pouze ohlásit	Produkt ponechá beze změny všechny škodlivé soubory, které byly nalezeny během ručního prověření, 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. Klepněte na hlavní stránce na možnost **Nastavení**.

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

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

Možnost	Popis
Denně	Hledání se bude opakovat každý den.
Týdn	Počítač bude prověřován ve vybrané dny v týdnu. Vyberte dny ze seznamu.
Měsíčně	Počítač bude prověřován ve vybrané dny v měsíci. Chcete-li vybrat dny: <ol style="list-style-type: none"> 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

as spuštění

Po neinnosti počítače po dobu

Popis

Hledání se spustí ve vybraný as.

Hledání se spustí po určité době neinnosti počítače.

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

Kontrola e-mail

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

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

Postup zapnutí kontroly e-mailu:

1. Klepněte na hlavní stránce na možnost **Nastavení**.

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


2. Vyberte možnost **Zabezpečení počítače > Hledání 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 umožňuje 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. Provuje 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 přístroje. Kontrola v reálném čase neprovuje připojené soubory, pokud přílohu neotevřete. To znamená, že pokud používáte webovou poštu a zprávu přepošlete před otevřením této přílohy, můžete přístrojem přeposlát nakažený e-mail.

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. Klepněte na hlavní stránce na možnost **Nastavení**.

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


2. Vyberte možnost **Zabezpečení počítače > Hledání 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.

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 takéž nevyloučíte.

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. Klepněte na hlavní stránce na možnost **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 počítače** > **Hledání virů a spywaru** lze z kontroly v reálném čase vyloučit určitý typ souborů.
- Výběrem položek **Jiná nastavení** > **Ruční kontrola** lze z kontroly v reálném čase vyloučit určitý typ souborů.

3. Klikněte na možnost **Vyloučit soubory z kontroly**.

4. Postup vyloučení typu souborů:

- 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** zavěte dialog **Vyloučit z kontroly**.

7. Chcete-li použít nové nastavení, klepněte na tlačítko **OK**.

Vybrané typy souborů budou vyloučeny z příštích kontrol.

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. Klepněte na hlavní stránce na možnost **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 **Pořadí** > **Kontrola virů a spywaru** vyloučíte umístění z kontroly v reálném čase.
- Výběrem položek **Pořadí** > **Ruční kontrola** vyloučíte umístění z ruční kontroly.

3. Klepněte na možnost **Vyloučit soubory z kontroly**.

4. Postup vyloučení souboru, jednotky nebo složky:

- Přejděte na kartu **Objekty**.
- Vyberte položku **Vyloučit objekty (soubory, složky, ...)**.
- Klepněte na tlačítko **Přidat**.
- Vyberte soubor, jednotku nebo složku, které chcete vyloučit z kontroly výskytu virů.

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

- Klepněte na tlačítko **OK**.

5. Opakujte předchozí krok pro vyloučení dalších souborů, jednotek nebo složek z kontroly výskytu virů.

6. Klepnutím na tlačítko **OK** zavěte dialog **Vyloučit z kontroly**.

7. Klepnutím na tlačítko **OK** použijte nová nastavení.

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

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 váš 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. Klepněte na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte, zda chcete zobrazit aplikace, které byly vyloučeny z kontroly v reálném čase nebo z ruční kontroly:

- Výběrem položek **Pořadí** > **Kontrola virů a spywaru** zobrazíte aplikace, které byly z kontroly v reálném čase vyloučeny.
- Výběrem položek **Pořadí** > **Ruční 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 provést:

- Vyberte aplikaci, kterou chcete zahrnout do kontroly.
- Klepněte na tlačítko **Odstranit**.

6. Klepnutím na tlačítko **OK** dialog **Vyloučit z kontroly** zavěte.
7. Klepnutím na tlačítko **OK** dialog zavěte.

Jak využívat karanténu?

Karanténa slouží jako úložiště potenciálně 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.

Zobrazení položek v karanténě

Můžete zobrazit další informace o položkách v karanténě.

Zobrazení podrobných informací o položkách v karanténě:

1. Klepněte na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte možnost **Zabezpečení počítače > Hledání 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 filtrovat 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**.

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. Klepněte na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte možnost **Zabezpečení počítače** > **Hledání virů a spywaru**.
3. Klikněte na možnost **Zobrazit karanténu**.
4. Vyberte položku karantény, kterou chcete obnovit.
5. Klepněte na položku **Obnovit**.

Co je DeepGuard?

Funkce DeepGuard analyzuje obsah souborů a chování aplikací a monitoruje aplikace, které nejsou dříve ryhodné.

