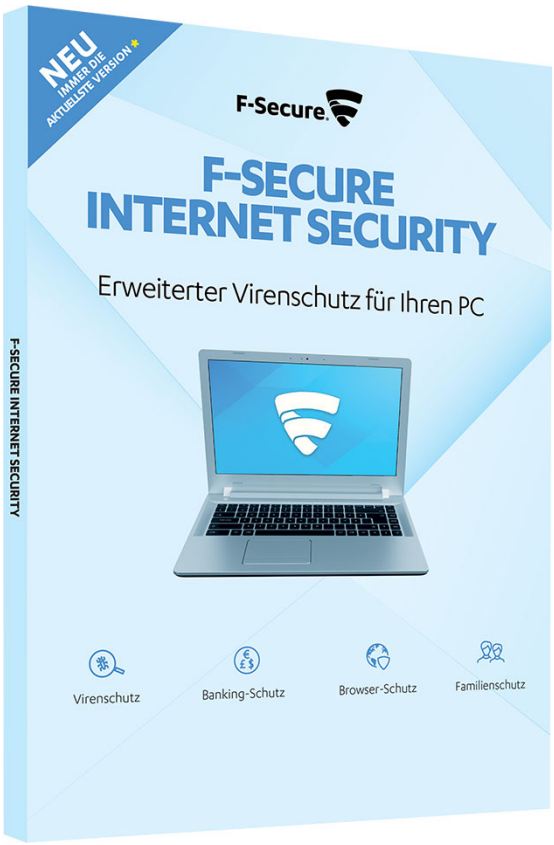
Handbuch
F-Secure Internet Security



Inhalt

Installation

Themen:

1.1 Vor der ersten Installation

Vielen Dank, dass Sie sich für unser Produkt entschieden haben.

Um das Produkt zu installieren, benötigen Sie Folgendes:

- Die Installations-CD oder ein Installationspacket.
- Ihr Abonnementschlüssel
- Eine Internetverbindung.

Wenn Sie ein Sicherheitsprodukt von einem anderen Anbieter verwenden, wird das Installationsprogramm versuchen, dieses automatisch zu entfernen. Sollte dies nicht automatisch geschehen, entfernen Sie es bitte manuell.

Hinweis: Wenn auf dem Computer mehr als ein Konto vorhanden ist, melden Sie sich bei der Installation mit Administratorrechten an.

1.2 Erstmalige Installation des Produkts

Anweisungen zur Produktinstallation.

Befolgen Sie diese Anweisungen, um das Produkt zu installieren:

1. Legen Sie die CD ein oder doppelklicken Sie auf das Installationsprogramm, das Sie heruntergeladen haben.

   Wenn die CD nicht automatisch startet, öffnen Sie Windows Explorer, doppelklicken Sie auf das CD-ROM-Symbol und doppelklicken Sie anschließend auf die Installationsdatei, um die Installation zu starten.

2. Befolgen Sie die 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.

   Sie müssen Ihren Computer möglicherweise neu starten, bevor Ihr Abonnement validiert werden kann und die neuesten Updates aus dem Internet heruntergeladen werden können. Wenn Sie die Installation mithilfe der CD durchführen, entnehmen Sie die Installations-CD, bevor Sie Ihren Computer neu starten.

1.3 Installation und Aktualisierung der Anwendungen

Anweisungen zum Aktivieren Ihres neuen Abonnements.

Befolgen Sie diese Anweisungen, um Ihr neues Abonnement zu aktivieren oder um mit dem Launch Pad eine neue Anwendung zu installieren:

Hinweis: Sie finden das Launch Pad-Symbol in der Windows-Taskleiste.

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Meine Abonnements anzeigen**.
3. Gehen Sie unter **Meine Abonnements** auf die Seite **Abonnementstatus** und klicken Sie auf **Abonnement aktivieren**.
   Das Fenster **Abonnement aktivieren** wird geöffnet.
4. Geben Sie Ihren Abonnementschlüssel für die Anwendung ein und klicken Sie auf **OK**.
5. Nachdem Ihr Abonnement validiert und aktiviert wurde, klicken Sie auf **Schließen**.
6. Gehen Sie unter **Meine Abonnements** zur Seite **Installationsstatus**. Sollte die Installation nicht automatisch starten, befolgen Sie diese Anweisungen:

a) Klicken Sie auf **Installieren**.
   Das Installationsfenster wird geöffnet.
b) Klicken Sie auf **Weiter**.
   Die Anwendung wird heruntergeladen und die Installation beginnt.
c) Klicken Sie auf **Schließen**, wenn die Installation abgeschlossen ist.

Das neue Abonnement wurde aktiviert.

1.4 Hilfe und Support

Sie können auf die Online-Produkthilfe zugreifen, indem Sie auf das Hilfesymbol klicken oder auf einem beliebigen Bildschirm des Produkts auf `F1` drücken.

Einstieg

Themen:

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

Die Einstellungen umfassen:

- 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.
- Abonnements für die installierten Programme.

2.1 Verwendung des Wartungscenters

Das Wartungcenter zeigt Ihnen wichtige Meldungen an

Wenn im Wartungscenter noch Aktionen ausstehen, werden Sie regelmäßig daran erinnert.

2.1.1 Öffnen des Wartungscenters

Öffnen Sie das Wartungscenter, um alle wichtigen Meldungen anzuzeigen.

Öffnen des Wartungscenters:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Wartungscenter öffnen**.
   Im Wartungscenter wird eine Liste aller durchzuführenden Aktionen angezeigt.
3. Klicken Sie auf die entsprechenden Elemente in der Liste, um weitere Informationen anzuzeigen.
4. Wenn Sie momentan keine der ausstehenden Aktionen durchführen möchten, klicken Sie auf **Verschieben**, um diese später durchzuführen.

   Tipp: Wenn Sie das Wartungscenter schließen und alle Aktionen abschließen möchten, klicken Sie auf **Alles verschieben**.

2.1.2 Installation einer Produktaktualisierung

Wenn eine kostenlose Aktualisierung für ein Produkt verfügbar ist, das Sie installiert haben, müssen Sie diese installieren, um die neue Version zu verwenden.

Aktualisierung des Produkts:

1. Wartungscenter öffnen.
   Im Wartungscenter wird das Element **Produkt-Upgrade verfügbar** angezeigt. Wenn mehrere Element im Wartungscenter angezeigt werden, klicken Sie auf das Element, um dieses zu öffnen.
2. Klicken Sie auf **Aktualisieren**.

   Hinweis: Sie haben die neuen Lizenzbedingungen zur Aktualisierung des Produkts nicht akzeptiert, falls diese sich geändert haben.

Möglicherweise müssen Sie Ihren Computer neu starten, sobald die Aktualisierung abgeschlossen ist.

2.1.3 Installation eines neuen Produkts

Wenn Sie ein neues Produkt zu Ihrem Abonnement hinzugefügt haben, können Sie es installieren und anschließend verwenden.

Sie können neue Produkte während der Laufzeit Ihres Abonnements hinzufügen.

Installation eines neuen Produkts:

1. Wartungscenter öffnen.
   Im Wartungscenter wird das Element **Neues Produkt installieren** angezeigt. Wenn mehrere Element im Wartungscenter angezeigt werden, klicken Sie auf das Element, um dieses zu öffnen.
2. Klicken Sie auf **Installieren**.

   Hinweis: Wenn Sie das Produkt nicht installieren möchten, klicken Sie auf das Papierkorbsymbol oben rechts, um die Erinnerung zu schließen und aus dem Wartungscenter zu entfernen.

3. Befolgen Sie die Anweisungen des Installationsassistenten, um das Produkt zu installieren.

Möglicherweise müssen Sie Ihren Computer neu starten, sobald die Installation abgeschlossen ist.

2.1.4 Abgelaufenes Produkt ersetzen

Wenn Ihr Abonnement abgelaufen ist und Ihr derzeitig installiertes Produkt nicht mehr verfügbar ist, können Sie Ihr Abonnement nicht mehr verlängern. Stattdessen können Sie gratis auf das neue Produkt aufrüsten.

Aktualisierung des Produkts:

1. Wartungscenter öffnen.
   Im Wartungscenter wird das Element **Produkt aufrüsten** angezeigt. Wenn mehrere Element im Wartungscenter angezeigt werden, klicken Sie auf das Element, um dieses zu öffnen.
2. Klicken Sie auf **Aktualisieren**.

Möglicherweise müssen Sie Ihren Computer neu starten, sobald die Aktualisierung abgeschlossen ist.

2.2 Verwendung von Automatische Updates

Automatische Updates schützen Ihren Computer vor den neuesten Bedrohungen.

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.

2.2.1 Den Update-Status überprüfen

Datum und Uhrzeit der letzten Aktualisierung anzeigen.

Normalerweise müssen Sie nicht selbst nach Updates suchen, da das Produkt die neuesten Updates automatisch erhält, sobald Sie mit dem Internet verbunden sind und automatische Updates aktiviert sind.

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Updates**.
4. Klicken Sie auf **Jetzt prüfen**.
   Das Produkt lädt die neuesten vorhandenen Updates herunter.

