F-Secure Internet Security 2013

Inhalt

Kapitel 1: Installation.....5

Vor der Erstinstallation.....6
Erstinstallation des Produkts.....6
Anwendungen installieren und aktualisieren.....6
Hilfe und Support.....7

Kapitel 2: Einstieg.....9

Verwendung von Automatische Updates.....10
Den Update-Status überprüfen.....10
Ändern der Einstellungen für die Internetverbindung.....10
Prüfen Sie den Status des Echtzeit-Schutznetzwerks.....11
Wie erkennt man, was das Produkt geleistet hat?.....11
Benachrichtigungsverlauf anzeigen.....11
Benachrichtigungseinstellungen ändern.....11
Echtzeit-Schutznetzwerk.....12
Was ist das Echtzeit-Schutznetzwerk?.....12
Die Vorteile des Echtzeit-Schutznetzwerks.....12
Welche Daten steuern Sie bei?.....13
So schützen wir Ihre Daten.....14
Werden Sie Teilnehmer am Echtzeit-Schutznetzwerk!.....14
Fragen zum Echtzeit-Schutznetzwerk.....15
Woher weiß ich, ob mein Abonnement gültig ist?.....15
Wartungscenter.....15
Abonnement aktivieren.....16

Kapitel 3: Einführung.....17

Ansicht meines allgemeinen Schutzstatus.....18
Anzeigen der Produktstatistikdaten.....18
Handhabung der Produkt-Updates.....19
Anzeigen der Datenbankversionen.....19
Einstellungen für mobiles Breitband ändern.....19
Was sind Viren und Malware?.....20
Viren.....20
Spyware.....21
Rootkits.....21
Riskware.....21

Kapitel 4: Schutz des Computers vor Malware.....23

Wie scanne ich meinen Computer?.....24
Automatisches Scannen von Dateien.....24
Manuelles Scannen von Dateien.....26
Scannen von E-Mails.....29
Anzeigen der Scanergebnisse.....30
Ausschließen von Dateien aus dem Scanvorgang.....31
Ausschließen bestimmter Dateitypen.....31
Ausschließen von Dateien nach Speicherort.....31
Anzeigen von ausgeschlossenen Anwendungen.....32
Wie verwende ich die Quarantäne?.....33
Anzeigen von unter Quarantäne gestellten Elementen.....33
Wiederherstellen von Elementen aus der Quarantäne.....34
Was ist DeepGuard?.....34
Aktivieren oder Deaktivieren von DeepGuard.....34
Zulassen der von DeepGuard blockierten Anwendungen.....35
Verwenden von DeepGuard im Kompatibilitätsmodus.....35
Handhabung von Warnmeldungen zu verdächtigem Verhalten.....35
Was ist eine Firewall?.....36
Aktivieren oder Deaktivieren der Firewall.....36
Ändern der Firewall-Einstellungen.....37
Verhindern, dass Anwendungen schädliche Dateien herunterladen.....37
Blockieren von Spams.....37
Aktivieren oder Deaktivieren der Spam- und Phishing-Filterung.....38
Schutz gegen Phishing-Versuche.....38
Einrichten meiner E-Mail-Programme zum Spam-Filtern.....38

Kapitel 5: Sichere Nutzung des Internets.....41

Ausführen allgemeiner Aufgaben.....42
Schützen von verschiedenen Benutzerkonten.....42
Erstellen und Bearbeiten von Windows-Benutzerkonten.....42
Was ist Surfschutz.....42
Den Surfschutz ein- oder ausschalten.....42
Surfschutz-Sicherheitsbewertungen.....43
Schutz gegen schädlichen Inhalt.....44
Was tun, wenn eine Webseite blockiert wird.....44
Sicherheitszusammenfassung für eine Webseite.....44
Sicheres Surfen.....45
Beschränken des Zugriffs auf Webinhalte.....45
Online-Zeiten festlegen.....47
Tägliche Internetzeiten einschränken.....47
Anzeigen der Statistik.....47

Kapitel

1

Installation

Themen:

- *Vor der Erstinstallation*
- *Erstinstallation des Produkts*
- *Anwendungen installieren und aktualisieren*
- *Hilfe und Support*

Vor der Erstinstallation

Vielen Dank, dass Sie sich für F-Secure entschieden haben.

Um das Produkt zu installieren, benötigen Sie Folgendes:

- Installations-CD oder Installationspaket. Wenn Sie ein Netbook ohne CD-Laufwerk verwenden, können Sie das Installationspaket von *www.f-secure.com/netbook* herunterladen.
- Ihr Abonnementschlüssel
- Eine Internetverbindung.

Sicherheitsprodukte von anderen Anbietern auf Ihrem Computer werden vom Installationsprogramm automatisch entfernt. Sollte dies nicht gelingen, entfernen Sie sie manuell.

Hinweis: Führen Sie bei mehreren Benutzerkonten auf einem Computer die Installation als Administrator durch.

Erstinstallation des Produkts

Installationsanleitung

Gehen Sie zur Installation des Produkts wie folgt vor:

1. Legen Sie die Installations-CD ein oder starten Sie das heruntergeladene Installationsprogramm mit einem Doppelklick.

   Sollte die CD nicht automatisch starten, öffnen Sie Windows Explorer und doppelklicken Sie auf das CD-ROM-Symbol. Öffnen Sie anschließend die Installationsdatei mit einem Doppelklick, um die Installation zu starten.

2. Folgen Sie den Anweisungen auf dem Bildschirm.

   - Wenn Sie das Produkt auf CD erworben haben, finden Sie den Abonnementschlüssel auf dem Deckblatt der Schnellinstallationsanleitung.
   - Wenn Sie das Produkt vom F-Secure eStore heruntergeladen haben, wurde Ihnen der Abonnementschlüssel in der Bestätigungs-E-Mail der Bestellung mitgeteilt.

   Bevor Ihr Abonnement bestätigt und die neuesten Updates heruntergeladen werden können, muss Ihr Computer neu gestartet werden. Nehmen Sie gegebenenfalls die Installations-CD aus dem Laufwerk, bevor Sie Ihren Computer neu starten.

Anwendungen installieren und aktualisieren

Anleitung zur Aktivierung Ihres neuen Abonnements

Folgen Sie diesen Anweisungen, um Ihr neues Abonnement zu aktivieren oder eine neue Anwendung über die Startansicht zu installieren:

Hinweis: Das Symbol für die Startansicht befindet sich in der Windows-Taskleiste.

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-Up-Menü wird geöffnet.
2. Wählen Sie **Meine Abonnements anzeigen**

3. Gehen Sie in **Meine Abonnements** zur Seite **Abonnement-Status** und klicken Sie auf **Abonnement aktivieren**.
   Das Fenster **Abonnement aktivieren** wird geöffnet.
4. Geben Sie Ihren Abonnement-Schlüssel für die Anwendung ein und klicken Sie auf **OK**.
5. Nachdem Ihr Abonnement bestätigt und aktiviert wurde, klicken Sie auf **Schließen**.
6. Gehen Sie in **Meine Abonnements** zur Seite **Installationsstatus**. Sollte die Installation nicht automatisch starten, folgen Sie diesen Anweisungen:
   a) Klicken Sie auf **Installieren**.
      Das Installationsfenster wird geöffnet.
   b) Klicken Sie auf **Weiter**.
      Nachdem die Anwendung heruntergeladen wurde, wird die Installation gestartet.
   c) Klicken Sie nach Fertigstellung der Installation auf **Schließen**.

Das neue Abonnement wurde aktiviert.

Hilfe und Support

Klicken Sie auf das Hilfe-Symbol oder drücken Sie F1, um zur Online-Produkthilfe zu gelangen.

Nachdem Sie sich mit Ihrer Lizenz registriert haben, können Sie Zusatzleistungen wie kostenlose Produktupdates und -hilfen in Anspruch nehmen. Registrieren Sie sich auf *www.f-secure.com/register*.

Kapitel

2

Einstieg

Themen:

- *Verwendung von Automatische Updates*
- *Wie erkennt man, was das Produkt geleistet hat?*
- *Echtzeit-Schutznetzwerk*
- *Woher weiß ich, ob mein Abonnement gültig ist?*

Erste Schritte mit dem Produkt

In diesem Abschnitt wird beschrieben, wie Sie die allgemeinen Einstellungen ändern und Ihre Abonnements über das Launchpad verwalten können.

Die allgemeinen Einstellungen des Launchpads sind diejenigen, die für alle im Launchpad installierten Programme übernommen werden. Anstatt die Einstellungen jedes Programms separat zu ändern, können Sie einfach die allgemeinen Einstellungen bearbeiten. Diese werden dann für alle installierten Programme übernommen.

Zu den allgemeinen Einstellungen des Launchpads gehören:

- Downloads. Hier können Sie sehen, welche Updates heruntergeladen wurden und die Verfügbarkeit neuer Updates manuell überprüfen.
- Verbindungseinstellungen. Hier können Sie die Internetverbindung Ihres Computers ändern.
- Benachrichtigungen. Hier können Sie vergangene Benachrichtigungen ansehen und einstellen, welche Benachrichtigungen Ihnen angezeigt werden sollen.
- Datenschutzeinstellungen. Hier können Sie auswählen, ob Ihrem Computer die Verbindung zum Echtzeit-Netzwerkschutz gewährt werden soll.

Über das Launchpad können Sie auch die Abonnements Ihrer installierten Programme verwalten.

Verwendung von Automatische Updates

Die Verwendung automatischer Updates hält den Schutz auf Ihrem Computer auf dem neuesten Stand.

Das Produkt lädt die neuesten Updates auf Ihren Computer herunter, wenn Sie mit dem Internet verbunden sind. Es erkennt den Netzwerkverkehr und stört auch bei einer langsamen Netzwerkverbindung nicht die Internetnutzung.

Den Update-Status überprüfen

Datum und Uhrzeit der letzten Aktualisierung anzeigen.

Wenn automatische Updates aktiviert sind, erhält das Produkt die neuesten Updates automatisch, sobald Sie mit dem Internet verbunden sind.

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Automatische Updates** > **Downloads**.
4. Klicken Sie auf **Jetzt prüfen**.
   Das Produkt stellt eine Verbindung mit dem Internet her und sucht nach den neuesten Updates. Falls der Schutz nicht aktuell ist, ruft es die neuesten Updates ab.

   Hinweis: Wenn Sie ein Modem verwenden oder eine ISDN-Verbindung zum Internet haben, muss die Verbindung aktiv sein, um nach Updates zu suchen.

Ändern der Einstellungen für die Internetverbindung

In der Regel müssen die Standardeinstellungen nicht geändert werden, sie können jedoch festlegen, wie der Server mit dem Internet verbunden wird, damit Sie Updates automatisch erhalten.

Gehen Sie wie folgt vor, um die Einstellungen für die Internetverbindung zu ändern:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Automatische Updates** > **Verbindung**.
4. Wählen Sie **Internetverbindung** aus, wie Ihr Computer mit dem Internet verbunden ist.
   - Wählen Sie **Ständige Verbindung voraussetzen**, wenn Sie eine permanente Netzwerkverbindung haben.

     Hinweis: Falls Ihr Computer keine ständige Netzwerkverbindung besitzt und bei Bedarf eine DFÜ-Verbindung herstellt, kann die Option **Ständige Verbindung voraussetzen** zu mehreren Einwahlversuchen führen.
   - Wählen Sie **Verbindung erkennen**, um Updates nur dann abzurufen, wenn das Produkt eine aktive Netzwerkverbindung erkennt.
   - Wählen Sie **Datenverkehr erkennen**, um Updates nur dann abzurufen, wenn das Produkt anderen Netzwerkverkehr erkennt.

     Tipp: Falls Sie eine ungewöhnliche Hardwarekonfiguration besitzen, die dafür sorgt, dass mit der Einstellung **Verbindung erkennen** auch dann eine aktive Netzwerkverbindung erkannt wird, wenn keine vorhanden ist, wählen Sie stattdessen **Datenverkehr erkennen**.

5. Wählen Sie in der Liste **HTTP-Proxy**, ob Ihr Computer einen *Proxyserver* nutzt, um eine Verbindung mit dem Internet herzustellen.
   - Wählen Sie **Kein HTTP-Proxy**, wenn Ihr Computer direkt mit dem Internet verbunden ist.
   - Wählen Sie **HTTP-Proxy manuell konfigurieren** aus, um die *HTTP-Proxy*-Einstellungen zu konfigurieren.
   - Wählen Sie **HTTP-Proxy meines Browsers verwenden**, um die gleichen *HTTP-Proxy*-Einstellungen zu verwenden, die in Ihrem Browser konfiguriert sind.

Prüfen Sie den Status des Echtzeit-Schutznetzwerks

Bei vielen Produktfunktionen hängt die richtige Funktionsweise von der Verbindung mit einem Echtzeit-Schutznetzwerk ab.

Falls Netzwerkprobleme bestehen oder Ihre Firewall den Netzwerkverkehr des Echtzeitschutzes blockiert, ist der Status 'getrennt'. Wenn keine Produktfunktionen installiert sind, die eine Verbindung mit dem Echtzeit-Schutznetzwerk erfordern, lautet der Status 'nicht in Verwendung'.

So prüfen Sie den Status:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Automatische Updates** > **Verbindung**.

Unter **Echtzeit-Schutznetzwerk** wird Ihnen der aktuelle Status des Echtzeit-Schutznetzwerks angezeigt.

Wie erkennt man, was das Produkt geleistet hat?

Auf der Seite **Benachrichtigungen** können Sie sehen, welche Aktionen das Produkt ausgeführt hat, um Ihren Computer zu schützen.