Funkce DeepGuard blokuje nové a neznámé viry, červy a jiné nebezpečné aplikace, které se snaží provést změny ve vašem počítači, a zabráňuje podezřelým aplikacím v přístupu na Internet.

Když funkce DeepGuard zjistí novou aplikaci, která se snaží provést potenciálně škodlivé změny v systému, umožní spuštění aplikace v bezpečné zóně. V bezpečné zóně nemůže aplikace poškodit. Funkce DeepGuard analyzuje, jaké změny se aplikace snaží provést, a na základě toho rozhodne, s jakou pravděpodobností se jedná o *malwarovou* aplikaci. Pokud je aplikace pravděpodobně *malwarová*, funkce DeepGuard ji zablokuje.

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

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


Zapnutí nebo vypnutí funkce DeepGuard

Ponechte funkci DeepGuard zapnutou, aby mohla bránit podezřelým aplikacím v provádění potenciálně škodlivých změn v systému v počítači.

Pokud máte systém Windows XP, ujistěte se, že máte nainstalovanou aktualizaci Service Pack 2, než funkci DeepGuard zapnete.

Zapnutí nebo vypnutí funkce DeepGuard:

1. Přejděte na hlavní stránku a klepněte na položku **Stav**.
2. Klepněte na položku **Změnit nastavení na této stránce**.

 **Poznámka:** Vypnutí bezpečních funkcí vyžaduje oprávnění správce.

3. Zapiňte nebo vypněte funkci **DeepGuard**.
4. Klepněte na položku **Zavírat**.


Povolení aplikací, které funkce DeepGuard zablokovala

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

Někdy 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 v 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 hlavní stránce klepněte na možnost **Nástroje**.
2. Klepněte na položku **Aplikace**.
Zobrazí se seznam **Monitorované aplikace**.
3. Vyhledejte aplikaci, kterou chcete povolit.

 **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.

4. Vyberte možnost **Povolit** ve sloupci **Povolení**.
5. Klepněte na položku **Zavít**.

Funkce DeepGuard umožní aplikaci znovu provést změny systému.

Použití funkce DeepGuard v režimu kompatibility

Aby byla zajištěna maximální ochrana, funkce DeepGuard dočasně nespustí programy, na které programy kontrolují, zda nejsou poškozeny nebo změněny, a nemusí být s touto funkcí kompatibilní. Například online hry s anti-cheatingovými nástroji kontrolují, zda nebyly nějak upraveny, při jejich spuštění. V těchto případech můžete zapnout režim kompatibility.

Zapnutí režimu kompatibility:

1. Klepněte na hlavní stránce na možnost **Nastavení**.

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

2. Vyberte možnost **Zabezpečení počítače > DeepGuard**.
3. Vyberte možnost **Použít režim kompatibility**.
4. Klepněte na tlačítko **OK**.

Co dlat při varování na podezřelé chování

Funkce DeepGuard monitoruje aplikace, které nejsou dříve rozhodné. Pokud se monitorovaná aplikace pokusí připojit k Internetu, provést změny ve vašem počítači nebo se chová podezřele, funkce DeepGuard ji zablokuje.

Pokud jste v nastavení funkce DeepGuard vybrali možnost **Varovat na podezřelé chování**, funkce DeepGuard vás upozorní, když zjistí potenciálně škodlivou aplikaci nebo když spustíte aplikaci s neznámou pověstí.

Chcete-li se rozhodnout, co se má provést s aplikací, kterou funkce DeepGuard zablokovala:

1. Klepnutím na možnost **Podrobnosti** zobrazíte další informace o programu.
V podrobnostech jsou uvedeny následující informace:
 - umístění aplikace,
 - pověst aplikace v síti s ochranou v reálném čase,
 - jak chová aplikace.
2. Rozhodněte se, zda je možné aplikaci, kterou funkce DeepGuard zablokovala, povolit:
 - Vyberte možnost **Aplikaci vím. 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 nevím. Je třeba ji ponechat blokovanou.**, chcete-li aplikaci nadále blokovat.
Aplikace je pravděpodobně nebezpečná, pokud:
 - Aplikace není příliš známá.
 - Pověst aplikace není známa.
 - Aplikaci neznáte.

3. Chcete-li odeslat podezřelou aplikaci k analýze:

a) Klepněte na možnost **Nahlásit aplikaci společnosti F-Secure**.

Produkt zobrazí podmínky odeslání.

b) Klepněte na možnost **Přijmout**, pokud s podmínkami souhlasíte a chcete vzorek odeslat.

Vzorek doporučíme odeslat v následujících případech:

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