   Hinweis: Ihre Internetverbindung muss aktiv sein, wenn Sie überprüfen möchten, ob es neue Updates gibt.

2.2.2 Ändern der Einstellungen für die Internetverbindung

Normalerweise müssen die Standardeinstellungen nicht geändert werden, aber Sie können konfigurieren, wie der Computer mit dem Internet verbunden ist, damit Sie automatisch Updates erhalten.

Hinweis: Die Funktion **Mobile Daten**ist nur in Microsoft Windows 7 und neueren Windows-Versionen verfügbar.

Für mobile Datenverbindungen werden Sicherheitsupdates standardmäßig 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: Die Einstellung **Mobile Daten**gilt nur für mobile Breitbandverbindungen. Wenn der Computer mit einem Festnetz oder Drahtlosnetzwerk verbunden ist, wird das Produkt automatisch aktualisiert.

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

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.

Ein Pop-up-Menü wird angezeigt.

2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Verbindung**.
4. Wählen Sie in der Liste **HTTP-Proxy**, ob Ihr Computer einen *Proxyserver* nutzt, um eine Verbindung mit dem Internet herzustellen.
   - Wählen Sie **Nicht verwenden**, wenn Ihr Computer direkt mit dem Internet verbunden ist.
   - Wählen Sie **Browsereinstellungen verwenden**, um die gleichen *HTTP-Proxy*-Einstellungen zu verwenden, die in Ihrem Browser konfiguriert sind.
   - Wählen Sie **Benutzerdefinierte Einstellungen** und klicken Sie auf **Konfigurieren**, um Ihre *HTTP-Proxy*-Einstellungen manuell zu konfigurieren.
5. Wählen Sie die bevorzugte Update-Option für Mobilverbindungen:
   - **Nie**- Es werden keine Updates heruntergeladen, wenn Sie mobiles Breitband verwenden.
   - **Nur im Netzwerk meines Anbieters**- Updates werden immer im Netzwerk Ihres Privatanbieters heruntergeladen. Wenn Sie ein Netzwerk eines anderen Anbieters verwenden, werden die Updates unterbrochen. Wir empfehlen Ihnen, diese Option zu wählen, um Ihr Sicherheitsprodukt zu den erwarteten Kosten auf dem neuesten Stand zu halten.
   - **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.

     Hinweis: 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 und neueren Windows-Versionen verfügbar.

2.3 Wie erkennt man, was das Produkt geleistet hat?

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

Das Produkt zeigt eine Benachrichtigung an, wenn es eine Aktion durchführt, beispielsweise um Dateien zu schützen, die auf Ihrem Computer gespeichert sind. Möglicherweise werden manche Benachrichtigungen auch an Ihren Service Provider gesendet, beispielsweise um Sie über neue verfügbare Services zu informieren.

So zeigen Sie die Produktzeitleiste an:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Klicken Sie auf **Produktzeitleiste öffnen**.
   Die Benachrichtigungsliste der Produktzeitleiste wird geöffnet.
3. Klicken Sie auf **Alle entfernen**, wenn Sie alle vorherigen Benachrichtigungen aus der Produkt-Zeitleiste entfernen möchten.

   Hinweis: Diese Aktion kann nicht rückgängig gemacht werden.

2.4 Spielmodus

Aktivieren Sie den *Spielmodus*, wenn Sie während des Spielens Systemressourcen freigeben wollen.

Computerspiele benötigen häufig viele Systemressourcen, um reibungslos zu funktionieren. Andere Anwendungen, die im Hintergrund ausgeführt werden, können die Leistung von Spielen verschlechtern, da Sie Systemressourcen und das Netzwerk belegen.

Der *Spielmodus* verringert den Einfluss des Produkts auf Ihren Computer und reduziert seine Netzwerkverwendung. Dadurch werden mehr Systemressourcen für Computerspiele freigegeben, während die Grundfunktionen des Produktes unbeeinflusst bleiben. So werden z. B. automatische Updates, geplante Scans und andere Vorgänge ausgesetzt, die viele Systemressourcen und Netzwerkverkehr benötigen.

Wenn Sie eine Anwendung im Vollbildmodus verwenden, z. B. eine Präsentation, Slideshow oder ein Video ansehen oder ein Spiel im Vollbildmodus spielen, zeigen wir nur essentielle Benachrichtigungen an, die Ihre unmittelbare Aufmerksamkeit erfordern. Andere Benachrichtigungen werden erst angezeigt, wenn Sie den Vollbildmodus oder *Spielmodus* verlassen.

2.4.1 Spielmodus aktivieren

Aktivieren Sie den *Spielmodus*, um die Leistungs von Spielen auf Ihrem Computer zu verbessern.

Spielmodus aktivieren:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Spielmodus**.
   Die Nutzung der Systemressourcen durch das Produkt ist nun optimiert und Spiele können auf Ihrem Computer reibungslos ausgeführt werden.

Vergessen Sie nicht den *Spielmodus* auszuschalten, wenn Sie das Spiel beenden. Der *Spielmodus* wird automatische deaktiviert, wenn Sie Ihren Computer neu starten oder den Energiesparmodus verlassen.

2.5 Woher weiß ich, ob mein Abonnement gültig ist?

Angaben zu Art und Status Ihres Abonnements finden Sie auf der Seite **Abonnements**.

Der Schutzstatus des Produktes ändert sich, wenn Ihr Abonnement in Kürze abläuft oder bereits abgelaufen ist.

So prüfen Sie die Gültigkeit Ihrer Anmeldung:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **Abonnementschlüssel**, um Informationen zu Ihren Abonnements für installierte Programme zu erhalten.
   - Wählen Sie **Installierte Anwendungen**, um zu sehen, welche Programme zur Installation zur Verfügung stehen.

Falls Ihr Abonnement abgelaufen ist, müssen Sie es erneuern, um weiterhin Updates zu erhalten und das Produkt verwenden zu können.

2.5.1 Abonnement aktivieren

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

Aktivierung eines Abonnements:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.

2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Klicken Sie auf **Neues Abonnement hinzufügen** auf der Abonnementschlüssel-Seite.
4. Geben Sie nun in das sich öffnende Dialogfeld Ihren Abonnementschlüssel oder Kampagnencode ein, und klicken Sie auf **Weiter**.

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 Gültigkeitsdatum des neuen Abonnements auf der Seite **Abonnementschlüssel** angezeigt.

2.5.2 Verlängerung Ihres Abonnements

Falls Ihr Produktabonnement bald abläuft, müssen Sie es verlängern, um das Produkt weiterhin zu verwenden.

Verlängerung Ihres Abonnements:

1. Wartungscenter öffnen.
   Im Wartungscenter wird das Element **Abonnement verlängern** angezeigt. Wenn mehrere Element im Wartungscenter angezeigt werden, klicken Sie auf das Element, um dieses zu öffnen.
2. Sie benötigen einen neuen Abonnementschlüssel, um Ihr Abonnement zu verlängern.
   - Wenn Sie bereits ein Abonnement haben, das Sie für diesen Computer verwenden können, klicken Sie auf **Aktivieren**, um das neue Abonnement zu verwenden.
   - Wenn Sie bereits einen neuen Abonnementschlüssel gekauft haben, klicken Sie auf **Schlüssel eingeben**.

     Geben Sie in das Dialogfeld, das geöffnet wird, Ihren neuen Abonnementschlüssel ein und klicken Sie auf **OK**.
   - Klicken Sie andernfalls auf **Jetzt verlängern**.

     Sie können Ihre Abonnement in unserem Online Store verlängern. Wenn Sie Ihr Abonnement verlängern, erhalten Sie einen neuen Abonnementschlüssel.

Wenn Sie Ihr Abonnement nicht verlängern möchten, deinstallieren Sie das Produkt mit dem abgelaufenen Abonnement.

2.6 Wo finde ich meine Konto-ID?

Wenn Sie unseren Kundensupport kontaktieren möchten, benötigen Sie unter Umständen Ihre Identitätscodes.

So können Sie Ihre Identitätscodes anzeigen:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie die Option **Kennungen**.

Security Cloud

Themen:

Dieses Dokument beschreibt die *Security Cloud* (zuvor bekannt als Echtzeit-Schutznetzwerk), ein Online-Service der F-Secure Corporation, der saubere Anwendungen und Websites identifiziert und Sie gleichzeitig vor Malware und gefährlichen Websites schützt.

3.1 Worum handelt es sich bei der *Security Cloud*?

Die *Security Cloud* ist ein Online-Service, der bei aktuellen Internet-Gefahren schnell reagiert.

Als Teilnehmer erlauben Sie der *Security Cloud*, Sicherheitsdaten zu sammeln, die es uns ermöglichen, Ihren Schutz vor neuen und aufkommenden Bedrohungen zu erhöhen. Die *Security Cloud* sammelt Informationen zu bestimmten unbekannten, bösartigen oder verdächtigen Anwendungen und nicht klassifizierten Websites. Diese Informationen sind anonym und werden zur kombinierten Datenanalyse an die F-Secure Corporation gesendet. Wir verwenden die analysierten Informationen, um Sie besser vor den aktuellsten Bedrohungen und bösartigen Dateien zu schützen.