Das Produkt zeigt eine Benachrichtigung an, sobald es eine Aktion ausführt. Dies ist beispielsweise der Fall, wenn es einen Virus findet und diesen blockiert. Einige Benachrichtigungen werden gegebenenfalls von Ihrem Dienstanbieter versendet, beispielsweise, um Sie über neue verfügbare Services zu informieren.

Benachrichtigungsverlauf anzeigen

Im Benachrichtigungsverlauf können Sie alle angezeigten Benachrichtigungen sehen.

Gehen Sie folgendermaßen vor, um den Benachrichtigungsverlauf zu sehen:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Sonstiges** > **Benachrichtigungen**.
4. Klicken Sie auf **Benachrichtigungsverlauf anzeigen**.
   Die Liste des Benachrichtigungsverlaufs wird geöffnet.

Benachrichtigungseinstellungen ändern

Sie können wählen, welche Art der Benachrichtigungen vom Produkt angezeigt werden sollen.

Gehen Sie folgendermaßen vor, um die Benachrichtigungseinstellungen zu ändern:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Sonstiges** > **Benachrichtigungen**.
4. Wählen oder deaktivieren Sie **Programmbenachrichtigungen zulassen**, um Programmbenachrichtigungen zuzulassen oder zu blockieren.

   Wenn diese Einstellung aktiviert ist, werden vom Produkt Benachrichtigungen zu installierten Programmen angezeigt.
5. Wählen oder deaktivieren Sie **Werbebenachrichtigungen zulassen**, um Werbebenachrichtigungen zuzulassen oder zu blockieren.
6. Klicken Sie auf **OK**.

Echtzeit-Schutznetzwerk

Dieses Dokument beschreibt das Echtzeit-Schutznetzwerk, ein Online-Service der F-Secure Corporation, der saubere Anwendungen und Websites identifiziert und Sie gleichzeitig vor Malware und gefährlichen Websites schützt.

Was ist das Echtzeit-Schutznetzwerk?

Das Echtzeit-Schutznetzwerk ist ein Online-Service, der bei aktuellen Internet-Gefahren schnell reagiert.

Wenn Sie Teilnehmer am Echtzeit-Schutznetzwerk sind, können Sie uns helfen, den Schutz vor neuen und aufkommenden Bedrohungen zu erhöhen. Das Echtzeit-Schutznetzwerk sammelt Statistiken über bestimmte unbekannte, bösartige oder verdächtige Anwendungen und darüber, welche Schäden sie auf Ihrem Gerät anrichten. Diese Informationen sind anonym und werden an die F-Secure Corporation zum Zwecke der kombinierten Datenanalyse gesendet. Die analysierten Informationen werden von uns verwendet, um die Sicherheit Ihres Geräts vor den aktuellsten Bedrohungen und vor bösartigen Dateien zu verbessern.

So funktioniert das Echtzeit-Schutznetzwerk

Wenn Sie Teilnehmer am Echtzeit-Schutznetzwerk sind, können Sie Informationen zu unbekannten Anwendungen und Websites sowie zu bösartigen Anwendungen und Sicherheitslücken auf Websites bereitstellen. Das Echtzeit-Schutznetzwerk verfolgt Ihre Internetaktivität nicht nach und sammelt auch keine Informationen zu Websites, die bereits analysiert wurden. Es werden auch keine Informationen zu sauberen Anwendungen gesammelt, die auf Ihrem Computer installiert sind.

Falls Sie diese Daten nicht bereitstellen möchten, werden die Informationen zu installierten Anwendungen oder besuchten Websites nicht vom Echtzeit-Schutznetzwerk gesammelt. Das Produkt muss jedoch die F-Secure-Server abfragen, um die Zuverlässigkeit von Anwendungen, Websites, Nachrichten und anderen Objekten zu gewährleisten. Die Abfrage geschieht mithilfe einer kryptographischen Prüfsumme. Das abgefragte Objekt wird dabei nicht an F-Secure gesendet. Wir verfolgen keine Daten einzelner Benutzer nach; lediglich der Zugriffszähler der Datei oder der Website wird erhöht.

Es ist nicht möglich, jeglichen Netzverkehr zum Echtzeit-Schutznetzwerk zu unterbinden, da hierdurch der vom Produkt hergestellte Schutz grundlegend gewährt wird.

Die Vorteile des Echtzeit-Schutznetzwerks

Mit dem Echtzeit-Schutznetzwerk haben Sie einen schnelleren und genaueren Schutz vor aktuellen Bedrohungen. Zudem werden Sie bei verdächtigen, aber nicht schädlichen Anwendungen nicht unnötig alarmiert.

Wenn Sie Teilnehmer am Echtzeit-Schutznetzwerk sind, können Sie uns dabei helfen, neue und unentdeckte Malware zu finden und mögliche falsche positive Werte aus unserer Virendefinitionsdatenbank zu entfernen.

Alle Teilnehmer des Echtzeit-Schutznetzwerks helfen sich gegenseitig. Wenn das Echtzeit-Schutznetzwerk eine verdächtige Anwendung auf Ihrem Gerät findet, profitieren Sie von den Analyseergebnissen, wenn diese Anwendung bereits auf anderen Geräten gefunden wurde. Das Echtzeit-Schutznetzwerk verbessert die Gesamtleistung Ihres Geräts, da das installierte Sicherheitsprodukt Anwendungen, die das Echtzeit-Schutznetzwerk schon analysiert und als sauber eingestuft hat, nicht noch einmal scannen muss. In ähnlicher Weise werden Informationen zu schädlichen Websites und unerwünschten Massen-Nachrichten über das Echtzeit-Schutznetzwerk weitergegeben. So können wir Ihnen einen genaueren Schutz vor gefährlichen Websites und Spam-Nachrichten bieten.

Je mehr Personen am Echtzeit-Schutznetzwerk teilnehmen, desto besser werden die einzelnen Teilnehmer geschützt.

Welche Daten steuern Sie bei?

Wenn Sie Teilnehmer am Echtzeit-Schutznetzwerk sind, stellen Sie Informationen zu Anwendungen bereit, die auf Ihrem Gerät und auf den Websites, die Sie besuchen, gespeichert sind. Das Echtzeit-Schutznetzwerk kann Sie somit vor den aktuellsten schädlichen Anwendungen und verdächtigen Websites schützen.

Analyse der Dateibewertung

Das Echtzeit-Schutznetzwerk sammelt nur Informationen von unbekannten Anwendungen und Dateien, die entweder verdächtig sind oder als Malware gelten.

Das Echtzeit-Schutznetzwerk erfasst anonyme Informationen von ordnungsgemäßen und verdächtigen Anwendungen auf Ihrem Gerät. Das Echtzeit-Schutznetzwerk erfasst nur Informationen von ausführbaren Dateien (wie beispielsweise portierbaren ausführbaren Dateien auf der Windows-Plattform mit den Erweiterungen .cpl, .exe, .dll, .ocx, .sys, .scr und .drv).

Die gesammelten Informationen beinhalten:

- den Dateipfad, unter dem sich die Anwendung auf Ihrem Gerät befindet,
- die Dateigröße sowie das Datum, an dem sie erstellt oder geändert wurde,
- Dateiattribute und Berechtigungen,
- Signaturinformationen der Datei,
- die aktuelle Version der Datei und das Unternehmen, das sie erstellt hat,
- den Dateiursprung oder seine Download-URL sowie
- Ergebnisse von F-Secure DeepGuard und Antivirusanalyse gescannter Dateien und
- sonstige ähnliche Informationen.

Das Echtzeit-Schutznetzwerk erfasst keine Informationen zu Ihren persönlichen Dokumenten, wenn diese nicht als infiziert gemeldet wurden. Für alle Arten von bösartigen Dateien erfasst das Programm die Bezeichnung der Infektion sowie den Bereinigungsstatus der Datei.

Mit dem Echtzeit-Schutznetzwerk können Sie auch verdächtige Anwendungen analysieren lassen. Anwendungen können ausschließlich als übertragbare ausführbare Dateien übermittelt werden. Das Echtzeit-Schutznetzwerk wird niemals Informationen über Ihre persönlichen Dokumente sammeln; diese werden auch niemals automatisch zur Analyse hochgeladen.

Dateien zur Analyse übermitteln

Mit dem Echtzeit-Schutznetzwerk können Sie auch verdächtige Anwendungen zur Analyse einsenden.

Auf Aufforderung des Produkts können Sie einzelne verdächtige Anwendungen manuell senden. Es können nur portierbare ausführbare Dateien gesendet werden. Das Echtzeit-Schutznetzwerk lädt niemals Ihre persönlichen Dokumente hoch.

Die Website-Bewertung analysieren

Das Echtzeit-Schutznetzwerk verfolgt weder Ihre Webaktivitäten noch sammelt es Informationen auf Websites, die bereits analysiert wurden. Es sorgt dafür, dass besuchte Websites sicher sind, während Sie im Internet surfen. Wenn Sie eine Website besuchen, überprüft das Echtzeit-Schutznetzwerk dessen Sicherheit und benachrichtigt Sie, sobald die Website als verdächtig oder schädlich bewertet wurde.

Wenn die besuchte Website schädliche oder verdächtige Inhalte oder eine bekannte Gefahr enthält, sammelt das Echtzeit-Schutznetzwerk die ganze URL der Seite, sodass der Inhalt der Website analysiert werden kann.

Wenn Sie eine Website besuchen, die noch nicht bewertet wurde, sammelt das Echtzeit-Schutznetzwerk die Namen der Domain und der Subdomain und in manchen Fällen auch den Pfad der besuchten Seite, sodass die Website analysiert und bewertet werden kann. Alle URL-Parameter, die vermutlich Informationen enthalten, die in einer persönlich identifizierbaren Weise mit Ihnen in Verbindung gebracht werden können, werden zum Schutz Ihrer Daten entfernt.

Hinweis: Das Echtzeit-Schutznetzwerk bewertet oder analysiert keine Webseiten in privaten Netzwerken. Deshalb sammelt es keine Informationen zu privaten IP-Netzwerkadressen, wie beispielsweise Firmen-Intranets.

Die Systeminformationen analysieren

Das Echtzeit-Schutznetzwerk sammelt den Namen und die Version Ihres Betriebssystems, Informationen zur Internetverbindung und Verwendungsstatistiken zum Echtzeit-Schutznetzwerk (z. B. wie oft die Website-Bewertung abgefragt wurde oder wie lange es durchschnittlich dauert, bis die Abfrage ein Ergebnis liefert). Auf diese Weise können wir unseren Service überwachen und verbessern.

So schützen wir Ihre Daten

Wir übertragen die Informationen sicher und entfernen automatisch alle persönlichen Informationen, die in den Daten enthalten sein könnten.

Das Echtzeit-Schutznetzwerk entfernt identifizierbare Daten, bevor diese an F-Secure gesendet werden. Außerdem entschlüsselt es alle während der Übertragung gesammelten Informationen, um diese vor nicht autorisiertem Zugriff zu schützen. Die gesammelten Informationen werden nicht einzeln verarbeitet. Sie werden mit Informationen von anderen Teilnehmern am Echtzeit-Schutznetzwerks zusammengeführt. Alle Daten werden statistisch und anonym analysiert. Das bedeutet, dass die Daten in keiner Weise mit Ihnen in Verbindung gebracht werden.

Jegliche Informationen, die Sie persönlich identifizieren könnten sind nicht in den gesammelten Daten enthalten. Das Echtzeit-Schutznetzwerk sammelt keine privaten IP-Adressen oder privaten Informationen, wie E-Mail-Adressen, Benutzernamen und Passwörter. Wir bemühen uns sehr, alle persönlich identifizierbaren Daten zu entfernen. Trotz allem ist es möglich, dass in den gesammelten Informationen noch immer einige identifizierbaren Daten enthalten sind. In diesen Fällen verwenden wir diese versehentlich gesammelten Daten nicht, um Sie zu identifizieren.

Wir legen großen Wert auf strenge Sicherheitsmaßnahmen sowie physische, administrative und technische Schutzmaßnahmen, um die gesammelten Informationen während deren Übertragung, Speicherung und Verarbeitung zu schützen. Die Informationen werden an gesicherten Orten und auf Servern gespeichert, die von uns kontrolliert werden und sich entweder in unseren Büros oder den Büros unserer Zulieferbetriebe befinden. Nur berechtigtes Personal darf auf diese gesammelten Informationen zugreifen.

F-Secure darf diese gesammelten Daten an seine Tochtergesellschaften, Zulieferbetriebe, Vertriebshändler und Partner weitergeben, jedoch grundsätzlich in einer nicht identifizierbaren, anonymen Art und Weise.

Werden Sie Teilnehmer am Echtzeit-Schutznetzwerk!

Sie helfen uns bei der Verbesserung des Echtzeit-Schutznetzwerks, indem Sie uns Informationen zu schädlichen Programmen und Websites mitteilen.

Sie können während der Installation entscheiden, ob Sie am Echtzeit-Schutznetzwerk teilnehmen möchten. Standardmäßig ist angegeben, dass Sie Daten im Echtzeit-Schutznetzwerk bereitstellen möchten. Sie können diese Einstellung jedoch später im Produkt ändern.

Befolgen Sie diese Anweisungen, um die Einstellungen des Echtzeit-Schutznetzwerks zu ändern:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Sonstiges** > **Datenschutz**.
4. Aktivieren Sie das entsprechende Kontrollkästchen, um am Echtzeit-Schutznetzwerk teilzunehmen.

Fragen zum Echtzeit-Schutznetzwerk

Kontaktdetails für Fragen zum Echtzeit-Schutznetzwerk

Für alle weiteren Fragen zum Echtzeit-Schutznetzwerk, wenden Sie sich an:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finnland

http://www.f-secure.com/de/web/home_global/support/contact

Die aktuelle Version dieser Bestimmung finden Sie jederzeit auf unserer Website.