So funktioniert die *Security Cloud*

Die *Security Cloud* sammelt Sicherheitsdaten zu unbekannten Anwendungen und Websites und zu schädlichen Anwendungen und Schwachstellen bei Websites. Wir sammeln diese Informationen, um Ihnen die von Ihnen abonnierten Sicherheitsdienste bereitstellen und um die Sicherheit unserer weiteren Dienste verbessern zu können. Wir müssen Sicherheitsdaten zu unbekannten Dateien, verdächtigem Geräteverhalten oder besuchten URLs sammeln. Diese Daten sind für unsere Arbeit unerlässlich.

Die *Security Cloud* verfolgt weder Ihre Webaktivitäten noch sammelt sie Informationen auf Websites, die bereits analysiert wurden. Sie sammelt auch keine Informationen zu sauberen Anwendungen, die auf Ihrem Computer installiert sind. Sicherheitsdaten werden nicht für personalisierte Werbung verwendet.

3.2 Vorteile der *Security Cloud*

Mit der *Security Cloud* haben Sie einen schnelleren und genaueren Schutz vor aktuellen Bedrohungen. Zudem werden Sie bei verdächtigen, aber nicht schädlichen Anwendungen nicht unnötig alarmiert.

Als Teilnehmer an der *Security Cloud* können Sie uns dabei helfen, neue und unentdeckte Malware zu finden und mögliche falsch positive Bewertungen zu entfernen.

Alle Teilnehmer an einer *Security Cloud* helfen sich gegenseitig. Wenn die *Security Cloud*eine verdächtige Anwendung findet, profitieren Sie von den Analyseergebnissen, wenn das gleiche Programm bereits von jemand anderem gefunden wurde. Die *Security Cloud* verbessert die Leistung insgesamt, da das installierte Sicherheitsprodukt keine Anwendungen scannen muss, die bereits von der *Security Cloud* analysiert und als sauber befunden wurden. Gleichermaßen werden Informationen zu schädlichen Websites und unangeforderte Bulk-Nachrichten in der *Security Cloud* geteilt. Somit können wir Sie zuverlässiger vor Website-Exploits und Spam-Nachrichten schützen.

Je mehr Personen an der *Security Cloud* teilnehmen, desto besser werden die einzelnen Teilnehmer geschützt.

3.3 Welche Daten steuern Sie bei?

Als Teilnehmer gestatten Sie der *Security Cloud*, Sicherheitsdaten zu den Anwendungen zu sammeln, die Sie installiert haben, und zu den Websites, die Sie besuchen. Somit kann die *Security Cloud*Sie besser vor den neuesten bösartigen Anwendungen und verdächtigen Websites schützen.

Analyse der Dateibewertung

Security Cloud sammelt nur Sicherheitsdaten von unbekannten Anwendungen und Dateien, die entweder verdächtig sind oder als Malware gelten.

Es werden ausschließlich Informationen zu Anwendungsdateien (ausführbare Dateien) gesammelt, nicht zu anderen Dateitypen.

Abhängig vom Produkt können die gesammelten Sicherheitsdaten Folgendes beinhalten:

- den Dateipfad der Anwendung (ohne personenbezogene Informationen),
- 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 (ohne personenbezogene Informationen),
- Ergebnisse von F-Secure DeepGuard und Antivirusanalyse gescannter Dateien und
- sonstige ähnliche Informationen.

Die Website-Bewertung analysieren

Die *Security Cloud* verfolgt Ihre Internetaktivität nicht nach. Es sorgt dafür, dass von Ihnen besuchte Websites sicher sind, wenn Sie im Internet surfen. Sobald Sie eine Website besuchen, wird deren Sicherheit von der *Security Cloud* untersucht und Sie werden benachrichtigt, falls die Website als verdächtig oder schädlich eingestuft wird.

Damit wir unseren Service verbessern und eine Einstufungen immer korrekt vornehmen können, sammelt die *Security Cloud* gegebenenfalls Informationen über besuchte Websites. Die Informationen werden gesammelt, falls die von Ihnen besuchte Website bösartige oder verdächtige Inhalte aufweist oder einen bekannten Exploit, bzw. falls die Inhalte der Website noch nicht bewertet oder kategorisiert wurden. Die gesammelten Informationen umfassen die URL und die Metadaten, die mit dem Besuch und der Website verbunden sind.

Die *Security Cloud* führt strenge Kontrollen durch, damit sichergestellt wird, dass keine persönlichen Daten gesendet werden. Die Anzahl der gesendeten URLs ist begrenzt. Alle eingereichten Daten werden nach personenbezogenen Informationen gefiltert, bevor sie gesendet werden, und alle Felder, die Informationen enthalten könnten, die mit Ihnen in Verbindung gebracht werden könnten, werden entfernt. Die *Security Cloud* bewertet und analysiert keine Webseiten in privaten Netzwerken und es sammelt keine Informationen zu privaten Netzwerkadressen oder Aliasen.

Die Systeminformationen analysieren

Die *Security Cloud* sammelt den Namen und die Version Ihres Betriebssystems, Informationen zur Internetverbindung und Verwendungsstatistiken zur *Security Cloud* (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.

3.4 So schützen wir Ihre Daten

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

Die gesammelten Sicherheitsdaten werden nicht einzeln verarbeitet. Sie werden mit Informationen anderer Teilnehmer an der *Security Cloud* kombiniert. Alle Daten werden statistisch und anonym analysiert. Das bedeutet, dass keine Daten mit Ihnen in Verbindung gebracht werden.

Jegliche Informationen, die Sie persönlich identifizieren könnten, sind nicht in den gesammelten Daten enthalten. Die *Security Cloud* 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 Sicherheitsdaten während deren Übertragung, Speicherung und Verarbeitung zu schützen. Die Sicherheitsdaten 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 Sicherheitsdaten zugreifen.

Sicherheitsdaten werden gesammelt

Unsere Kernregel ist, dass Daten, die Sie identifizieren oder Sie persönlich mit den auf Ihrem Gerät gesammelten Sicherheitsdaten in Verbindung bringen, zum Schutz Ihrer Privatsphäre entweder gelöscht oder dauerhaft verschlüsselt werden. Möglicherweise stellen wir derartige Sicherheitsdaten unseren Geschäftspartnern, Computer Emergency Response Teams (CERTs) und Dritten bereit. Dabei stellen wir jedoch die Anonymität der Daten sicher.

Wir behandeln die Sicherheitsdaten oder die entstandenen Metadaten nur in besonderen Fällen in persönlich identifizierbarer Form, etwa wenn wir unsere Dienste sonst nicht bereitstellen könnten. Dies ist beispielsweise dann der Fall, wenn wir mit Ihrer ausdrücklichen Zustimmung eine Support-Anfrage für Sie bearbeiten. Ein weiteres Beispiel ist, wenn die Malware auf infizierten Geräten auf unserem unternehmenseigenen Produktmanagement-Portal angezeigt wird. Wenn dies erforderlich ist, können wir derartige identifizierbare Daten unseren Geschäftspartnern, Subunternehmen und Vertriebspartnern übermitteln, wenn diese die Daten unbedingt benötigen. Detaillierte Daten zu Ihrem Browsing-Verhalten werden immer anonym behandelt und können nicht in identifizierbarer Form weitergegeben werden.

3.5 Inhalte werden mit der Security Cloud gescannt.

Die Security Cloud scannt Anwendungsdateien in der Cloud, um zu überprüfen, ob diese sicher sind.

Mit unseren Desktop-Produkten können Sie einzelne verdächtige Anwendungen an die *Security Cloud* übermitteln, wenn das Produkt Sie dazu auffordert. Die *Security Cloud* lädt niemals Ihre persönlichen Dokumente hoch.

3.6 Werden Sie Teilnehmer an der *Security Cloud*.

Sie helfen uns bei der Verbesserung der *Security Cloud*, indem Sie uns Sicherheitsdaten zu schädlichen Programmen und Websites übermitteln.

Sie können wählen, ob Sie bei der *Security Cloud* teilnehmen möchten und können Ihre Teilnahme jederzeit in den Produkteinstellungen aussetzen. Beachten sie, dass auch wenn Sie nicht bei der Security Cloud teilnehmen möchten, bestimmte Produktfunktionen dennoch mit der Security Cloud kommunizieren müssen, so dass der von Ihnen abonnierte Sicherheitsdienst einwandfrei funktioniert. Telemetrische Daten, beispielsweise über die Häufigkeit des Zugriffs auf die Security Cloud, Zeitstempel und Versionsnummern der Antiviren-Datenbank werden der Security Cloud übermittelt, auch wenn Sie den Dienst nicht nutzen.

Ablehnen

Falls Sie diese Daten nicht bereitstellen möchten, werden die Informationen zu installierten Anwendungen oder besuchten Websites nicht von der *Security Cloud* 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 zu *Security Cloud* zu unterbinden, da hierdurch der vom Produkt hergestellte Schutz grundlegend gewährt wird.