Woher weiß ich, ob mein Abonnement gültig ist?

Auf der Seite **Abonnementstatus** werden Ihr Abonnement und der Status angezeigt.

Wenn Ihr Abonnement bald abläuft oder bereits abgelaufen ist, ändert sich das entsprechende Symbol im Launchpad, das den allgemeinen Schutzstatus des Programms anzeigt.

So prüfen Sie die Gültigkeit Ihrer Anmeldung:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Meine Abonnements anzeigen**.
3. Unter **Abonnementstatus** finden Sie Informationen zu Abonnements Ihrer installierten Programme.
4. Unter **Installationsstatus** sehen Sie, welche Programme installiert werden können.

Status und Ablaufdatum Ihres Abonnements werden auch auf der Seite **Statistik** angezeigt. Ist Ihr Abonnement abgelaufen, müssen Sie es erneuern, um weiterhin Updates zu erhalten und das Produkt verwenden zu können.

Hinweis: Wenn Ihr Abonnement abgelaufen ist, blinkt das Produktstatus-Symbol auf Ihrer Systemleiste.

Wartungscenter

Das Wartungcenter zeigt Ihnen wichtige Meldungen an

Wenn Ihr Abonnement abgelaufen ist oder bald abläuft, erhalten Sie eine Benachrichtigung vom Wartungscenter. Die Hintergrundfarbe und der Inhalt Ihrer Wartungscenter-Meldung sind abhängig von Ihrem Abonnementtyp und -status.

- Wenn Ihr Abonnement bald abläuft und kostenlose Abonnements verfügbar sind, hat die Nachricht einen weißen Hintergrund und verfügt über die Schaltfläche **Aktivieren**.
- Wenn Ihr Abonnement bald abläuft und keine kostenlosen Abonnements zur Verfügung stehen, hat die Nachricht einen gelben Hintergrund und verfügt über die Schaltflächen **Kaufen** und **Schlüssel eingeben**. Wenn Sie bereits ein neues Abonnement gekauft haben, klicken Sie auf **Schlüssel eingeben**, um den Abonnementschlüssel einzugeben und Ihr neues Abonnement zu aktivieren.
- Wenn Ihr Abonnement abgelaufen ist und kostenlose Abonnements verfügbar sind, hat die Nachricht einen roten Hintergrund und verfügt über die Schaltfläche **Aktivieren**.
- Wenn Ihr Abonnement abgelaufen ist und keine kostenlosen Abonnements zur Verfügung stehen, hat die Nachricht einen roten Hintergrund und verfügt über die Schaltflächen **Kaufen** und **Schlüssel eingeben**. Wenn Sie bereits ein neues Abonnement gekauft haben, klicken Sie auf die Schaltfläche **Schlüssel eingeben**, um den Abonnementschlüssel einzugeben und Ihr neues Abonnement zu aktivieren.

Hinweis: Über den Link **Benachrichtigungsverlauf** im Wartungscenter wird eine Liste mit Produktbenachrichtigungen angezeigt, jedoch keine früheren Wartungscenter-Meldungen.

Abonnement aktivieren

Wenn Sie einen neuen Abonnementschlüssel oder einen Aktionscode für ein Produkt erhalten haben, müssen Sie diesen aktivieren.

Aktivierung eines Abonnements:

1. Führen Sie auf der Startansicht einen Rechtsklick auf das Symbol ganz rechts aus.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Meine Abonnements anzeigen**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Abonnement aktivieren**.
   - Klicken Sie auf **Kampagnencode aktivieren**.
4. Geben Sie nun in das Dialogfeld Ihren Abonnementschlüssel oder Kampagnencode ein, und klicken Sie auf **OK**.

   Tipp: Wenn Sie Ihren Abonnementschlüssel per E-Mail erhalten haben, können Sie den Schlüssel aus der E-Mail-Nachricht kopieren und in das Feld einfügen.

Nachdem Sie den neuen Abonnementschlüssel eingegeben haben, wird das neue Gültigkeitsdatum des Abonnements auf der Seite **Abonnementstatus** angezeigt.

Kapitel

3

Einführung

Themen:

- *Ansicht meines allgemeinen Schutzstatus*
- *Anzeigen der Produktstatistikdaten*
- *Handhabung der Produkt-Updates*
- *Was sind Viren und Malware?*

Dieses Produkt schützt Ihren Computer vor Viren und anderen schädlichen Anwendungen.

Dazu werden Dateien gescannt, Anwendungen analysiert und automatisch Aktualisierungen durchgeführt. Ein Eingriff durch den Benutzer ist nicht erforderlich.

Ansicht meines allgemeinen Schutzstatus

Auf der Seite **Status** wird eine Kurzübersicht der installierten Produktfunktionen und deren aktuellem Status angezeigt.

So öffnen Sie die Seite **Status**:

Klicken Sie auf der Haupseite auf **Status**.

Die Seite **Status** wird geöffnet.

Die Symbole zeigen den Status des Programms und dessen Sicherheitsfunktionen an.

Status-Symbol	Statusbezeichnung	Beschreibung
	OK	Ihr Computer ist geschützt. Die Funktion ist aktiviert und arbeitet ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über den bestimmten Status einer Funktion. So werden Sie beispielsweise darauf hingewiesen, dass die Funktion gerade aktualisiert wird.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Dadurch wird längere Zeit kein Produkt-Update empfangen und der eventuell kritische Status einer Funktion kann nicht geprüft werden.
	Fehler	Ihr Computer ist nicht geschützt. Das ist z. B. der Fall, wenn Ihr Abonnement abgelaufen ist oder eine kritische Funktion deaktiviert wurde.
	Aus	Eine nicht-kritische Funktion ist ausgeschaltet.

Anzeigen der Produktstatistikdaten

Sie können sehen, was das Produkt seit dem letzten Installieren auf der Seite **Statistiken** geleistet hat.

Zum Öffnen der Seite **Statistiken**:

Klicken Sie auf der Startseite auf **Statistiken**.

Die Seite **Statistiken** wird geöffnet.

- **Letzte erfolgreiche Update-Überprüfung** zeigt den Zeitpunkt der letzten Aktualisierung an.
- **Viren- und Spyware-Scan** zeigt an, wie viele Dateien das Produkt seit der Installation gescannt und gesäubert hat.
- Unter **Anwendungen** sehen Sie, wie viele Programme DeepGuard seit der Installation zugelassen oder blockiert hat.
- **Firewall-Verbindungen** zeigt die Anzahl der seit der Installation zugelassenen und blockierten Verbindungen an.
- **Spam- und Phishing-Filter** gibt an, wie viele E-Mail-Nachrichten das Produkt als gültige E-Mail-Nachrichten und als Spam-Nachrichten identifiziert hat.

Handhabung der Produkt-Updates

Das Produkt sorgt für eine regelmäßige und automatische Aktualisierung des gebotenen Schutzes.

Anzeigen der Datenbankversionen

Auf der Seite **Datenbank-Updates** werden die neuesten Update-Zeiten und Versionsnummern angezeigt.

So öffnen Sie die Seite **Datenbank-Updates**:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Sonstige Einstellungen** > **Datenbankversionen**.

Auf der Seite **Datenbankversionen** werden das Datum, an dem die Virus- und Spyware-Definitionen, DeepGuard und Spam- und Phishing-Filter aktualisiert wurden, sowie die entsprechenden Versionsnummern angezeigt.

Einstellungen für mobiles Breitband ändern

Wählen Sie, ob Sie bei der Verwendung von mobilem Breitband Sicherheitsupdates herunterladen möchten.

Hinweis: Diese Funktion ist nur in Microsoft Windows 7 verfügbar.

Standardmäßig werden Sicherheitsupdates immer heruntergeladen, wenn Sie mit dem Netzwerk Ihres Privatanbieters verbunden sind. Die Updates werden jedoch unterbrochen, sobald Sie auf ein Netzwerk eines anderen Anbieters zugreifen. Dies liegt daran, dass die Verbindungspreise zwischen Anbietern, beispielsweise in verschiedenen Ländern, variieren können. Sie sollten diese Einstellung nicht ändern, wenn Sie bei Ihrem Besuch Bandbreite und möglicherweise auch Kosten sparen möchten.

Hinweis: Diese Einstellung gilt nur für mobile Breitbandverbindungen. Wenn der Computer mit einem Festnetz oder Drahtlosnetzwerk verbunden ist, wird das Produkt automatisch aktualisiert.

So ändern Sie die Einstellung:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Sonstige Einstellungen** > **Mobiles Breitband** > **Sicherheits-Updates herunterladen**.
3. Wählen Sie die bevorzugte Update-Option für Mobilverbindungen:
   - **Nur im Netzwerk meines Heimbetreibers.**

Updates werden im Netzwerk Ihres Privatanbieters immer heruntergeladen. Wenn Sie ein Netzwerk eines anderen Anbieters besuchen, werden die Updates unterbrochen. Wir empfehlen Ihnen, diese Option zu wählen, um Ihr Sicherheitsprodukt zu den erwarteten Kosten auf dem neuesten Stand zu halten.

- **Nie**

  Es werden keine Updates heruntergeladen, wenn Sie mobiles Breitband verwenden.

- **Immer**

  Updates werden immer heruntergeladen, egal welches Netzwerk Sie verwenden. Wählen Sie diese Option, wenn Sie sicherstellen möchten, dass die Sicherheit Ihres Computers, unabhängig von den Kosten, stets aktuell ist.

4. Wenn Sie jedes Mal erneut auswählen möchten, sobald Sie das Netzwerk Ihres Heimbetreibers verlassen, wählen Sie**Jedes Mal nachfragen, sobald ich das Netzwerk meines Heimbetreibers verlasse**.

Sicherheitsupdates unterbrochen

Die Sicherheitsupdates können unterbrochen werden, wenn Sie mobiles Breitband außerhalb des Netzwerks Ihres Privatanbieters nutzen.

In diesem Fall sehen Sie die Benachrichtigung **Angehalten** in der unteren rechten Ecke Ihres Bildschirms. Die Updates werden unterbrochen, da die Verbindungspreise je nach Anbieter und Land variieren können. Sie sollten in Betracht ziehen, diese Einstellung nicht zu ändern, wenn Sie Bandbreite und dadurch mögliche Kosten sparen möchten. Wenn Sie jedoch die Einstellungen trotzdem ändern möchten, klicken Sie auf den Link **Ändern**.

Hinweis:

Diese Funktion ist nur in Microsoft Windows 7 verfügbar.

Was sind Viren und Malware?

Als Malware werden Programme bezeichnet, die speziell entwickelt wurden, um Ihren Computer zu beschädigen oder ohne Ihr Wissen zu illegalen Zwecken zu verwenden oder aber um Informationen von Ihrem Computer zu stehlen.

Malware kann:

- die Kontrolle über Ihren Webbrowser übernehmen,
- Ihre Suche umleiten,
- unerwünschte Werbung einblenden,
- die von Ihnen besuchten Websites aufzeichnen,
- persönliche Informationen stehlen, wie Ihre Kontodaten,
- Ihren Computer zum Versenden von Spam benutzen und
- Ihren Computer benutzen, um andere Computer anzugreifen.

Malware kann außerdem dazu führen, dass Ihr Computer langsam und instabil wird. Der Verdacht, dass sich *Malware* auf Ihrem Computer befindet, liegt dann nahe, wenn er plötzlich sehr langsam wird und häufig abstürzt.

Viren

Ein Virus ist in der Regel ein Programm, das sich selbst an Dateien anhängt und sich ständig selbst repliziert; es kann die Inhalte anderer Dateien so verändern oder ersetzen, dass Ihr Computer dadurch beschädigt wird.

Ein *Virus* ist ein Programm, das normalerweise ohne Ihr Wissen auf Ihrem Computer installiert wird. Anschließend versucht der Virus, sich zu replizieren. Der Virus:

- verwendet einige der Systemressourcen Ihres Computers,
- kann Dateien auf Ihrem Computer verändern oder beschädigen,
- versucht wahrscheinlich, Ihren Computer zu benutzen, um andere Computer zu infizieren,
- kann zulassen, dass Ihr Computer für illegale Zwecke verwendet wird.

Spyware

Spyware sind Programme, die Ihre persönlichen Informationen sammeln.

Spyware kann persönliche Daten sammeln, wie:

- Internet-Websites, die Sie besucht haben,
- E-Mail-Adressen auf Ihrem Computer,
- Passwörter oder
- Kreditkartennummern.

Spyware installiert sich fast immer selbst, ohne Ihre ausdrückliche Erlaubnis. Spyware wird unter Umständen zusammen mit einem nützlichen Programm installiert. Es ist aber auch möglich, dass Sie in einem irreführenden Popup-Fenster versehentlich auf eine Option klicken.

Rootkits

Rootkits sind Programme, die dafür sorgen, dass *Malware* schwer zu finden ist.

Rootkits verstecken Dateien und Prozesse. In der Regel, um schädliche Aktivitäten auf dem Computer zu verbergen. Wenn ein Rootkit *Malware* versteckt, ist es nicht einfach, die Malware auf Ihrem Computer zu finden.

Dieses Produkt besitzt einen Rootkit-Scanner, der gezielt nach Rootkits sucht, wodurch *Malware* sich nicht problemlos verstecken kann.

Riskware

Riskware wurde nicht speziell entwickelt, um Ihrem Computer zu schaden, sie kann Ihrem Computer aber schaden, wenn sie missbräulich verwendet wird.

Riskware ist genau genommen keine Malware. Riskware-Programme führen einige nützliche, aber potenziell gefährliche Funktionen durch.