3.7 Fragen zu *Security Cloud*

Kontaktdetails für Fragen zur *Security Cloud*

Für alle weiteren Fragen zur *Security Cloud* 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.

Computer wird nach schädlichen Dateien durchsucht

Themen:

Der Virenschutz schützt den Computer vor Programmen, die möglicherweise persönliche Informationen stehlen, den Computer beschädigen oder ihn für illegale Zwecke verwenden.

Das Produkt bearbeitet standardmäßig alle gefundenen schädlichen Dateien sofort, so dass sie keinen Schaden anrichten können.

Das Produkt scannt standardmäßig alle Ihre lokalen Festplatten, Wechseldatenträger (wie z. B. tragbare Laufwerke oder DVDs) und sämtliche heruntergeladenen Inhalte automatisch.

Zudem können Sie festlegen, dass das Produkt auch Ihre E-Mails automatisch scannt.

Das Produkt überprüft Ihren Computer zudem auf sämtliche Änderungen, die ein Hinweis sein könnten, dass sich schädliche Dateien auf Ihrem Computer befinden. Wenn das Produkt gefährliche Systemänderungen, wie beispielsweise Änderungen in den Systemeinstellungen oder Versuche, wichtige Systemprozesse zu ändern, erkennt, stoppt die DeepGuard-Komponente die Anwendung, da diese schädlich sein kann.

4.1 Computer wird vor schädlichen Anwendungen geschützt

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

Das Produkt schützt Ihren Computer vor Anwendungen, die möglicherweise Ihre persönlichen Daten stehlen, Ihre Dateien beschädigen oder Ihren Computer für illegale Zwecke benutzen.

Das Viren-Scanning durchsucht Ihren Computer automatisch nach schädlichen Dateien.

DeepGuard überwacht Anwendungen, um potenziell schädliche Änderungen an Ihrem System zu erkennen und zu verhindern. Zudem hält es Eindringlinge und schädliche Anwendungen davon ab, über das Internet Zugang zu Ihrem Computer zu erhalten.

Das Produkt sorgt dafür, dass Ihr Schutz immer auf dem neuesten Stand ist. Es lädt Datenbanken herunter, die Informationen über das automatische Finden und Entfernen von schädlichen Inhalten enthalten.

Hinweis: Das Produkt lädt die aktuellsten Datenbanken herunter, nachdem die Installation abgeschlossen ist. Währenddessen kann das Viren-Scanning nicht alle Gefahren erkennen. Andere Produktfunktionen, wie etwa DeepGuard, schützen Ihren Computer jedoch während dieser Zeit.

4.1.1 Schutzstatus-Symbole

Die Symbole auf der **Status**-Seite zeigen den Gesamtstatus des Produkts und seine Funktionen an.

Die folgenden Symbole zeigen Ihnen den Status des Programms und seiner Sicherheitsfunktionen an.

Status-Symbol	Statusbezeichnung	Beschreibung
	OK	Ihr Computer ist geschützt. Die Funktionen sind aktiviert und arbeiten ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über einen besonderen Status. Alle Funktionen arbeiten korrekt, aber das Produkt lädt z. B. gerade Updates herunter.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Sie sollten das Produkt überprüfen, z. B. weil es seit langem keine Updates mehr erhalten hat.
	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.

4.1.2 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 **Statistiken**.

Die Seite **Statistiken** zeigt folgende Informationen:

- **Viren- und Spyware-Scan** zeigt an, wie viele Dateien das Produkt seit der Installation gescannt und bereinigt hat.
- Unter **Anwendungen** sehen Sie, wie viele Programme DeepGuard seit der Installation zugelassen oder blockiert hat.

4.1.3 Handhabung der Produkt-Updates

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

Anzeigen der Datenbankversionen

Die aktuellsten Update-Zeiten und Versionsnummern finden Sie auf der Seite **Datenbankversionen**.

So öffnen Sie die Seite **Datenbankversionen**:

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

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

2. Wählen Sie **Datenbank-Updates**.

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 und neueren Windows-Versionen 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 mit der rechten Maustaste auf das Produktsymbol auf der Taskleiste.
   Ein Pop-up-Menü wird angezeigt.
2. Wählen Sie **Allgemeine Einstellungen öffnen**.
3. Wählen Sie **Verbindung**.
4. Wählen Sie die bevorzugte Update-Option für Mobilverbindungen:
   - **Nie**- Es werden keine Updates heruntergeladen, wenn Sie mobiles Breitband verwenden.
   - **Nur im Netzwerk meines Anbieters**- Updates werden immer im Netzwerk Ihres Privatanbieters heruntergeladen. Wenn Sie ein Netzwerk eines anderen Anbieters verwenden, werden die Updates unterbrochen. Wir empfehlen Ihnen, diese Option zu wählen, um Ihr Sicherheitsprodukt zu den erwarteten Kosten auf dem neuesten Stand zu halten.

- **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.

  Hinweis: 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 und neueren Windows-Versionen verfügbar.

4.1.4 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.

Potenziell unerwünschte Anwendungen

Potenziell unerwünschte Anwendungen können die Sicherheit Ihres Computers gefährden oder diesen langsamer machen.

Potenziell unerwünschte Anwendungen können schädlich für Ihren Computer oder für Anwendungen, die Sie nutzen möchten, sein. Möglicherweise haben Sie die potenziell unerwünschte Anwendung selbst auf Ihren Computer heruntergeladen oder sie wurde zusammen mit anderer Software installiert.

Da einige potenziell unerwünschte Anwendungen möglicherweise im Hintergrund laufen und Ihren Computer verlangsamen oder Ihr Browser-Verhalten aufzeichnen und Ihnen unerwünschte Werbung anzeigen, sollten Sie sie blockieren, es sei denn, es handelt sich um eine Anwendung, die Sie nutzen möchten.

4.2 Wie scanne ich meinen Computer?

Wenn der Virenschutz aktiviert ist, durchsucht er Ihren Computer automatisch nach schädlichen Dateien.

Wir empfehlen Ihnen, den Virenschutz immer aktiviert zu lassen. Zudem können Sie Dateien manuell scannen und geplante Scans festlegen, wenn Sie sichergehen möchten, dass sich keine schädlichen Dateien auf Ihrem Computer befinden, oder wenn Sie vom Echtzeit-Scan ausgeschlossene Dateien überprüfen möchten. Legen Sie einen geplanten Scan fest, wenn Sie Ihren Computer täglich oder wöchentlich überprüfen möchten.

4.2.1 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 Ihr Computer versucht auf eine Datei zuzugreifen, scannt der Echtzeit-Scan die Datei auf Malware bevor der Zugriff auf die Datei erlaubt wird.

Wenn der Echtzeit-Scan gefährliche Inhalte findet, wird die Datei in Quarantäne gesetzt, bevor Schaden entstehen 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 Statusseite auf **Einstellungen**.

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

2. So wird der **Virenschutz** ein- oder ausgeschaltet.
3. Klicken Sie auf **OK**.

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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Virenschutz**.
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

Der Virenschutz 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.
Anwendung unter Quarantäne stellen	Die Anwendung wird in die Quarantänezone verschoben, in der Sie keinen Schaden auf Ihrem Computer anrichten kann.
Anwendung entfernen	Die Anwendung dauerhaft von Ihrem Computer entfernen
Anwendung vorerst blockieren	Der Zugriff auf die Anwendung wird blockiert, verbleibt jedoch auf Ihrem Computer.
Anwendung nicht blockieren	Die Ausführung der Anwendung wird zugelassen und die Anwendung wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

Potenziell unerwünschte Anwendungen bearbeiten

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

Wählen Sie eine der folgenden Aktionen, wenn eine potenziell unerwünschte Anwendung identifiziert wird:

Durchzuführende Aktion	Was mit der Anwendung passiert
Anwendung unter Quarantäne stellen	Die Anwendung wird in die Quarantänezone verschoben, in der Sie keinen Schaden auf Ihrem Computer anrichten kann.
Anwendung entfernen	Die Anwendung dauerhaft von Ihrem Computer entfernen
Anwendung vorerst blockieren	Der Zugriff auf die Anwendung wird blockiert, verbleibt jedoch auf Ihrem Computer.
Anwendung nicht blockieren	Die Ausführung der Anwendung wird zugelassen und die Anwendung wird bei allen weiteren Scanvorgängen nicht mehr berücksichtigt.

Schädliche E-Mail-Anhänge automatisch entfernen

Der Echtzeit-Scan kann schädliche E-Mail-Anhänge automatisch, d. h. ohne Ausgabe von Fragen an den Benutzer, entfernen.

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

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

2. Wählen Sie **Virenschutz**.
3. Wählen Sie **Schädliche E-Mail-Anhänge entfernen**.

4.2.2 Manuelles Scannen von Dateien

Sie können Ihren gesamten Computer scannen, um sicherzugehen, dass sich keinerlei schädliche Dateien oder unerwünschte Anwendungen darauf befinden.