Beispiele für Riskware-Programme:

- Programme für Instant Messaging, etwa IRC (Internet Relay Chat),
- Programme zur Übertragung von Dateien über das Internet von einem Computer auf einen anderen,
- oder Programme für die Internet-Telefonie, etwa VoIP (*Voice over Internet Protocol*).
- Fernzugriffs-Software, z. B. VNC,
- Scareware; versucht durch Verschrecken oder Betrug zum Kauf gefälschter Sicherheitssoftware zu bewegen
- Software, die für die Umgehung von CD-Prüfungen oder Kopierschutz programmiert ist

Wenn Sie das Porgramm explizit installiert und richtig eingerichtet haben, ist es wahrscheinlich ungefährlich.

Wenn die Riskware ohne Ihr Wissen installiert wurde, wurde sie wahrscheinlich in böser Absicht installiert und sollte entfernt werden.

Kapitel

4

Schutz des Computers vor Malware

Themen:

- *Wie scanne ich meinen Computer?*
- *Ausschließen von Dateien aus dem Scanvorgang*
- *Wie verwende ich die Quarantäne?*
- *Was ist DeepGuard?*
- *Was ist eine Firewall?*
- *Blockieren von Spams*

Durch Viren- und Spyware-Scanning wird der Computer vor Programmen geschützt, die persönliche Informationen stehlen, den Server beschädigen oder ihn zu illegalen Zwecken nutzen können.

Alle Arten von Malware werden nach ihrem Fund sofort behandelt, sodass sie keine Schäden verursachen können.

Standardmäßig werden bei Viren- und Spywarescans automatisch Ihre lokalen Festplatten, alle Wechselmedien (wie externe Festplatten oder CDs) und heruntergeladene Inhalte gescannt. Außerdem können Sie ein automatisches Scannen Ihrer E-Mails festlegen.

Bei Viren- und Spywarescans wird Ihr Computer außerdem auf jedwede Änderungen überprüft, die auf *Malware* schließen lassen könnten. Wenn gefährliche Systemänderungen festgestellt werden – beispielsweise Änderungen an Systemeinstellungen oder Versuche, wichtige Systemprozesse zu ändern –, verhindert DeepGuard die Ausführung des Programms, da es sich dabei wahrscheinlich um *Malware* handelt.

Wie scanne ich meinen Computer?

Wenn Sie das Viren- und Spyware-Scanning aktivieren, wird Ihr Computer automatisch nach schädlichen Dateien durchsucht. Sie können Dateien auch manuell scannen und Scanvorgänge für einen bestimmten Zeitpunkt planen.

Das Viren- und Spyware-Scanning sollte stets aktiviert sein. Führen Sie für Ihre Dateien einen manuellen Scanvorgang durch, wenn Sie sichergehen möchten, dass auf Ihrem Computer keine schädlichen Dateien vorhanden sind, oder wenn Sie Dateien prüfen möchten, die Sie vom Echtzeit-Scan ausgeschlossen haben.

Durch die Planung von Scanvorgängen können schädliche Dateien zu einem ganz bestimmten Zeitpunkt über das Viren- und Spyware-Scanning von Ihrem Computer entfernt werden.

Automatisches Scannen von Dateien

Beim Echtzeit-Scanning wird der Computer geschützt, indem alle Dateien gescannt werden, wenn auf sie zugegriffen wird, und der Zugriff auf Dateien, die *Malware* enthalten, gesperrt wird.

Wenn Sie versuchen, auf eine Datei zuzugreifen, überprüft die Echtzeit-Scanfunktion die Datei zunächst auf Malware, bevor sie dem Computer den Zugriff auf die Datei ermöglicht. Wenn beim Echtzeit-Scanning schädlicher Inhalt identifiziert wird, wird die Datei in Quarantäne gesetzt, damit sie keinen Schaden anrichten kann.

Beeinträchtigt das Echtzeit-Scanning die Leistung meines Computers?

Normalerweise bemerken Sie den Scanvorgang nicht, da er nur kurz dauert und wenig Systemressourcen benötigt. Wie lange das Scannen in Echtzeit dauert und wie viele Systemressourcen benötigt werden, hängt beispielsweise vom Inhalt, dem Speicherort und dem Typ der Datei ab.

Dateien, bei denen das Scannen länger dauert:

- Dateien auf Wechseldatenträgern wie CDs, DVDs und tragbaren USB-Laufwerken.
- Komprimierte Dateien, wie *.zip*.

  Hinweis: Komprimierte Dateien werden nicht automatisch gescannt.

Das Scannen in Echtzeit kann Ihren Computer verlangsamen, wenn:

- Sie mit einem Computer arbeiten, der nicht den Systemanforderungen entspricht.
- Sie auf zahlreiche Dateien gleichzeitig zugreifen. Wenn Sie z. B. ein Verzeichnis öffnen, das eine große Anzahl Dateien enthält, die gescannt werden müssen.

Aktivieren oder Deaktivieren des Echtzeit-Scannings

Das Echtzeit-Scanning sollte stets aktiviert sein, damit *Malware* gestoppt wird, noch bevor sie Schaden auf Ihrem Computer anrichten kann.

So aktivieren bzw. deaktivieren Sie das Echtzeit-Scanning:

1. Klicken Sie auf der Haupseite auf **Status**.
2. Klicken Sie auf **Einstellungen auf dieser Seite ändern**.

   Hinweis: Sie benötigen Administrator-Zugriffsrechte, um die Sicherheitsfunktionen deaktivieren zu können.

3. Aktivieren oder deaktivieren Sie **Viren- und Spyware-Scanning**.
4. Klicken Sie auf den Link **Schließen**.

Automatische Handhabung schädlicher Dateien

Beim Echtzeit-Scanning können schädliche Dateien automatisch, d. h. ohne Ausgabe von Fragen an den Benutzer, verwaltet werden.

So bestimmen Sie die automatische Handhabung schädlicher Dateien beim Echtzeit-Scanning:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Wählen Sie **Schädliche Dateien automatisch verwalten**.

Wenn schädliche Dateien nicht automatisch verwaltet werden sollen, werden Sie beim Echtzeit-Scanning aufgefordert, die durchzuführende Aktion auszuwählen, wenn eine schädliche Datei identifiziert wird.

Handhabung von Spyware

Die Viren- und Spyware-Scanfunktion blockiert Spyware sofort beim Ausführungsversuch.

Bevor eine Spyware-Anwendung ausgeführt werden kann, wird sie vom Scanner blockiert. Sie können dann die weitere Vorgehensweise bestimmen.

Wählen Sie eine der folgenden Aktionen, wenn Spyware identifiziert wird:

Durchzuführende Aktion	Was mit der Spyware geschieht
Automatisch handhaben	Die Scanfunktion sucht die beste Aktion für die identifzierte Spyware aus.
Spyware in Quarantäne stellen	Die Spyware wird in eine Quarantänezone verschoben, in der Sie keinen Schaden auf Ihrem Computer anrichten kann.
Spyware löschen	Alle Spyware-bezogenen Dateien werden vom Computer entfernt.
Spyware nur blockieren	Der Zugriff auf die Spyware wird blockiert, die Spyware verbleibt jedoch auf Ihrem Computer.
Spyware vom Scan ausschließen	Die Ausführung von Spyware wird zugelassen und Spyware wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

Handhabung von Riskware

Die Viren- und Spyware-Scanfunktion blockiert Riskware direkt beim Ausführungsversuch.

Bevor eine Riskware-Anwendung ausgeführt werden kann, wird sie blockiert. Sie können dann die weitere Vorgehensweise bestimmen.

Wählen Sie eine der folgenden Aktion, wenn Riskware identifiziert wurde:

Durchzuführende Aktion	Was mit der Riskware passiert
Riskware nur blockieren	Der Zugriff auf die Riskware wird blockiert, die Riskware verbleibt jedoch auf Ihrem Computer.
Riskware in Quarantäne stellen	Die Riskware wird in eine Quarantänezone verschoben, in der sie keinen Schaden auf dem Computer anrichten kann.
Riskware löschen	Alle Riskware-bezogenen Dateien werden vom Computer entfernt.
Riskware vom Scanvorgang ausschließen	Die Ausführung von Riskware wird zugelassen und Riskware wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

Automatisches Entfernen von Tracking-Cookies

Wenn Sie Tracking-Cookies entfernen, können Sie verhindern, dass Websites einen Einblick in die von Ihnen im Internet besuchten Sites erhalten.

Tracking-Cookies sind kleine Dateien, die es Websites ermöglichen, die von Ihnen besuchten Websites aufzuzeichnen. Halten Sie sich an die nachstehenden Anweisungen, um Ihren Computer frei von Tracking-Cookies zu halten.

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Wählen Sie **Tracking-Cookies entfernen**.
4. Klicken Sie auf **OK**.

Manuelles Scannen von Dateien

Sie können Ihre Dateien manuell scannen, wenn Sie z. B. ein externes Gerät an Ihren Computer anschließen. Dadurch können Sie sicherstellen, dass keine Malware vorhanden ist.

Starten des manuellen Scanvorgangs

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von *Malware* oder einen bestimmten Bereich scannen.

Wenn Sie einen bestimmten Typ von *Malware* befürchten, können Sie nur nach diesem Typ scannen. Wenn Sie im Bezug auf einen bestimmten Bereich Ihres Computers einen Verdacht haben, dann scannen Sie nur diesen Bereich. Diese Scans verlaufen viel schneller als ein vollständiger Scan des gesamten Computers.

So starten Sie das Scannen Ihres Computers manuell:

1. Klicken Sie auf der Hauptseite auf den Pfeil unter **Scannen**.

   Die Scan-Optionen werden angezeigt.

2. Wählen Sie den Scan-Typ.

   Wählen Sie **Scanning-Einstellungen ändern** , um den Ablauf der manuellen Scanvorgänge auf Ihrem Computer für die Suche nach Viren und anderen schädlichen Anwendungen zu optimieren.

3. Bei Auswahl von **Elemente für Scan wählen** wird ein Fenster geöffnet, in dem Sie das zu prüfende Verzeichnis oder Objekt angeben können.
   Der **Scan-Assistent** wird geöffnet.

Scantypen

Sie können Ihren gesamten Computer scannen oder nach einem bestimmten Typ von Malware oder einen bestimmten Bereich scannen.

Dies sind die verschiedenen Scantypen:

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
Viren- und Spyware-Scanning	Teile Ihres Computers auf Viren, Spyware und Riskware	Diese Art des Scannens ist weitaus schneller als ein vollständiger Scan.Es werden nur die Teile Ihres Systems durchsucht, die installierte Programmdateien enthalten. Dieser Scantyp wird empfohlen, wenn Sie rasch überprüfen möchten, ob Ihr Computer sauber ist, da Sie mit dieser Funktion aktive Malware auf Ihrem Computer rasch entdecken können.

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
Vollständiger Scan des Computers	Ihr gesamter Computer (interne und externe Festplatten) auf Viren, Spyware und Riskware	Wenn Sie absolut sicher sein wollen, dass keine Malware oder Riskware auf Ihrem Computer ist.Diese Art des Scannens dauert am längsten.Sie kombiniert den schnellen Malware-Scan und den Festplattenscan. Außerdem sucht sie nach Elementen, die unter Umständen durch ein Rootkit verborgen sind.
Auswahl für Scan...	Eine spezielle Datei, ein spezieller Ordner oder ein spezielles Laufwerk für Viren, Spyware und Riskware	Wenn Sie den Verdacht haben, dass sich an einem bestimmten Speicherort Ihres Computers Malware befindet, weil sich dort Downloads von potenziell gefährlichen Quellen, wie Peer-to-Peer File Sharing-Netzwerken, befinden.Wie lange der Scan dauert, hängt von der Größte des zu scannenden Ziels ab.Der Scan wird beispielsweise schnell abgeschlossen, wenn Sie einen Ordner mit nur ein paar kleinen Dateien scannen.
Rootkit-Scan	Wichtige Sytembereiche, wo verdächtige Elemente zu einem Sicherheitsproblem werden könnenScannt nach verborgenen Dateien, Ordnern, Laufwerken oder Prozessen	Wenn Sie vermuten, dass auf Ihrem Computer ein Rootkit installiert ist. Beispielsweise, wenn vor kurzem auf Ihrem Computer Malware entdeckt wurde und Sie sichergehen möchten, dass dabei kein Rootkit installiert wurde.

Im Windows Explorer scannen

Sie können Datenträger, Ordner und Dateien im Windows Explorer in Bezug auf *Viren*, *Spyware* und *Riskware* scannen.

So scannen Sie einen Datenträger, einen Ordner oder eine Datei:

1. Platzieren Sie den Mauszeiger auf dem zu scannenden Datenträger, dem Ordner oder der Datei und klicken Sie mit der rechten Maustaste.
2. Wählen Sie im Kontextmenü **Ordner nach Viren scannen**. (Der Name der Option hängt davon ab, ob Sie einen Datenträger, einen Ordner oder eine Datei scannen.)
   Das Fenster **Scan-Assistent** wird geöffnet und der Scanvorgang beginnt.

Wenn ein *Virus* oder *Spyware* gefunden wird, führt Sie der **Scan-Assistent** durch die für die Bereinigung erforderlichen Schritte.

Auswählen von Dateien für den Scanvorgang

Sie können die Dateitypen auswählen, die auf *Viren* und *Spyware* manuell oder geplant gescannt werden sollen.