Der Scan des ganzen Computers scannt alle internen und externen Festplatten auf Viren, Spyware und potenziell unerwünschte Anwendungen. Zudem wird auch nach Elementen gesucht, die möglicherweise von einem Rootkit versteckt werden. Der Scan des ganzen Computers kann unter Umständen lange dauern. Sie können auch nur die einzelnen Teile Ihres Systems scannen, die installierte Anwendungen enthalten, um unerwünschte Anwendungen und schädliche Elemente auf Ihrem Computer noch effizienter zu finden und diese zu entfernen.

Scannen von Dateien und Ordnern

Wenn Sie glauben, dass sich bestimmte Dateien auf Ihrem Computer befinden, haben Sie die Möglichkeit, lediglich diese Dateien oder Ordner zu scannen. Diese Scanvorgänge sind deutlich schneller abgeschlossen als ein Scan Ihres gesamten Computers. Wenn Sie beispielsweise eine externe Festplatte oder eine USB-Speichermedium mit Ihrem Computer verbinden, können Sie dieses scannen, um sicherzugehen, dass sich keinerlei schädliche Dateien darauf befinden.

Durchführen eines manuellen Scans

Sie können Ihren gesamten Computer scannen oder einen effizienteren Virenscan durchführen, der nur die Teile Ihres Systems scannt, die mit größerer Wahrscheinlichkeit schädliche Dateien und unerwünschte Anwendungen enthalten.

So scannen Sie Ihren Computer:

1. Wählen Sie die Art des Scans aus, den Sie starten möchten.
   - Wenn Sie Ihren Computer schnell scann möchten, klicken Sie auf der **Status**-Seite auf **Virenscan**.
   - Wenn Sie Ihren Computer komplett scannen möchten, wählen Sie **Tools** > **Erweiterter Scan** > **Vollständiger Computer-Scan**.

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

   Der manuelle Scan wird gestartet.

2. Wenn der manuelle Scan schädliche Elemente findet, wird die Liste der entdeckten schädlichen Elemente angezeigt.
3. Klicken Sie auf das entdeckte Element, um zu entscheiden, wie Sie mit dem schädlichen Inhalt umgehen möchten.

Option	Beschreibung
Bereinigen	Dateien automatisch bereinigen. Dateien, die nicht bereinigt werden können, werden unter Quarantäne gestellt.
Quarantäne	Speichern Sie die Dateien an einem sicheren Ort, von dem aus sie nicht andere Dateien infizieren oder Ihren Computer schädigen können.
Löschen	Löschen Sie die Dateien dauerhaft von Ihrem Computer.
Überspringen	Unternehmen Sie vorerst nichts und lassen Sie die Dateien auf Ihrem Computer.
Ausschließen	Die Ausführung der Anwendung zugelassen und die sie von allen künftigen Scanvorgängen ausschließen

Hinweis: Einige Optionen sind nicht für alle schädlichen Dateitypen verfügbar.

4. Klicken Sie auf **Alle bearbeiten**, um mit dem Bereinigungsprozess zu beginnen.
5. Der manuelle Scan zeigt die Endergebnisse und die Anzahl der schädlichen Elemente an, die bereinigt wurden.

Hinweis: Beim manuellen Scan müssen Sie unter Umständen Ihren Computer neu starten, um den Bereinigungsvorgang abzuschließen. Wenn für den Bereinigungsprozess ein Neustart Ihres Computers erforderlich ist, klicken Sie auf**Neu starten**, um das Bereinigen der schädlichen Elemente abzuschließen und Ihren Computer neu zu starten.

In manchen Fällen kann es vorkommen, dass der manuelle Scan ein entdecktes schädliches Element nicht entfernen kann. Nutzen Sie das *Cleanup-Tool*, um die schädlichen Dateien zu entfernen, die vom manuellen Scan nicht entfernt werden konnten.

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 potenziell unerwünschte Anwendungen	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 schädliche Elemente auf Ihrem Computer schnell entdecken können.
Vollständiger Scan des Computers	Ihr gesamter Computer (interne und externe Festplatten) auf Viren, Spyware und potenziell unerwünschte Anwendungen	Nutzen Sie diesen Scan, wenn Sie absolut sicher sein wollen, dass sich keine schädlichen Dateien oder unerwünschten Anwendungen auf Ihrem Computer befinden. Diese Art des Scannens dauert am längsten. Sie kombiniert den schnellen Viren- und Spyware-Scan mit dem Festplattenscan. Außerdem sucht sie nach Elementen, die unter Umständen durch ein Rootkit verborgen sind.
Auswahl für Scan...	Ein spezieller Ordner oder ein spezielles Laufwerk auf Viren, Spyware und	Nutzen Sie diese Art des Scans, wenn Sie glauben, dass ein bestimmter Teil Ihres Computers schädliche Dateien enthält. Beispielsweise dann, wenn Sie Dateien, die Sie von einer potenziell gefährlichen Quelle wie etwa einem

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
	potenziell unerwünschte Anwendungen	Peer-to-Peer-Filesharing-Netzwerk heruntergeladen haben, scannen möchten. Abhängig von der Größe und Anzahl der Dateien, die Sie scannen möchten, kann der Scanvorgang schnell beendet sein oder länger dauern. Wenn Sie beispielsweise einen Ordner, der nur weniger kleine Dateien enthält, scannen, ist der Scanvorgang schnell abgeschlossen.

Scannen von Dateien und Ordnern

Sie können Dateien und Ordner auf Viren, andere schädliche Dateien und unerwünschte Anwendungen scannen.

Sie können Dateien und Ordner scannen, wenn Sie glauben, dass ein bestimmter Teil Ihres Computers schädliche Dateien enthält. Beispielsweise dann, wenn Sie Dateien, die Sie von einer potenziell gefährlichen Quelle wie etwa einem Peer-to-Peer-Filesharing-Netzwerk heruntergeladen haben, scannen möchten. Abhängig von der Größe und Anzahl der Dateien, die Sie scannen möchten, kann der Scanvorgang schnell beendet sein oder länger dauern. Wenn Sie beispielsweise einen Ordner, der nur weniger kleine Dateien enthält, scannen, ist der Scanvorgang schnell abgeschlossen.

So scannen Sie Dateien und Ordner:

1. Wählen Sie im File Explorer die Dateien und Ordner, die Sie scannen möchten.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Elemente und wählen Sie im Menü **Ausgewählte Dateien/Ordner auf Viren und Spyware scannen**.
3. Platzieren Sie den Mauszeiger auf dem zu scannenden Datenträger, dem Ordner oder der Datei und klicken Sie mit der rechten Maustaste.
4. Der manuelle Scan wird gestartet.

Auswählen von Dateien für den Scanvorgang

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

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

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

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

Nur bekannte Dateitypen scannen
Um nur die Dateitypen zu scannen, die mit einer höheren Wahrscheinlichkeit infiziert sind, beispielsweise ausführbare Dateien. Das Auswählen dieser Option beschleunigt den Scanvorgang. 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, 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 Standardaktion, die bei der Identifizierung von schädlichen Inhalten im Rahmen eines manuellen Scanvorgangs durchzuführen ist:

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

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

2. Wählen Sie **Manuelle Scans**.
3. Wählen Sie unter **Wenn etwas Schädliches 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.
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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Geplante Scans**.
3. Aktivieren Sie **Geplante Scans**.

Der geplante Scan verwendet beim Scannen Ihres Computers die Einstellungen des manuellen Scans. Der Unterschied ist jedoch, dass er Archive jedes Mal scannt und schädliche Dateien automatisch bereinigt.

Hinweis: Geplante Scans werden ausgesetzt wenn der *Spielmodus* an ist. Wenn er ausgeschaltet wird, wird der ausgesetzte Scan automatisch fortgesetzt.

4.2.3 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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Virenschutz**.
3. Wählen Sie **Schädliche E-Mail-Anhänge entfernen**.
4. Klicken Sie auf **OK**.

Wann werden E-Mail-Nachrichten und Anhänge gescannt?

Der Virenschutz kann schädliche Inhalte aus von Ihnen empfangenen E-Mails entfernen.

Der Virenschutz entfernt schädliche E-Mails, die von E-Mail-Programmen wie Microsoft Outlook und Outlook Express, Microsoft Mail oder Mozilla Thunderbird empfangen werden. Er durchsucht verschlüsselte E-Mail-Nachrichten und Anhänge, sobald Ihr E-Mail-Programm diese vom Mail Server unter Verwendung des POP3-Protokolls empfängt.

Der Virenschutz 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-Anhängen 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.

4.2.4 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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Virenschutz**.
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

4.2.5 Bereinigungs-Tool verwenden

Mithilfe des Bereinigungs-Tools können Sie schädliche Dateien entfernen, die der manuelle Scan nicht entfernen kann.

Hinweis: Diese Funktion steht nicht in allen Versionen des Produkts zur Verfügung.

Sie benötigen eine Internetverbindung, um das Cleanup-Tool verwenden zu können.

So führen Sie das Bereinigungs-Tool aus:

1. Klicken Sie auf der Seite **Tools** auf **Bereinigungs-Tool**.
2. Das Produkt sucht die aktuellste Version des Cleanup-Tools und lädt diese vom Internet herunter. Das Cleanup-Tool startet automatisch, nachdem die aktuellste Version installiert wurde.
3. Klicken Sie im Fenster des Bereinigungs-Tools auf **Scan starten**, um Ihren Computer zu scannen.
   - Falls die Lizenzvereinbarung angezeigt wird, lesen Sie sie und klicken Sie auf **Akzeptieren**, um fortzufahren.

   Das Bereinigungs-Tool scannt Ihren Computer und entfernt alle entdeckten schädlichen Dateien. Falls erforderlich startet das Bereinigungs-Tool Ihren Computer neu, um schädliche Dateien zu entfernen.

4.3 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.

4.3.1 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 Statusseite 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 **Virenschutz**, um den Dateityp vom Echtzeit-Scanning auszuschließen.
   - Wählen Sie **Manuelles Scanning**, um den Dateityp vom manuellen Scanning auszuschließen.
3. Klicken Sie auf den Link **Dateien vom Scan ausschließen**.
   Die Seite **Vom Scan ausschließen** wird geöffnet.
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 die neuen Einstellungen anzuwenden und um das Dialogfeld **Vom Scan ausschließen** zu schließen.

Die angegebenen Dateitypen werden von allen weiteren Scanvorgängen ausgeschlossen.

4.3.2 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 Statusseite 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 **Virenschutz**, um den Speicherort vom Echtzeit-Scanning auszuschließen.
   - Wählen Sie **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.

4.3.3 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 das Produkt eine potenziell unerwünschte Anwendung entdeckt, von der Sie wissen, dass sie sicher ist, oder wenn Spyware erkannt wird, die Sie benötigen, um eine andere Anwendung zu nutzen, können Sie diese vom Scan ausschließen, sodass Ihnen das Produkt keine Warnungen mehr anzeigt.

Hinweis: Wenn sich eine Anwendung wie ein Virus oder eine andere schädliche Anwendung verhält, kann sie nicht ausgeschlossen werden.

So zeigen Sie vom Scanvorgang ausgeschlossene Anwendungen an:

1. Klicken Sie auf der Statusseite 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 **Virenschutz**, um die vom Echtzeit-Scanning ausgeschlossenen Anwendungen anzuzeigen.
- Wählen Sie **Manuelles Scanning**, um die vom manuellen Scanning ausgeschlossenen Anwendungen anzuzeigen.

3. Klicken Sie auf **Dateien vom Scan ausschließen**.
   Die Seite **Vom Scan ausschließen** wird geöffnet.
4. Wählen Sie die Registerkarte **Anwendungen**.
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**.

Neue Anwendungen werden erst zur Ausschussliste hinzugefügt, wenn Sie sie während dem Scanvorgang ausgeschlossen haben. Sie können nicht direkt zur Ausschlussliste hinzugefügt werden.

4.4 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 sowohl schädliche Elemente als auch potenziell unerwünschte Anwendungen unter Quarantäne stellen, damit sie keinen Schaden anrichten können. 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.

- In der Regel können Sie Viren und andere schädliche Elemente, die sich in Quarantäne befinden, löschen.
- In der Regel können Sie *Spyware*, die sich in Quarantäne befindet, löschen.

  Manchmal kann es vorkommen, das die unter Quarantäne gestellte *Spyware* Teil einer anderen Anwendung ist. Wenn die *Spyware* entfernt wird, kann es sein, dass diese Anwendung nicht mehr ausgeführt werden kann. Wenn Sie diese Anwendung jedoch weiterhin nutzen möchten, müssen Sie die unter Quarantäne gestellte *Spyware* wiederherstellen.

- Unter Quarantäne gestellte potenziell unerwünschte Anwendungen können für Ihren Computer oder Anwendungen, die Sie nutzen möchten, schädlich sein.

  Wenn Sie die Anwendung bewusst installiert und richtig eingerichtet haben, ist es weniger wahrscheinlich, dass diese schädlich ist. Wenn die Anwendung ohne Ihre Kenntnis installiert wurde, ist es sehr wahrscheinlich, dass sie bösartige Inhalte enthält und sollte entfernt werden.

4.4.1 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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Virenschutz**.
3. Klicken Sie auf **Quarantäne anzeigen**.
   Die Seite **Quarantäne** zeigt die Gesamtzahl der in der Quarantäne gespeicherten Elemente an.
4. Um detaillierte Informationen zu einem ausgewählten Element unter Quarantäne anzuzeigen, klicken Sie auf **Details**.

5. Wenn Sie weitere Informationen zu einem unter Quarantäne gestellten Element anzeigen möchten, klicken Sie neben dem Element auf das Symbol .

4.4.2 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 Statusseite auf **Einstellungen**.

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

2. Wählen Sie **Virenschutz**.
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?

Themen:

DeepGuard überwacht Anwendungen, um potenziell gefährliche Änderungen für das System zu ermitteln.

DeepGuard stellt sicher, dass Sie nur sichere Anwendungen nutzen. Die Sicherheit einer Anwendung wird durch den vertrauenswürdigen Cloud-Service verifiziert. Wenn die Sicherheit einer Anwendung nicht verifiziert werden kann, beginnt DeepGuard mit der Überwachung der Anwendung.

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

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.

5.1 Wählen Sie aus, was DeepGuard überwachen soll.

DeepGuard überwacht wichtige Systemeinstellungen und -dateien sowie jegliche Versuche, wichtige Anwendungen – einschließlich dieses Sicherheitsprodukts – zu deaktivieren.

Um zu wählen, was DeepGuard überwachen soll:

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

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

2. Wählen Sie **DeepGuard**.
3. Stellen Sie sicher, dass **DeepGuard** aktiviert ist.
4. Wählen Sie die Einstellungen für DeepGuard:

Bei verdächtigem Verhalten Warnung ausgeben	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit verdächtiges Verhalten angezeigt wird. Wird die Einstellung deaktiviert, beendet DeepGuard die Überwachung von verdächtigem Verhalten und das Sicherheitsniveau wird gesenkt.
Bei Auftreten von Anwendungs-Exploits Warnung ausgeben	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit Sie bei potenziellen Exploit-Versuchen gewarnt werden. Wenn diese Einstellung deaktiviert wird, können schädliche Websites und Dokumente auf Ihre Anwendungen zugreifen. Dadurch wird die Sicherheit beeinträchtigt. Wir empfehlen, dass Sie diese Einstellung nie deaktivieren.
Internetverbindung nur mit Erlaubnis herstellen	Stellen Sie sicher, dass diese Einstellung aktiv ist, damit Sie benachrichtigt werden, wenn eine unbekannte Anwendung versucht, eine Verbindung zum Internet herzustellen.
Wählen Sie Kompatibilitätsmodus verwenden (senkt die Sicherheit).	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.

5. Klicken Sie auf **OK**.

5.1.1 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 lassen Sie die von DeepGuard blockierte Anwendung zu:

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

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

2. Wählen Sie **DeepGuard**.
3. Klicken Sie auf**Anwendungsberechtigungen ändern**.
   Die Liste **Überwachte Anwendungen** wird angezeigt.
4. Wählen Sie die Anwendung aus, die Sie zulassen möchten, und klicken Sie auf **Details**.

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.

5. Wählen Sie **Zulassen**.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf den Link **Schließen** aus.

DeepGuard lässt erneut Systemänderungen durch die Anwendung zu.

5.2 Handhabung von Warnmeldungen zu verdächtigem Verhalten

DeepGuard blockiert die überwachten Anwendungen, wenn sie verdächtig agieren oder versuchen eine Verbindung zum Internet herzustellen.

Sie können je nach Situation entscheiden, ob Sie der Anwendung erlauben fortzufahren oder nicht.

5.2.1 DeepGuard blockiert eine schädliche Anwendung.

Sie erhalten eine Benachrichtigung von DeepGuard, wenn eine schädliche Anwendung erkannt und blockiert wurde.

Wenn die Benachrichtigung geöffnet wird:

Klicken Sie auf **Details**, um mehr Informationen zur Anwendung anzuzeigen.
Der Detailbereich enthält folgende Angaben:

- Speicherort der Anwendung
- die Bewertung der Anwendung in Security-Cloud,
- Verbreitung der Anwendung und
- Name der erkannten Malware.

Sie können eine verdächtige Anwendung zu Analyse einsenden.

5.2.2 DeepGuard blockiert eine verdächtige Anwendung.

Wenn die Einstellung **Bei verdächtigem Verhalten Warnung ausgeben** in DeepGuard aktiviert ist, werden Sie benachrichtigt, wenn sich eine Anwendung verdächtig verhält. Wenn Sie der Anwendung vertrauen, können Sie das Fortfahren zulassen.

So legen Sie fest, wie Sie mit der von DeepGuard blockierten Anwendung umgehen möchten:

1. Klicken Sie auf **Details**, um mehr Informationen zur Anwendung anzuzeigen.
   Der Detailbereich enthält folgende Angaben:
   - Speicherort der Anwendung
   - die Bewertung der Anwendung in Security-Cloud,
   - Verbreitung der Anwendung und
   - Name der Malware.
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.

Sie können eine verdächtige Anwendung zur Analyse einsenden.