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Sonstige Einstellungen** > **Manuelle Scans**.
3. Wählen Sie unter **Suchoptionen** aus den folgenden Einstellungen:

Nur bekannte Dateitypen scannen	Zum Scannen von nur denjenigen Dateitypen, bei denen eine Infektion am wahrscheinlichsten ist, z. B. ausführbaren Dateien. Durch Auswahl dieser Option wird das Scannen außerdem beschleunigt. Die Dateien mit den folgenden Erweiterungen werden gescannt: `.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 und .hqx.
Komprimierte Dateien scannen	Zum Scannen von Archivdateien und -ordnern.
Erweiterte Heuristik verwenden	Zur Verwendung aller verfügbaren heuristischen Methoden während des Scans, um neue oder unbekannte Malware besser aufzuspüren. **Hinweis:** Wenn Sie diese Option wählen, dauert der Scanvorgang länger und kann zu mehr Fehlarmen führen (harmlose Dateien, die als verdächtig gemeldet werden).

4. Klicken Sie auf **OK**.

Hinweis: Die ausgeschlossenen Dateien in der Liste der ausgeschlossenen Elemente werden nicht gescannt, selbst wenn Sie sie hier für einen Scanvorgang auswählen.

Durchzuführende Aktionen bei der Identifizierung schädlicher Dateien

Sie können bestimmen, wie schädliche Dateien nach ihrer Identifzierung gehandhabt werden.

So wählen Sie die Aktion, die bei der Identifizierung von schädlichem Inhalt im Rahmen eines manuellen Scanvorgangs durchzuführen ist:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Sonstige Einstellungen** > **Manuelle Scans**.
3. Wählen Sie unter **Wenn Viren oder Spyware gefunden wird** eine der folgenden Optionen:

Option	Beschreibung
Mich fragen (Standard)	Sie können für jedes beim manuellen Scanning identifizierte Element die jeweils durchzuführende Aktion wählen.
Dateien säubern	Das Produkt versucht, die beim manuellen Scanning gefundenen infizierten Dateien automatisch zu säubern. **Hinweis:** Wenn eine infizierte Datei nicht gesäubert werden kann, wird sie in Quarantäne gestellt (es sei denn, sie wurde im Netzwerk oder auf einem Wechseldatenträger gefunden), damit sie keinen Schaden auf dem Computer anrichten kann.
Dateien unter Quarantäne stellen	Das Produkt verschiebt alle beim manuellen Scanning identifizierten schädlichen Dateien in eine Quarantänezone, in der sie keinen Schaden auf dem Computer anrichten können.
Dateien löschen	Alle beim manuellen Scanning identifizierten schädlichen Dateien werden gelöscht.

Option	Beschreibung
Nur Bericht	Die beim manuellen Scanning gefundenen schädlichen Dateien bleiben unberührt, ihre Identifizierung wird im Scanbericht aufgezeichnet. **Hinweis:** Bei der Wahl dieser Option kann Malware auf Ihrem Computer immer noch Schaden anrichten, wenn das Echtzeit-Scanning deaktiviert ist.

Hinweis: Wenn beim manuellen Scanning schädliche Dateien identifziert werden, werden diese automatisch gesäubert.

Planen von Scans

Programmieren Sie Ihren Computer für die Durchführung automatischer Scanvorgänge und das Entfernen von Viren und anderen schädlichen Anwendungen, wenn Sie nicht arbeiten. Sie können auch periodische Scanvorgänge planen, um sicherzustellen, dass Ihr Computer virusfrei ist.

So planen Sie einen Scan:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Sonstige Einstellungen** > **Geplante Scans**.
3. Aktivieren Sie **Geplantes Scanning**.
4. Geben Sie an, wann der Scanvorgang gestartet werden soll.

Option	Beschreibung
Täglich	Der Computer wird jeden Tag gescannt.
Wöchentlich	Ihr Computer wird an den angegebenen Wochentagen gescannt. Wählen Sie die gewünschten Tage in der Liste aus.
Monatlich	Ihr Computer wird an den angegebenen Monatstagen gescannt. So wählen Sie die gewünschten Tage aus: 1. Wählen Sie eine Option für **Tag** aus. 2. Wählen Sie in der Liste neben dem ausgewählten Tag den Tag des Monats aus.

5. Wählen Sie aus, wann Sie den Scan an den ausgewählten Tagen starten möchten.

Option	Beschreibung
Startzeit	Der Scanvorgang wird zur vorgegebenen Uhrzeit gescannt.
Nachdem der Computer nicht benutzt wurde für	Der Scanvorgang wird gestartet, nachdem der Computer während des angegebenen Zeitraums nicht verwendet wurde.

Für das geplante Scanning werden die Einstellungen des manuellen Scannings verwendet. Allerdings werden bei jedem geplanten Scanvorgang die Archive gescannt und schädliche Dateien automatisch gesäubert.

Scannen von E-Mails

Durch das Scannen Ihrer E-Mail schützen Sie sich vor dem Empfang schädlicher Dateien in den an Sie gesendeten E-Mails.

Die Viren- und Spyware-Scanfunktion muss aktiviert werden, damit E-Mails auf Viren überprüft werden.

So aktivieren Sie den E-Mail-Scan:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Wählen Sie **Schädliche E-Mail-Anhänge entfernen**.
4. Klicken Sie auf **OK**.

Wann werden E-Mail-Nachrichten und Anhänge gescannt?

Viren- und Spyware-Scans können schädliche Inhalte aus von Ihnen empfangenen E-Mails entfernen.

Viren- und Spyware-Scans entfernen schädliche E-Mails, die von E-Mail-Programmen wie Microsoft Outlook und Outlook Express, Microsoft Mail oder Mozilla Thunderbird empfangen werden. Sie durchsuchen verschlüsselte E-Mail-Nachrichten und Anhänge, sobald Ihr E-Mail-Programm diese vom Mail Server unter Verwendung des POP3-Protokolls empfängt.

Die Viren- und Spyware-Scanfunktion kann jedoch keine E-Mail-Nachrichten in Webmail scannen. Dazu gehören auch E-Mail-Anwendungen, die in Ihrem Webbrowser ausgeführt werden, z. B. Hotmail, Yahoo! mail oder Gmail. Sie sind aber dennoch vor *Viren* geschützt, auch wenn schädliche Anhänge nicht entfernt werden oder Sie Webmail verwenden. Beim Öffnen von E-Mail-Anhang entfernt die Echtzeit-Scanfunktion alle schädlichen Anhänge, bevor diese Schaden anrichten können.

Hinweis: Das Echtzeit-Scanning schützt nur Ihren Computer, jedoch nicht Ihre Freunde. Dabei werden angehängte Dateien erst dann gescannt, wenn Sie den Anhang öffnen. Wenn Sie folglich Webmail verwenden und eine Nachricht weiterleiten, bevor sie den Anhang öffnen, leiten Sie ggf. infizierte E-Mail an Ihre Freunde weiter.

Anzeigen der Scanergebnisse

Im Virus- und Spyware-Verlauf werden alle vom Produkt identifizierten schädlichen Dateien angezeigt.

In manchen Fällen kann das Produkt die Aktion, die sie als Reaktion auf die Identifizierung eines schädlichen Elements ausgewählt haben, nicht durchführen. Wenn Sie z. B. Dateien säubern möchten und eine Datei nicht gesäubert werden kann, wird sie in Quarantäne gestellt. Sie können diese Informationen im Virus- und Spyware-Verlauf anzeigen.

So rufen Sie den Verlauf auf:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Klicken Sie auf **Verlauf der Entfernungsaktionen anzeigen**.

Der Virus- und Spyware-Verlauf enthält folgende Informationen:

- Datum und Uhrzeit der Identifizierung der schädlichen Datei
- Name der Malware und deren Speicherort auf Ihrem Computer
- Durchgeführte Aktion

Ausschließen von Dateien aus dem Scanvorgang

In manchen Fällen müssen bestimmte Dateien oder Anwendungen vom Scanvorgang ausgeschlossen werden. Ausgeschlossene Elemente werden nicht gescannt, bis sie aus der Liste der ausgeschlossenen Elemente wieder entfernt werden.

Hinweis: Für das Echtzeit- und das manuelle Scanning sind separate Ausschlusslisten vorhanden. Wenn Sie beispielsweise eine Datei vom Echtzeit-Scan ausschließen, wird diese beim manuellen Scanning dennoch gescannt, bis Sie sie auch vom manuellen Scanning ausschließen.

Ausschließen bestimmter Dateitypen

Beim Ausschluss von Dateien nach Dateityp werden alle Dateien mit den angegebenen Erweiterungen nicht nach schädlichem Inhalt untersucht.

So fügen Sie auszuschließende Dateitypen hinzu bzw. entfernen Sie sie:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob der Dateityp vom Echtzeit- oder vom manuellen Scanning ausgeschlossen werden soll:
   - Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**, um den Dateityp von Echtzeit-Scans auszuschließen.
   - Wählen Sie **Sonstige Einstellungen** > **Manuelle Scans**, um den Dateityp von manuellen Scans auszuschließen.
3. Klicken Sie auf **Dateien vom Scan ausschließen**.
4. So schließen Sie einen Dateityp aus:
   a) Wählen Sie die Registerkarte **Dateitypen** aus.
   b) Wählen Sie **Dateien mit diesen Erweiterungen ausschließen**.
   c) Geben Sie eine Dateierweiterung, die den Typ der Dateien angibt, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.

      Um Dateien ohne Erweiterung anzugeben, geben Sie '.' ein. Sie können den Platzhalter '?' für ein beliebiges Zeichen verwenden oder den Platzhalter '*' für eine beliebige Anzahl von Zeichen.

      Um beispielsweise ausführbare Dateien auszuschließen, geben Sie in das Feld `exe` ein.
   d) Klicken Sie auf **Hinzufügen**.
5. Wiederholen Sie den vorherigen Schritt für alle anderen Erweiterungen, die Sie aus dem Virenscan ausschließen möchten.
6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die angegebenen Dateitypen werden von allen weiteren Scanvorgängen ausgeschlossen.

Ausschließen von Dateien nach Speicherort

Bei einem Ausschluss von Dateien nach Speicherort werden alle Dateien auf den angegebenen Laufwerken bzw. in den angegebenen Ordnern nicht beim Scanning nach schädlichem Inhalt berücksichtigt.

So fügen Sie vom Scanning auszuschließende Dateispeicherorte hinzu bzw. entfernen Sie sie:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob der Speicherort vom Echtzeit- oder vom manuellen Scanning ausgeschlossen werden soll:
   - Wählen Sie **Computer** > **Viren- und Spyware-Scanning**, um den Speicherort vom Echtzeit-Scanning auszuschließen.
   - Wählen Sie **Computer** > **Manuelles Scanning**, um den Speicherort vom manuellen Scanning auszuschließen.
3. Klicken Sie auf **Dateien vom Scan ausschließen**.
4. So schließen Sie eine Datei, ein Laufwerk oder einen Ordner aus:
   a) Klicken Sie auf die Registerkarte **Objekte**.
   b) Wählen Sie die Option **Objekte ausschließen (Dateien, Ordner, ...)** aus.
   c) Klicken Sie auf **Hinzufügen**.
   d) Wählen Sie die Datei, das Laufwerk oder den Ordner aus, der beim Virenscan nicht berücksichtigt werden soll.

      Hinweis: Einige Laufwerke sind möglicherweise Wechseldatenträger, etwa CDS, DVDs oder Netzwerkdatenträger. Netzwerkdatenträger und leere Wechseldatenträger können nicht ausgeschlossen werden.

   e) Klicken Sie auf **OK**.
5. Wiederholen Sie die vorherigen Schritte, um andere Dateien, Laufwerke oder Ordner vom Scanvorgang auszuschließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen.

Die ausgewählten Dateien, Laufwerke oder Ordner werden von allen weiteren Scanvorgängen ausgeschlossen.

Anzeigen von ausgeschlossenen Anwendungen

Sie können die Anwendungen anzeigen, die Sie vom Scanning ausgeschlossen haben, und sie aus der Liste der ausgeschlossenen Elemente entfernen, wenn sie bei den nächsten Scanvorgängen wieder berücksichtigt werden sollen.

Wenn beim Echtzeit- oder beim manuellen Scanning eine Anwendung identifiziert wird, die sich wie Spyware oder Riskware verhält, von der Sie jedoch wissen, dass sie sicher ist, dann können Sie sie vom Scanning ausschließen. In diesem Fall erhalten Sie keine Warnmeldung bezüglich dieser Anwendung mehr.

Hinweis: Wenn sich eine Anwendung wie ein Virus oder eine andere bösartige Software verhält, kann sie nicht augeschlossen werden.

Sie können Anwendungen nicht direkt ausschließen. Neue Anwendungen werden nur dann in der Ausschlussliste aufgeführt, wenn Sie sie während des Scanvorgangs ausschließen.

So zeigen Sie vom Scanvorgang ausgeschlossene Anwendungen an:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Geben Sie an, ob Sie die vom Echtzeit- oder die vom manuellen Scanning ausgeschlossenen Anwendungen anzeigen möchten:
   - Wählen Sie **Computer** > **Viren- und Spyware-Scanning**, um die vom Echtzeit-Scanning ausgeschlossenen Anwendungen anzuzeigen.
   - Wählen Sie **Computer** > **Manuelles Scanning**, um die vom manuellen Scanning ausgeschlossenen Anwendungen anzuzeigen.

3. Klicken Sie auf **Dateien vom Scan ausschließen**.
4. Wählen Sie die Registerkarte **Anwendungen**.

   Hinweis: Ausgeschlossen werden können Spyware- und Riskware-Anwendungen, nicht aber Viren.

5. Wenn eine ausgeschlossene Anwendung erneut gescannt werden soll:
   a) Wählen Sie die Anwendung, die erneut beim Scanning berücksichtigt werden soll.
   b) Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** zu schließen.
7. Klicken Sie zum Beenden auf **OK**.