5.2.3 Eine unbekannte Anwendung versucht eine Verbindung zum Internet herzustellen.

Wenn die Einstellung **Internetverbindung nur mit Erlaubnis herstellen** in DeepGuard aktiviert wird, werden Sie benachrichtigt, wenn eine unbekannte Anwendung versucht, eine Verbindung zum Internet herzustellen. Wenn Sie der Anwendung vertrauen, können Sie das Fortfahren zulassen.

So legen Sie fest, wie Sie mit der von DeepGuard blockierten Anwendung umgehen möchten:

1. Klicken Sie auf **Details**, um mehr Informationen zur Anwendung anzuzeigen.
   Der Detailbereich enthält folgende Angaben:
   - Speicherort der Anwendung
   - die Bewertung der Anwendung in Security-Cloud,
   - Verbreitung der Anwendung
   - was die Anwendung zu tun versucht hat und
   - wo die Anwendung eine Verbindung herzustellen versucht hat.
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 permanent 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.

Wenn der *Spielmodus* an ist, erlaubt DeepGuard auch unbekannten Anwendungen den Zugriff auf das Internet. Es blockiert aber weiterhin gefährliche Anwendungen, die versuchen eine Verbindung zum Internet herzustellen, auch wenn der *Spielmodus* an ist.

Sie können eine verdächtige Anwendung zur Analyse einsenden.

5.2.4 DeepGuard hat einen möglichen Exploit entdeckt.

Wenn die Einstellung **Bei Auftreten von Anwendungs-Exploits Warnung ausgeben** in DeepGuard aktiviert ist, erhalten Sie einen Hinweis, dass DeepGuard verdächtiges Verhalten entdeckt hat, nachdem Sie eine schädliche Website oder ein Dokument geöffnet haben.

So legen Sie fest, wie Sie mit der von DeepGuard blockierten Anwendung umgehen möchten:

1. Klicken Sie auf **Details**, um mehr Informationen zur Anwendung anzuzeigen.
   Der Detailbereich enthält folgende Angaben:
   - Name der Malware und
   - die Quelle des Exploits (eine schädliche Website oder ein Dokument), falls bekannt.

2. Geben Sie an, ob Sie der von DeepGuard blockierten Anwendung vertrauen:
   - Wählen Sie **Anwendung nicht schließen (kann Ihr Gerät gefährden)**, wenn die Anwendung nicht geschlossen werden soll.

     Möglicherweise wollen Sie die Anwendung zu diesem Zeitpunkt nicht schließen, wenn dadurch nicht gespeicherte Daten verloren gehen könnten.
   - Wählen Sie **Anwendung schließen, um Exploit zu verhindern**, wenn Sie die Anwendung schließen und sicherstellen möchten, dass Ihr Gerät keinem Risiko ausgesetzt wird.

     Wir empfehlen, dass Sie die Anwendung schließen, um Ihr Gerät keinem Risiko auszusetzen.

Wenn die Quelle des Exploits identifziert wurde, können Sie eine Probe zur Analyse einsenden.

5.3 Eine verdächtige Anwendung zur Analyse einsenden

Sie können dazu beitragen, den Schutz zu verbessern, wenn Sie verdächtige Anwendungen zur Analyse einsenden.

Wenn DeepGuard eine Anwendung blockiert, weil sie beispielsweise ein mögliches Sicherheitsrisiko für Ihren Computer darstellt oder versucht hat, eine möglicherweise schädliche Aktion auszuführen, können Sie uns ein Muster der Anwendung zur Sicherheitsforschung senden.

Sie können dies tun, wenn Sie wissen, dass die von DeepGuard blockierte Anwendung sicher ist oder wenn Sie den Verdacht haben, dass es sich um eine schädliche Anwendung handelt.

Um eine Probe zur Analyse einzusenden:

1. Wenn DeepGuard eine Anwendung blockiert, können Sie wählen, ob Sie die Anwendung blockieren oder dennoch ausführen möchten.
2. DeepGuard fragt, ob Sie die Anwendung zur Analyse einreichen möchten. Klicken Sie auf **Einreichen**, um das Muster einzureichen.

   Hinweis: DeepGuard fordert Sie nicht immer auf, ein Muster einzureichen. Beispielsweise dann nicht, wenn Sie bereits Informationen zu der blockierten Anwendung haben.

Was ist eine Firewall?

Themen:

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

Die Firewall lässt nur sichere Internetverbindungen auf Ihrem Computer zu und blockiert unberechtigte Eingriffe über das Internet.

6.1 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 Statusseite auf **Einstellungen**.

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

2. Aktivieren bzw. deaktivieren Sie **Firewall**.

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

3. Klicken Sie auf **OK**.

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.

6.2 Firewall-Einstellungen ändern

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 Windows Firewall-Einstellungen:

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

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

2. Wählen Sie **Firewall**.
3. Klicken Sie auf **Windows Firewall-Einstellungen ändern**.

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

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

6.3 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 Statusseite auf **Einstellungen**.

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

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

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

6.4 Verbindungen zu gefälschten Websites verhindern

Sie können benachrichtigt werden, wenn Ihr Netzwerk versucht, eine Verbindung mit einer gefälschten Website herzustellen.

Das Domain Name System (DNS) übersetzt Webadressen, die Sie eingeben, in ihre jeweilige IP-Adressen. Normalerweise ist Ihr Router mit einem DNS-Server verbunden, der Ihrem Internet-Anbieter gehört und von diesem auch verwaltet wird. Wenn sich ein Hacker oder schädliche Software Zugang zum Router verschafft, können sie diesen so modifizieren, dass er einen gefälschten DNS-Server nutzt.

Wenn der Router, mit dem Sie verbunden sind, auf diese Art und Weise gehackt wurde, leitet er Sie möglicherweise auf gefälschte Websites weiter, und führt Sie nicht auf die von Ihnen gewünschten Websites.

So erhalten Sie Benachrichtigungen, wenn Ihr aktuelles Netzwerk gehackt wurde:

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

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

2. Wählen Sie **Firewall**.
3. Wählen Sie **Ich möchte eine Warnung erhalten, wenn das aktuelle Netzwerk gefährdet ist**.

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

6.5 Verwendung von persönlichen Firewalls

Dieses Produkt ist auf die Verwendung mit Windows Firewall eingerichtet. Zur Verwendung mit anderen persönlichen Firewalls muss das Produkt individuell eingerichtet werden.

Das Produkt verwendet Windows Firewall für alle Firewall-Grundfunktionen, wie z. B. die Kontrolle des eingehenden Netzwerkverkehrs und die Trennung Ihres internen Netzwerks vom öffentlichen Internet. Zusätzlich überwacht DeepGuard installierte Anwendungen und verhindert, dass verdächtige Anwendungen ohne Ihre Zustimmung auf das Internet zugreifen.

Stellen Sie sicher, dass wenn Sie Windows Firewall durch eine andere persönliche Firewall ersetzen, diese allen ein- und ausgehenden Netzwerkverkehr für alle F-Secure-Prozesse zulässt, und dass Sie die F-Secure-Prozesse zulassen, wenn die persönliche Firewall dies anfragt.

Tipp: Wenn Ihre persönliche Firewall über einen manuellen Filtermodus verfügt, verwenden Sie diesen, um alle F-Secure-Prozesse zuzulassen.

Blockieren von Spams

Themen:

Verwenden Sie die Spam-Filterung, um den Eingang von Spam- und Phishing-Nachrichten in Ihrem Postfach zu verhindern.

Oft erkennt man aufgrund der Unmenge an *Spam*- und *Phishing*-Nachrichten die erwünschten E-Mails nicht mehr.

Eine E-Mail wird als *Spam* bezeichnet, wenn sie im Rahmen mehrerer Nachrichten mit fast identischem Inhalt versendet wird und Sie dem Erhalt dieser Nachricht nicht zugestimmt haben.

Mithilfe von *Phishing*-Nachrichten sollen Ihre persönlichen Daten gestohlen werden. Diese authentisch wirkenden Nachrichten werden von scheinbar seriösen Unternehmen verschickt und 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.

7.1 Aktivieren oder Deaktivieren der Spam-Filterung

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

So aktivieren bzw. deaktivieren Sie die Spam-Filterung:

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

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

2. Aktivieren oder deaktivieren Sie den **Spam-Filter**.
3. Klicken Sie auf **OK**.

Tipp: Erstellen Sie eine Spamfilterregel in Ihrem E-Mail-Programm, um Massenwerbung und betrügerische E-Mails automatisch in einen Spam-Ordner zu verschieben.

7.2 Spam-Nachrichten kennzeichnen

Spam-Filter können das Betrefffeld von Spam-Nachrichten kennzeichnen.

Hinzufügen des Textes [SPAM] zu Spam- und Phishing-Nachrichten:

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

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

2. Wählen Sie **Spamfilter**.
3. Wählen Sie **Spam im E-Mail-Betreff mit [SPAM] markieren**.
4. Klicken Sie auf **OK**.

Wenn Sie Spam- oder Phishing-E-Mails erhalten, fügt die Spam-Filterung den Text `[SPAM]` in die Betreffzeile des E-Mails ein.