Wie verwende ich die Quarantäne?

Als Quarantäne wird ein sicheres Repository für möglicherweise schädliche Dateien bezeichnet.

Dateien, die sich in Quarantäne befinden, können sich weder verbreiten noch Ihrem Computer schaden.

Das Produkt kann *Malware*, *Spyware* und *Riskware* unter Quarantäne stellen, damit sie keinen Schaden anrichten kann. Sie können Anwendungen oder Dateien später aus der Quarantäne wiederherstellen, wenn Sie sie benötigen.

Wenn Sie ein unter Quarantäne stehendes Element nicht benötigen, können Sie es löschen. Das Löschen eines Elements aus der Quarantäne entfernt es endgültig von Ihrem Computer.

- *Malware*, die sich in Quarantäne befindet, können Sie in der Regel löschen.
- *Spyware*, die sich in Quarantäne befindet, können Sie in den meisten Fällen löschen. Es ist möglich, dass die isolierte *Spyware* Teil eines seriösen Softwareprogramms ist und das Löschen dazu führt, dass das Programm nicht mehr richtig ausgeführt werden kann. Wenn Sie das Programm auf Ihrem Computer lassen möchten, können Sie die *Spyware* aus der Quarantäne wiederherstellen.
- *Riskware*, die sich in Quarantäne befindet, kann ein seriöses Softwareprogramm sein. Wenn Sie das Programm selbst installiert und eingerichtet haben, können Sie es aus der Quarantäne wiederherstellen. Wenn die *Riskware* ohne Ihr Wissen installiert wurde, wurde sie sehr wahrscheinlich mit böser Absicht installiert und kann gelöscht werden.

Anzeigen von unter Quarantäne gestellten Elementen

Sie können weitere Informationen zu Elementen unter Quarantäne anzeigen.

So zeigen Sie detaillierte Informationen zu Elementen unter Quarantäne an:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Klicken Sie auf **Quarantäne anzeigen**.
   Die Seite **Quarantäne** zeigt die Gesamtzahl der in der Quarantäne gespeicherten Elemente an.
4. Detaillierte Informationen zu den Elementen unter Quarantäne erhalten Sie unter **Details**.

   Sie können den Inhalt entweder nach Malwarename oder Dateipfad sortieren.

   Es wird eine Liste der ersten 100 Elemente mit dem Typ der in Quarantäne gestellten Elemente, ihrem Namen und dem Pfad angezeigt, unter dem die Dateien gespeichert sind.
5. Wenn Sie weitere Informationen zu einem unter Quarantäne gestellten Element anzeigen möchten, klicken Sie neben dem Element in der Spalte **Status** auf das Symbol ⓘ.

Wiederherstellen von Elementen aus der Quarantäne

Unter Quarantäne gestellte Elemente, die Sie benötigen, können Sie wiederherstellen.

Anwendungen oder Dateien, die Sie benötigen, können Sie aus der Quarantäne wiederherstellen. Stellen Sie keine Elemente aus der Quarantäne wieder her, wenn Sie nicht sicher sind, dass sie keine Bedrohung sind. Wiederhergestellte Elemente werden an den Originalspeicherort auf dem Computer verschoben.

Wiederherstellen von Elementen aus der Quarantäne

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Viren- und Spyware-Scan**.
3. Klicken Sie auf **Quarantäne anzeigen**.
4. Wählen Sie die unter Quarantäne stehenden Elemente aus, die wiederhergestellt werden sollen.
5. Klicken Sie auf **Wiederherstellen**.

Was ist DeepGuard?

DeepGuard analysiert den Inhalt von Dateien sowie das Verhalten von Anwendungen und überwacht nicht vertrauenswürdige Anwendungen.

DeepGuard blockiert neue und unentdeckte *Viren*, *Würmer* und sonstige schädliche Anwendungen, die versuchen, Ihren Computer zu verändern und verhindert, dass verdächtige Anwendungen auf das Internet zugreifen.

Sobald DeepGuard eine neue Anwendung identifiziert, die potenziell schädliche Änderungen am System vorzunehmen versucht, wird die Ausführung der Anwendung in einer Sicherheitszone zugelassen. In dieser Sicherheitszone kann die Anwendung keinen Schaden am Computer anrichten. DeepGuard analysiert die von der Anwendung versuchten Änderungen und entscheidet auf der Grundlage des Analyseergebnisses, ob die Anwendung als *Malware* einzustufen ist. Wenn es sich bei der Anwendung mit großer Wahrscheinlich um *Malware* handelt, wird ihre Ausführung von DeepGuard blockiert.

Folgende Systemänderungen werden von DeepGuard u. a. als potenziell gefährlich eingestuft:

- Änderung von Systemeinstellungen (Windows-Registry),
- Versuche, wichtige Systemprogramme zu beenden, wie z. B. Sicherheitsprogramme wie dieses, und
- Versuche, wichtige Systemdateien zu verändern.

Aktivieren oder Deaktivieren von DeepGuard

DeepGuard sollte stets aktiviert sein, damit verdächtige Anwendungen keine potenziell schädigenden Systemänderungen auf Ihrem Computer vornehmen können.

Wenn Sie mit Windows XP arbeiten, müssen Sie sicherstellen, dass das Service Pack 2 installiert wurde, bevor Sie DeepGuard aktivieren.

So aktivieren bzw. deaktivieren Sie DeepGuard:

1. Klicken Sie auf der Haupseite auf **Status**.
2. Klicken Sie auf **Einstellungen auf dieser Seite ändern**.

   Hinweis: Sie benötigen Administrator-Zugriffsrechte, um die Sicherheitsfunktionen deaktivieren zu können.

3. Aktivieren oder deaktivieren Sie **DeepGuard**.
4. Klicken Sie auf den Link **Schließen**.

Zulassen der von DeepGuard blockierten Anwendungen

Sie können bestimmen, welche Anwendungen von DeepGuard zugelassen und blockiert werden.

Es kann vorkommen, dass DeepGuard die Ausführung einer sicheren Anwendung verhindert, obwohl Sie mit dieser Anwendung arbeiten möchten und genau wissen, dass sie sicher ist. Das ist darauf zurückzuführen, dass die Anwendung versucht, Systemänderungen vorzunehmen, die sich als potenziell schädlich erweisen könnten. Oder Sie haben die Anwendung bei der Anzeige eines DeepGuard-Popupfensters versehentlich blockiert.

So genehmigen Sie die Ausführung einer von DeepGuard blockierten Anwendung:

1. Klicken Sie auf der Hauptseite auf **Tools**.
2. Klicken Sie auf **Anwendungen**.
   Die Liste **Überwachte Anwendungen** wird angezeigt.
3. Identifizieren Sie die Anwendung, deren Ausführung Sie genehmigen möchten.

   Hinweis: Sie können die Liste durch einen Klick auf die verschiedenen Spaltenüberschriften sortieren. Wenn Sie z. B. auf die Spalte **Genehmigung** klicken, wird die Liste nach genehmigten und zurückgewiesenen Programmen sortiert.

4. Wählen Sie **Zulassen** in der Spalte **Genehmigung**.
5. Klicken Sie auf den Link **Schließen**.

DeepGuard lässt erneut Systemänderungen durch die Anwendung zu.

Verwenden von DeepGuard im Kompatibilitätsmodus

Um maximalen Schutz zu gewährleisten, nimmt DeepGuard an aktiven Programmen temporäre Änderungen vor. Bestimmte Programme überprüfen allerdings, ob sie nicht beschädigt oder geändert wurden, und sind deshalb unter Umständen nicht mit dieser Funktion kompatibel. Online-Spiele mit Anti-Betrug-Tools z. B. prüfen, ob sie bei ihrer Ausführung nicht auf die eine oder andere Weise geändert wurden. In diesem Fall können Sie den Kompatibilitätsmodus aktivieren.

So aktivieren Sie den Kompatibilitätsmodus:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **DeepGuard**.
3. Wählen Sie **Kompatibilitätsmodus verwenden**.
4. Klicken Sie auf **OK**.

Handhabung von Warnmeldungen zu verdächtigem Verhalten

DeepGuard überwacht nicht vertrauenswürdige Anwendungen. Wenn eine überwachte Anwendung versucht, auf das Internet zuzugreifen, Änderungen an Ihrem System vorzunehmen oder sich verdächtig verhält, wird sie von DeepGuard blockiert.

Wenn Sie in den DeepGuard-Einstellungen die Option **Warnmeldung bei verdächtigem Verhalten anzeigen** gewählt haben, erhalten Sie von DeepGuard eine Warnmeldung, wenn eine potenziell schädliche Anwendung identifiziert wird oder Sie versuchen, eine Anwendung mit unbekanntem Ruf auszuführen.

So geben Sie an, wie eine von DeepGuard blockierte Anwendung gehandhabt werden soll:

1. Klicken Sie auf **Details**, um mehr Informationen zum Programm anzuzeigen.
   Der Detailbereich enthält folgende Angaben:
   - Speicherort der Anwendung
   - Ruf der Anwendung im Realtime Protection Network
   - Verbreitung der Anwendung
2. Geben Sie an, ob Sie der von DeepGuard blockierten Anwendung vertrauen:
   - Wählen Sie **Ich vertraue der Anwendung. Ausführung fortsetzen.**, wenn die Anwendung nicht blockiert werden soll.

     In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit sicher:
     - DeepGuard hat die Anwendung nach einer von Ihnen durchgeführten Aktion blockiert.
     - Sie kennen die Anwendung.
     - Sie haben die Anwendung von einer vertrauenswürdigen Quelle erhalten.
   - Wählen Sie **Ich vertraue der Anwendung nicht. Ausführung blockieren.**, wenn die Anwendung blockiert werden soll.

     In folgenden Fällen ist eine Anwendung mit großer Wahrscheinlichkeit nicht sicher:
     - Die Anwendung ist nicht sehr geläufig.
     - Der Ruf der Anwendung ist nicht bekannt.
     - Sie kennen die Anwendung nicht.
3. Sie möchten eine verdächtige Anwendung einer Analyse unterziehen:
   a) Klicken Sie auf **Anwendung bei F-Secure melden**.
   Das Produkt zeigt die Bedingungen für eine Übertragung an.
   b) Klicken Sie auf **Akzeptieren**, wenn Sie die Bedingungen anerkennen und das Probeexemplar übertragen möchten.

   In folgenden Fällen sollten Sie ein Probeexemplar übertragen:
   - DeepGuard blockiert einen Anwendung, von der Sie wissen, dass sie sicher ist.
   - Sie haben den Verdacht, dass es sich bei der Anwendung um *Malware* handeln könnte.

Was ist eine Firewall?

Die *Firewall* verhindert das Eindringen von Hackern und schädlichen Anwendungen über das Internet in Ihren Computer.

Firewalls lassen nur sichere Internetverbindungen auf Ihrem Computer zu und blockieren unberechtigte Eingriffe über das Internet.

Aktivieren oder Deaktivieren der Firewall

Die Firewall sollte stets aktiviert sein, um ungewollten Zugriff auf Ihren Computer zu verhindern.

So aktivieren bzw. deaktivieren Sie die Firewall:

1. Klicken Sie auf der Haupseite auf **Status**.
2. Klicken Sie auf **Einstellungen auf dieser Seite ändern**.

   Hinweis: Sie benötigen Administrator-Zugriffsrechte, um die Sicherheitsfunktionen deaktivieren zu können.

3. Aktivieren bzw. deaktivieren Sie **Firewall**.

   Hinweis: Ihr Computer ist nicht vollständig geschützt, wenn Sie die Sicherheitsfunktionen deaktivieren.

4. Klicken Sie auf den Link **Schließen** aus.

Sie sollten die *Firewall* nicht deaktivieren, da Sie dadurch Ihren Computer ungeschützt Netzwerkangriffen aussetzen. Wenn eine Anwendung nicht ausgeführt werden kann, da sie auf das Internet zugreifen muss, deaktivieren Sie keinesfalls die *Firewall*, sondern ändern Sie die *Firewall-Einstellungen* entsprechend.

Ändern der Firewall-Einstellungen

Wenn die Firewall aktiviert ist, begrenzt sie den Zugriff von Ihrem Computer sowie auf Ihren Computer. Für manche Anwendungen müssen Sie ggf. die Firewall durchlässig machen, damit sie ordnungsgemäß funktionieren.

Das Produkt greift für den Schutz Ihres Computers auf die Windows Firewall zurück.

So ändern Sie die Einstellungen für die Windows Firewall:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Firewall**.
3. Klicken Sie auf die Einstellungen **Windows Firewall ändern**.

   Hinweis: Sie benötigen Administrator-Zugriffsrechte, um die Einstellungen bearbeiten zu können.

Detaillierte Informationen zur Windows Firewall finden Sie in der Dokumentation von Microsoft Windows.

Verhindern, dass Anwendungen schädliche Dateien herunterladen

Sie können verhindern, dass Anwendungen auf Ihrem Computer schädliche Dateien aus dem Internet herunterladen.

Manche Websites nutzen Sicherheitslücken des Comupters aus oder enthalten schädliche Dateien, die Ihren Computer beschädigen können. Mit dem erweiterten Netzwerkschutz verhindern Sie, dass Anwendungen schädliche Dateien herunterladen, noch bevor diese auf Ihrem Computer gespeichert werden.

So verhindern Sie, dass Anwendungen schädliche Dateien herunterladen:

1. Klicken Sie auf der Hauptseite auf **Einstellungen**.

   Hinweis: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.

2. Wählen Sie **Computersicherheit** > **Firewall**.
3. Wählen Sie **Nicht zulassen, dass Anwendungen schädliche Dateien herunterladen**.

Hinweis: Diese Einstellung gilt auch dann, wenn Sie die Firewall deaktivieren.

Blockieren von Spams

Der Spam- und Phishing-Filter schützt Ihren Computer vor E-Mail-Nachrichten, bei denen es sich in Wahrheit um *Spams* und *Phishing*-Versuche handelt.

Eine E-Mail-Nachricht wird als *Spam* eingestuft, wenn sie als Teil einer umfangreichen Gruppe von Nachrichten mit nahezu identischem Inhalt gesendet wird und die Empfänger keine überprüfbare Genehmigung für die Übertragung der Nachricht erteilt haben. Eine große Anzahl von *Spam*- und *Phishing*-Nachrichten überdeckt häufig erwünschte E-Mail-Nachrichten.

Verwenden Sie die Spam- und Phishing-Filterung, um Spam- und Phishing-Nachrichten zu erfassen und sie im *Spam*-Ordner abzulegen.

Aktivieren oder Deaktivieren der Spam- und Phishing-Filterung

Die Spam- und Phishing-Filterung sollte stets aktiviert sein, damit Spam- und Phishing-Nachrichten aus dem Posteingang entfernt werden.

So aktivieren bzw. deaktivieren Sie die Spam- und Phishing-Filterung:

1. Klicken Sie auf der Haupseite auf **Status**.
2. Klicken Sie auf **Einstellungen auf dieser Seite ändern**.

   Hinweis: Sie benötigen Administrator-Zugriffsrechte, um die Sicherheitsfunktionen deaktivieren zu können.

3. Aktivieren oder deaktivieren Sie **Spam- und Phishing-Filter**.
4. Klicken Sie auf den Link **Schließen**.

Schutz gegen Phishing-Versuche

Der Spam- und Phishing-Filter schützt Ihren Computer vor *Phishing*-Versuchen, die falsche E-Mail-Nachrichten verwenden und von legitimen Firmen zu stammen scheinen, um Ihre persönlichen Daten zu stehlen.

Diese authentisch wirkenden Nachrichten sollen Sie dazu veranlassen, Ihre persönlichen Daten preiszugeben, beispielsweise Ihre Bankkontonummern, Passwörter und Kreditkarten- oder Krankenversicherungsnummern. Der Inhalt von E-Mail-Nachrichten, die vom Spam- und Phishing-Filter erfasst wurden, ist keinesfalls vertrauenswürdig.

Wenn Sie eine E-Mailnachricht erhalten, die als *Phishing*-Versuch identifiziert wurde, wird diese automatisch im *Spam*-Ordner abgelegt.

In Microsoft Outlook, Outlook Express und Windows Mail werden die *Phishing*-Regeln automatisch erstellt. Falls Sie ein anderes E-Mail-Programm verwenden, müssen Sie die Filterregeln manuell erstellen.

Einrichten meiner E-Mail-Programme zum Spam-Filtern

Sie können in Ihrem E-Mail-Programm einen *Spam*- und einen *Phishing*-Ordner anlegen und Filterregeln erstellen, um *Spam* zu filtern.

Das E-Mail-Filtern erstellt automatisch in Microsoft Outlook, Microsoft Outlook Express und Windows Mail (bei Windows Vista)einen *Spam*- und einen *Phishing* -Ordner und Filterregeln. Wenn Sie ein anderes E-Mail-Programm verwenden, müssen Sie die Ordner und die Filterregeln von Hand erstellen. Wenn Sie mehrere E-Mail-Konten haben, müssen Sie für jedes Konto separate Filterregeln erstellen.

Hinweis: *Spam*- und *Phishing*-Filterung unterstützt nur das POP3-Protokoll. Webbasierte E-Mail-Programme oder andere Protokolle werden nicht unterstützt.

Wie funktioniert das Zusammenspiel zwischen meinen eigenen Filterregeln und den E-Mail-Filterregeln?	Das E-Mail-Filtern filtert E-Mail-Nachrichten auf Grundlage eigener Filterregeln.Es filtert keine E-Mail-Nachrichten, die einer von Ihnen erstellten Regel entsprechen. Wenn Sie beispielsweise eine Regel erstellt haben, die alle E-Mail-Nachrichten von einem Webstore in den Webstore-Ordner filtert, werden sowohl Ihre Nachrichten bezüglich

Auftragsbestätigungen als auch Werbematerial aus diesem Webstore aus Ihrem Posteingang entfernt und in den Webstore-Ordner verschoben.

Dieser Abschnitt enthält eine Anleitung zum Erstellen des Spam-Ordners und der Filterregel für Microsoft E-Mail-Programme, Netscape, Mozilla Thunderbird und Eudora. Sie können anhand dieser Anleitung auch in anderen E-Mail-Programmen vergleichbare Filterregeln erstellen.

Microsoft E-Mail-Programme

Der E-Mail-Filter erstellt Ordner für *Spam*- und *Phishing*-E-Mails. Die Filterregeln gelten automatisch für Microsoft Outlook, Microsoft Outlook Express undWindows Mail.

Hinweis: Bei E-Mail-Konten, die mit dem E-Mail-Applet der Windows-Systemsteuerung erstellt wurden, funktioniert das automatische Filtern möglicherweise nicht. Wenn Sie Spam- und Phishing-Nachrichten erhalten, nachdem Sie den E-Mail-Filter aktiviert haben, verwenden Sie den Nachrichtenbetreff `[SPAM]`, um Spam- und Phishing-Nachrichten zu filtern.

Blockieren von Spams in Mozilla Thunderbird und Eudora OSE

Suchtitel: Erstellen von Spam-Filterregeln in Mozilla Thunderbird und Eudora OSE.

Um *Spam*- und Phishing-E-Mails zu filtern, müssen Sie einen Spam-Ordner und die Filterregel erstellen.

So erstellen Sie eine *Spam*-Filterregel:

1. Klicken Sie rechts auf **Lokale Ordner** und wählen Sie **Neuer Ordner**.
2. Geben Sie `Spam` als neuen Ordnernamen ein.
3. Wählen Sie **Extras** > **Nachrichtenfilter**.
4. Klicken Sie auf **Neu**.
5. Geben Sie `Spam` als **Filtername** ein.
6. Erstellen Sie eine entsprechende Regel, um Spam-Nachrichten zu finden:
   a) Stellen Sie sicher, dass bei den Filteroptionen **Betreff** und **enthält** ausgewählt sind.
   b) Geben Sie im dritten Feld `[SPAM]` ein.
7. Erstellen Sie eine Aktivität, die Spam-Nachrichten in den Spam-Ordner verschiebt:
   a) Wählen Sie in der ersten Liste **Nachricht verschieben nach**.
   b) Wählen Sie den *Spam*-Ordner in der zweiten Dropdown-Liste aus.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.
9. Schließen Sie das Dialogfenster **Nachrichtenfilter**.

Sie haben jetzt die *Spam*-Filterregel erstellt. Ab sofort werden *Spam*-E-Mails in den *Spam*-Ordner gefiltert.

Blockieren von Spams in Opera.

Suchtitel: Erstellen von Spam-Filterregeln in Opera.

Um *Spam*- und Phishing-E-Mails zu filtern, müssen Sie einen Spam-Ordner und die Filterregel erstellen.

Hinweis: Die hier angegebenen Schritte beziehen sich auf Opera Version 11. Die Schritte für andere Versionen können leicht abweichen.

So erstellen Sie eine *Spam*-Filterregel:

1. Öffnen Sie **Opera Mail**.
2. Klicken Sie rechts auf Ihren standardmäßigen *Spam*-Ordner und wählen Sie **Eigenschaften**.
3. Klicken Sie auf **Regel hinzufügen**.
4. Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht in den *Spam*-Filter:
   a) Stellen Sie sicher, dass bei den Filteroptionen **Betreff** und **enthält** ausgewählt sind.
   b) Geben Sie im dritten Feld `[SPAM]` ein.

5. Klicken Sie auf **Schließen**, um Ihre neue *Spam*-Filterregel zu bestätigen.

Sie haben jetzt die *Spam*-Filterregel erstellt. Ab sofort werden *Spam*-E-Mails in den *Spam*-Ordner gefiltert.

Kapitel

5

Sichere Nutzung des Internets

Themen:

- *Ausführen allgemeiner Aufgaben*
- *Schützen von verschiedenen Benutzerkonten*
- *Was ist Surfschutz*
- *Sicheres Surfen*
- *Online-Zeiten festlegen*
- *Anzeigen der Statistik*

Erste Schritte mit dem Produkt

Mithilfe dieses Produkts surfen Sie sicher im Web. Zusätzlich schützen Sie sich gegen schädliche Software und Webseiten und können außerdem festlegen, welche Inhaltstypen von den verschiedenen Benutzerkonten angezeigt werden können.

Das Produkt verwendet Windows-Benutzerkonten, um die Einstellungen für jede Person, die den Computer verwendet, zu überwachen. Nur Benutzer mit Administratorrechten können die Produkteinstellungen für die verschiedenen Windows-Benutzerkonten ändern. Wir empfehlen Ihnen, für jede Person, die den Computer verwendet, ein separates Windows-Benutzerkonto auf Ihrem Computer einzurichten. Beispielsweise sollten Gäste keine Administratorrechte für Ihr Windows-Benutzerkonto haben.

Ausführen allgemeiner Aufgaben

Auf der Seite **Aufgaben** können Sie sehen, was Sie mit dem Produkt tun können, und häufige Aufgaben ausführen.

So öffnen Sie die Seite **Aufgaben**:

Klicken Sie auf der Hauptseite auf **Tools**.

Die Seite **Aufgaben** wird geöffnet.

Schützen von verschiedenen Benutzerkonten

Um den bestmöglichen Schutz gegen Online-Bedrohungen zu gewährleisten, sollten Sie separate Windows-Benutzerkonten für jeden Benutzer des Computers verwenden.

Mithilfe des Produkts können Sie verschiedene Einstellungen für die jeweiligen Benutzerkonten auf Ihrem Computer einrichten. Nur Benutzer mit Administratorrechten können die Produkteinstellungen für andere Benutzerkonten ändern. Alle Benutzer, mit Ausnahme des Administrators, sollten nur über normale Zugriffsrechte verfügen, damit Sie nicht die von Ihnen festgelegten Einstellungen ändern können.

Erstellen und Bearbeiten von Windows-Benutzerkonten

Sie können über das Produkt auf die Einstellungen der Windows-Benutzerkonten zugreifen.

So erstellen oder bearbeiten Sie Windows-Benutzerkonten:

1. Klicken Sie auf der Hauptseite auf **Tools**.
2. Klicken Sie auf **Neues Konto erstellen** oder auf **Benutzerkonten bearbeiten**.
   Hierüber werden die Benutzerkonteneinstellungen in Windows geöffnet.
3. Geben Sie die erforderlichen Informationen ein, um das Benutzerkonto zu erstellen oder zu bearbeiten.

Was ist Surfschutz

Der Surfschutz erlaubt Ihnen, die Sicherheit von Webseiten, die Sie besuchen, zu beurteilen und bewahrt Sie so davor, unabsichtlich auf schädliche Webseiten zuzugreifen.

Browsing Protection ist ein Browser-Plug.in, das Ihnen Sicherheitsbewertungen für Webseiten anzeigt, die in den Ergebnissen von Suchmaschinen aufgelistet werden. Browsing Protection hilft Ihnen, Websites zu vermeiden, die Sicherheitsbedrohungen aufweisen, wie beispielsweise Malware (Viren, Würmer, Trojaner) und Phishing. So schützen Sie die Sicherheitsbewertungen von Browsing Protection vor den neuesten Sicherheitsbedrohungen im Internet, die noch nicht durch herkömmliche Antiviren-Programme erkannt werden.

Es gibt vier verschiedene Sicherheitsbewertungen für Webseiten: sicher, verdächtig, schädlich und unbekannt. Diese Sicherheitsbewertungen basieren auf Informationen aus verschiedenen Quellen, wie z. B. Malware-Analytikern von F-Secure selbst oder seinen Partnern oder von anderen Surfschutz-Benutzern.

Den Surfschutz ein- oder ausschalten

Wenn der Surfschutz eingeschaltet ist, wird Ihr Zugriff auf schädliche Webseiten blockiert.

So wird der Surfschutz ein- oder ausgeschaltet:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie auf die Schaltfläche neben **Browser-Schutz**.
   Je nach vorheriger Einstellung ist nun der Browser-Schutz für diesen Benutzer entweder aktiviert oder deaktiviert.
3. Wenn Ihr Browser geöffnet sie, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

Surfschutz-Sicherheitsbewertungen

Browsing Protection zeigt Sicherheitsbewertungen für Websites in Suchmaschinenergebnissen an.

Farbcodierte Symbole zeigen die Sicherheitsbewertung der aktuellen Seite an (in der Toolbar). Die Sicherheitsbewertung jedes Links in den Ergebnissen der Suchmaschine wird ebenfalls mit den gleichen Symbolen angezeigt. Es werden vier verschiedene farbcodierte Symbole verwendet:

- Ein grünes bedeutet, dass die Seite sicher ist.
- Ein orangenes bedeutet, dass die Seite verdächtig ist. Gemäß der Sicherheitsanalyse der Seite ist sie sicher; sie hat jedoch von vielen Nutzern eine niedrige Sicherheitsbewertung erhalten.
- Ein rotes bedeutet, dass die Seite schädlich ist.
- Ein graues bedeutet, dass die Seite noch nicht analysiert wurde und dass derzeit keine Informationen über sie vorliegen.

Sicherheitsbewertungen sind auf den folgenden Suchseiten verfügbar:

- Google
- MSN Live
- Yahoo

Abhängig von Ihren Surfschutz-Einstellungen können Sie auch auf Webseiten zugreifen, die als unsicher eingestuft worden sind. Diese Webseiten werden entweder automatisch blockiert oder Sie werden nur auf ein mögliches Risiko hingewiesen.

Beurteilungen für Weblinks anzeigen

Browsing Protection-Bewertungen können für Suchmaschinenergebnisse angezeigt werden.

So legen Sie fest, wo Surfschutz-Bewertungen angezeigt werden:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie auf **Einstellungen** neben **Browser-Schutz**.
   Das Dialogfenster **Browser-Schutz** wird geöffnet.
3. Aktivieren oder deaktivieren Sie unter **Bewertungen anzeigen** die Option **Suchmaschinenergebnisse (Google, Yahoo)**.
   Wenn diese Option ausgewählt ist, werden Surfschutz-Bewertungen für die von Suchmaschinen aufgelisteten Webseiten angezeigt (Google, Yahoo usw.).
4. Klicken Sie auf **OK**.

Sicherheitsbewertungen werden entsprechend den von Ihnen ausgewählten Einstellungen angezeigt.

Tipp: Sie können auf **Sicherheitszusammenfassung für diese Webseite** im Pop-up-Menü Sicherheitsbewertung klicken, um zum Surfschutz-Portal zu gelangen, wo Sie weitere Einzelheiten über die Webseite finden sowie Informationen dazu, worauf die Sicherheitsbewertung beruht.

Die Bewertung von Webseiten

Sie können jede Webseite, auf die Sie zugreifen, als sicher oder schädlich bewerten.

So bewerten Sie eine Webseite:

1. Wählen Sie **Verständigen Sie uns** aus dem Menü "Browser-Schutz" in Ihrem Browser aus.
   Das Dialogfeld **Verständigen Sie uns** öffnet sich.
2. Wählen Sie eine Bewertung, um Ihre Einschätzung der Sicherheit einer Webseite abzugeben (**Sie ist sicher**, **Sie ist schädlich** oder **Ich weiß nicht**).
3. Klicken Sie auf **OK**.
   Das Dialogfeld für die Bewertungsbestätigung wird geöffnet.

   Tipp: Wählen Sie **Diese Meldung nicht wieder anzeigen**, wenn Sie das Bestätigungs-Dialogfeld nicht mehr sehen möchten, wenn Sie in Zukunft Webseiten bewerten.

4. Klicken Sie auf **OK**.

Ihre Bewertung wird nun den Analyse- und Bewertungsinformationen, die über diese Webseite gesammelt werden, hinzugefügt.

Schutz gegen schädlichen Inhalt

Der Surfschutz blockiert den Zugriff auf unsichere Webseiten auf der Grundlage der ausgewählten Einstellungen.

So bestimmen Sie, wann der Zugriff auf eine Webseite blockiert wird:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie auf **Einstellungen** neben **Browser-Schutz**.
   Das Dialogfenster **Browser-Schutz** wird geöffnet.
3. Wählen Sie **Websites, die als schädlich eingestuft sind** aus, um den Zugriff auf Websites, die als schädlich eingestuft wurden, zu sperren.
4. Klicken Sie auf **OK**.

Der Browser-Schutz sperrt den Zugriff auf Websites gemäß den ausgewählten Einstellungen.

Was tun, wenn eine Webseite blockiert wird

Es erscheint eine Surfschutz-Blockierungsseite, wenn Sie versuchen, auf eine Webseite zuzugreifen, die als schädlich eingestuft wurde.

Wenn eine Blockierungsseite erscheint:

1. Klicken Sie auf **Startseite**, um auf Ihre Homepage zuzugreifen, ohne die schädliche Website aufzurufen.
   Wir empfehlen Ihnen diese Maßnahme dringend.

   Tipp: Sie können auf **Sicherheitszusammenfassung für diese Webseite** klicken, um zum Surfschutz-Portal zu gehen, wo Sie weitere Einzelheiten über die Webseite finden sowie Informationen dazu, worauf die Sicherheitsbewertung beruht.

2. Wenn Sie dennoch auf diese Website zugreifen möchten, klicken Sie auf **Website aufrufen**.

Sicherheitszusammenfassung für eine Webseite

Eine Zusammenfassung der Bewertungsinformationen für alle überprüften Webseiten ist im Surfschutz-Portal verfügbar.

In der Sicherheitszusammenfassung finden Sie weitere Details dazu, worauf die Sicherheitsbewertung beruht. Beispielsweise kann die Sicherheitszusammenfassung zeigen, ob die Sicherheitsbewertung auf Malware beruht, also bösartiger Software, die auf der Website gefunden wurde, auf schlechten Bewertungen durch andere Benutzer oder auf beidem. Auf die Sicherheitszusammenfassung kann aus verschiedenen Richtungen zugegriffen werden:

- Vom Sicherheitsbewertungsmenü in der Symbolleiste,
- vom Pop-up-Menü Sicherheitsbewertung für Webseiten-Links und
- vom Link Sicherheitszusammenfassung auf Webseiten, die durch Surfschutz blockiert wurden.

Durch Klicken auf einen beliebigen dieser Links gelangen Sie zum Surfschutz-Portal, wo Sie Details zur Sicherheitsbewertung der Webseite einsehen können.

Sicheres Surfen

Sie können sich vor vielen dieser Internetbedrohungen schützen, indem Sie die Surfaktivitäten aller Ihrer Windows-Benutzerkonten auf Ihrem Computer überwachen.

Das Internet enthält viele interessante Webseiten, aber es lauern auch viele Risiken. Viele Webseiten enthalten Materialien, die Sie möglicherweise als unangemessen empfinden. Benutzer können auf unangemessene Materialien stoßen oder belästigende Nachrichten per E-Mail oder in einem Chat erhalten. Sie können versehentlich Dateien herunterladen, die für den Computer schädliche *Viren* enthalten.

Hinweis: Das Einschränken von Online-Inhalten schützt Ihre Benutzerkonten vor Chat- und E-Mail-Programmen, die in Ihrem Webbrowser ausgeführt werden. Über die Application Control-Sicherheitskomponente können Sie den Zugriff auf andere Chat- oder E-Mail-Programme blockieren.

Sie können die anzeigbaren Webseiten einschränken und die Zeit festlegen, die zum Surfen zur Verfügung steht. Diese Einschränkungen gelten für Windows-Benutzerkonten. Sobald sich jemand mit seinem eigenen Benutzerkonto anmeldet, gelten diese Einschränkungen.

Beschränken des Zugriffs auf Webinhalte

Sie können die Filterart auswählen, die Sie für die verschiedenen Windows-Benutzerkonten verwenden möchten.

Der Webseitenfilter blockiert den Zugriff auf von Ihnen nicht zugelassene Webseiten oder auf Webseiten, die Inhalte enthalten, die Sie blockiert haben.

Zugriff auf Webseiten ermöglichen

Sie können den Zugriff auf die Webseiten eingrenzen, denen Sie vertrauen. Fügen Sie diese hierzu zur Liste der zulässigen Webseiten hinzu.

So gewähren Sie Zugriff auf bestimmte Webseiten:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen** neben **Webseitenfilter**.
   Der Assistent für den Webfilter wird geöffnet.
3. Klicken Sie auf der ersten Seite auf **Weiter**.
4. Wählen Sie **Nur ausgewählte Websites zulassen** aus und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Hinzufügen**, um Websites zur Liste **Zugelassene Websites** hinzuzufügen.
6. Sobald Sie alle zulässigen Webseiten hinzugefügt haben, klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**, um den Webfilter-Assistenten zu schließen.

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er auf die Webseiten zugreifen, die Sie zur Liste der zulässigen Webseiten hinzugefügt haben.

Webseiten anhand ihres Inhalts sperren

Über die Webfilterung können Sie den Zugriff auf Websites und Seiten zulassen, sperren oder einfach protokollieren.

So wählen Sie die zulässigen Inhaltstypen aus:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie auf **Einstellungen** neben **Webseitenfilter**.
   Der Assistent für den Webfilter wird geöffnet.
3. Klicken Sie auf der ersten Seite auf **Weiter**.
4. Wählen Sie **Surfen nach Inhalten** aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite **Eingeschränkte Web-Inhalte** die zu blockierenden Inhaltstypen aus.
6. Wenn Sie alle Inhaltstypen ausgewählt haben, die Sie sperren möchten, klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**, um den Webfilter-Assistenten zu schließen.

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er nicht auf Webseiten zugreifen, die Inhaltstypen enthalten, die Sie blockiert haben.

Zugelassene und blockierte Websites bearbeiten

Sie können bestimmte Websites auswählen, die von der Webfilterung blockiert werden. Sie können auch einzelne Websites blockieren, die in keinem Webfilter-Inhaltstyp eingeschlossen sind.

Möglicherweise stufen Sie eine Webseite als sicher ein, obwohl Sie andere Webseiten mit diesem Inhaltstyp blockieren möchten. Sie können ebenso eine bestimmte Webseite blockieren, obwohl andere Webseiten dieses Inhaltstyps zulässig sind.

Website zulassen oder blockieren:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten und klicken Sie dann auf **Website-Liste öffnen**.

   Wird die Website, die Sie bearbeiten möchten, bereits als zugelassen oder blockiert aufgelistet und Sie möchten diese von einer zur anderen Liste verschieben, gehen Sie folgendermaßen vor:

   a) Klicken Sie abhängig von der Website-Liste, die Sie bearbeiten möchten auf die Registerkarte **Zulassen** oder **Blockieren**.
   b) Klicken Sie mit der rechten Maustaste auf die Website in der Liste und wählen Sie **Zulassen** oder **Blockieren**.

   Ist die Website in keiner Liste enthalten, gehen Sie folgendermaßen vor:

   a) Klicken Sie auf die Registerkarte **Zulassen**, wenn Sie eine Website zulassen möchten. Klicken Sie auf die Registerkarte **Blockieren**, wenn Sie eine Website sperren möchten.
   b) Klicken Sie auf **Hinzufügen**, um die neue Website zur Liste hinzuzufügen.
   c) Geben Sie im Dialogfeld **Website hinzufügen** die Adresse der Website ein, die Sie hinzufügen möchten und klicken Sie auf **OK**.
3. Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren.

Um die Adresse einer zugelassenen oder blockierten Website zu ändern, klicken Sie mit der rechten Maustaste auf die Website in der Liste und wählen Sie die Option **Bearbeiten**.

Um eine zugelassene oder blockierte Website von der Liste zu entfernen, wählen Sie die entsprechende Website aus und klicken Sie auf **Entfernen**.

Online-Zeiten festlegen

Sie können die Zeit kontrollieren, die mit dem Surfen im Internet über Ihren Computer verbracht werden darf.

Sie können für jedes Windows-Benutzerkonto unterschiedliche Einschränkungen auf Ihrem Computer einrichten. Folgendes können Sie kontrollieren:

- Wenn jemand im Internet surfen darf, können Sie beispielsweise festlegen, dass das Surfen nur vor 8 Uhr abends möglich ist.
- Wie lange jemand im Internet surfen darf. Sie können beispielsweise festlegen, dass täglich nur eine Stunde im Internet gesurft werden darf.

Hinweis: Wenn Sie die Zeitbeschränkungen aufheben, ist das Surfen im Internet ohne zeitliche Einschränkungen möglich.

Wenn die Einschränkung der Surfzeit die Verbindung zum Internet blockiert, gibt eine entsprechende Anzeige im Webbrowser an, wann Sie wieder auf das Internet zugreifen können. Falls Ihr Windows-Benutzerkonto über Administratorzugriffsrechte verfügt, können Sie die Surfzeit ausdehnen, indem Sie das Passwort Ihres Windows-Benutzerkontos eingeben und mehr Zeit auswählen.

Tägliche Internetzeiten einschränken

Sie können tägliche Zeitbeschränkungen verwenden, um den Internetzugriff einzugrenzen.

Sie können auf Ihrem Computer unterschiedliche zeitliche Beschränkungen für jedes Windows-Benutzerkonto einrichten.

So richten Sie zeitliche Beschränkungen ein:

1. Klicken Sie auf der Hauptseite auf **Benutzer**.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie auf **Einstellungen** neben **Zeitbeschränkungen**.
   Der Assistent **Surfzeiten einschränken** wird geöffnet.
3. Klicken Sie auf der ersten Seite auf **Weiter**.
4. Wählen Sie in der Tabelle **Surfen zu diesen Zeiten erlauben** die Uhrzeiten aus, zu denen am jeweiligen Tag das Surfen im Internet erlaubt ist.
5. Klicken Sie auf **Weiter**, wenn Sie die zulässigen Surfzeiten eingerichtet haben.
6. Wählen Sie aus, wie viele Stunden an Wochentagen und an Wochenenden gesurft werden dürfen. Klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**, um den Assistenten für die Einrichtung der Surfzeiten zu schließen.

Wenn sich jemand mit dem von Ihnen bearbeiteten Windows-Benutzerkonto auf Ihrem Computer anmeldet, kann er nur während zu den zulässigen Zeiten im Internet surfen.

Anzeigen der Statistik

Auf der Seite **Statistik** können Sie sehen, welche Webseiten angezeigt und blockiert wurden.

Das Produkt sammelt Informationen zu besuchten und blockierten Websites. Diese Informationen sind benutzerspezifisch und werden für jedes Windows-Benutzerkonto erstellt.

Blockierte Websites werden unterteilt in Websites, die durch den Webseitenfilter blockiert wurden und Websites, die durch den Browser-Schutz blockiert wurden. So sehen Sie, ob eine blockierte Seite Inhalte aufweist, die Sie absichtlich blockiert haben, oder ob das Produkt die Seite als potenziell schädlich identifiziert hat.