7.3 Einrichten meiner E-Mail-Programme zum Spam-Filtern

Sie können in Ihrem E-Mail-Programm Regeln zur *Spam*- und *Phishing*-Filterung erstellen, damit unerwünschte Nachrichten direkt in einen separaten Ordner verschoben werden.

Der Spam-Filter markiert alle entdeckten E-Mails im Betrefffeld mit dem Präfix [SPAM]. Falls Sie diese Nachrichten automatisch aus Ihrem Posteingang entfernen möchten, müssen Sie einen Spam-Ordner und entsprechende Filterregeln in Ihrem E-Mail-Programm erstellen. Falls Sie mehrere E-Mail-Konten besitzen, müssen Sie für jedes Konto separat Filterregeln erstellen.

In diesem Abschnitt finden Sie Anleitungen zur Erstellung des Spam-Ordners und der Filterregeln für Windows Mail, Microsoft Outlook, Mozilla Thunderbird, Eudora und Opera. Mithilfe dieser Anleitungen können Sie auch ähnliche Filterregeln in anderen E-Mail-Programmen erstellen.

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

7.3.1 Spam in Windows Mail blockieren

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

Wenn Sie Spam- und Phishing-Filterung für Windows Mail verwenden, stellen Sie sicher, dass **Spam im E-Mail-Betreff mit [SPAM] markieren** in den Einstellungen **Spamfilterung** aktiviert ist.

So erstellen Sie eine *Spam*-Filterregel:

1. Wählen Sie im Menü von **Windows Mail** die Option **Ordner** > **Nachrichtenregeln**.

   Hinweis: Wenn das Fenster **Neue E-Mail- Regel** nicht automatisch angezeigt wird, klicken Sie auf der Registerkarte **E-Mail-Regeln** auf **Neu**.

2. Erstellen Sie im Fenster **Neue E-Mail-Regel** eine Regel, um eine E-Mail-Nachricht in den *Spam*-Ordner zu verschieben:
   a) Wählen Sie im Feld "Bedingungen" **Betreff enthält Suchbegriffe**.
   b) Wählen Sie im Aktionsfeld **In angegebenen Ordner verschieben**.
3. Klicken Sie im Feld für die Regelbeschreibung auf den Link **Enthält Suchbegriffe**.
   a) Geben Sie im Fenster **Suchbegriffe eingeben** `[SPAM]` ein und klicken Sie auf **Hinzufügen**.
   b) Klicken Sie auf **OK**, um das Fenster **Suchbegriffe eingeben** zu schließen.
4. Klicken Sie im Feld für die Regelbeschreibung auf den Link **Angegebener** Ordner.
   a) Klicken Sie im Fenster **Verschieben** auf **Neuer Ordner**.
   b) Geben Sie als neuen Ordnernamen `Spam` ein und klicken Sie auf **OK**.
   c) Klicken Sie auf **OK**, um das Fenster **Verschieben** zu schließen.
5. Geben Sie in das Feld für den Regelnamen `Spam` ein.
6. Klicken Sie auf **Regel speichern**, um das Fenster **Neue E-Mail-Regel** zu schließen.
   Das Fenster **Regeln** wird geöffnet.
7. Klicken Sie auf "OK", um das Fenster **Regeln** zu schließen.
   Wenn Sie die neue Regel für E-Mail-Nachrichten verwenden möchten, die sich bereits in Ihrem Posteingang befinden, wählen Sie die Regel **Spam** und klicken Sie auf **Jetzt anwenden**.

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

7.3.2 Spam in Microsoft Outlook blockieren

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

Wenn Sie Spam- und Phishing-Filterung für Microsoft Outlook verwenden, stellen Sie sicher, dass **Spam im E-Mail-Betreff mit [SPAM] markieren** in den Einstellungen **Spamfilterung** aktiviert ist.

Hinweis: Die hier angegebenen Schritte beziehen sich auf Microsoft Outlook 2007. Die Schritte für andere Versionen können leicht abweichen.

So erstellen Sie eine *Spam*-Filterregel:

1. Wählen Sie im Menü **Extras Regeln und Benachrichtigungen**.
2. Klicken Sie auf der Registerkarte **E-Mail-Regeln** auf **Neue Regel**.
3. Wählen Sie in der Liste **Den Überblick behalten** die Vorlage **Nachrichten mit bestimmten Wörtern im Betreff in einen Ordner verschieben**.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie im Bereich **2. Schritt: Regelbeschreibung bearbeiten** auf den Link**bestimmten Wörtern**.
   a) Geben Sie im Feld **Im Betreff oder Text zu suchende Wörter** `[SPAM]` ein und klicken Sie auf **Hinzufügen**.
   b) Klicken Sie auf **OK**, um das Fenster **Suchbegriffe eingeben** zu schließen.
6. Klicken Sie im Bereich **2. Schritt: Regelbeschreibung bearbeiten** auf den Ordnerlink **Zielordner**.
   a) Klicken Sie im Fenster **Regeln und Benachrichtigungen** auf **Neu**.
   b) Geben Sie als neuen Ordnernamen `Spam` ein und klicken Sie auf **OK**.
   c) Klicken Sie auf **OK**, um das Fenster **Regeln und Benachrichtigungen** zu schließen.
7. Klicken Sie auf **Fertig stellen**.
8. Klicken Sie auf **OK**.
   Wenn Sie die neue Regel für E-Mail-Nachrichten verwenden möchten, die sich bereits in Ihrem Posteingang befinden, klicken Sie auf **Regeln jetzt anwenden**, bevor Sie das Fenster schließen.

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

7.3.3 Blockieren von Spams 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. Erstellen eines neuen Ordners für Spam- und Phishing-Nachrichten:
   a) Rechtsklicken Sie auf den Namen Ihres E-Mail-Kontos und wählen Sie **Neuer Ordner**.
   b) Geben Sie `Spam` als neuen Ordnernamen ein.
   c) Klicken Sie auf **Ordner erstellen**.
2. Stellen Sie sicher, dass Ihr Kontoname ausgewählt ist und klicken Sie auf **Nachrichtenfilter verwalten** in der Liste **Erweiterte Funktionen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie `Spam` als **Filtername** ein.
5. Erstellen Sie einen benutzerdefinierten Headereintrag:
   a) In der Liste **Trifft auf alle folgenden zu** öffnen Sie das erste Drop-Down-Menü, das standardmäßig **Betreff** ausgewählt hat.
   b) Wählen Sie in der ersten Dropdown-Liste **Anpassen** aus.
   c) Geben Sie im Dialogfeld **Header anpassen** als neuen Nachrichten-Header `X-Spam-Flag` ein und klicken sie auf **Hinzufügen**.
   d) Klicken Sie auf **OK**, um das Dialogfeld **Header anpassen** zu schließen.
6. Erstellen einer Regel zum Filtern von Spam-Nachrichten:
   a) In der Liste **Trifft auf alle folgenden zu** öffnen Sie das erste Drop-Down-Menü und wählen Sie das im vorhergehenden Schritt erstellte **X-Spam-Flag** aus.
   b) Wählen Sie **enthält** aus dem zweiten Drop-Down-Menü aus.
   c) Geben Sie `Ja` als Text ein, der auf die letzte Textbox in der Zeile zutreffen soll.
7. Erstellen Sie eine Aktivität, die Spam-Nachrichten in den Spam-Ordner verschiebt:
   a) In der Liste **Diese Aktionen ausführen** wählen Sie**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.

7.3.4 Blockieren von Spams in Opera

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

Hinweis: Die hier angegebenen Schritte gelten für Opera Version 12. Die erforderlichen Schritte für die anderen 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) Wählen Sie aus der ersten Liste die Option **Beliebiger Header**.
   b) Wählen Sie aus der zweiten Liste die Option **enthält**.
   c) Geben Sie im Textfeld `X-Spam-Flag: Yes` als Text für die Übereinstimmung ein.
   Achten Sie darauf, dass sich zwischen dem Doppelpunkt und `Ja` ein Leerzeichen befinden muss.
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.

Sichere Nutzung des Internets

Themen:

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.

Hinweis: Die von Ihnen installierte Version des Produkts verfügt möglicherweise nicht über alle hier beschriebenen Funktionen.

8.1 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.

8.1.1 Erstellen von Windows-Benutzerkonten

Über dieses Produkt können Sie neue Windows-Benutzerkonten erstellen.

So erstellen Sie Windows-Benutzerkonten:

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

Auf der Hauptseite des Produkts werden sowohl der Benutzername als auch die Art des Benutzerkontos angezeigt.

8.1.2 Anzeigen der Statistik

Auf der Seite **Einstellungen** > **Andere** > **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.

Die Informationen geben an, ob die blockierte Seite über von Ihnen bewusst blockierte Inhalte verfügt oder ob das Produkt die Seite als potentiell schädlich einstuft.

8.2 Die Funktionen von Browser-Erweiterungen

Das Produkt installiert Erweiterungen (Plug-in-Anwendungen mit zusätzlichen Funktionen) auf allen Ihren Browsern, um beispielsweise den Browser-Schutz auf sicheren (HTTPS-) Websites zu unterstützen.

Durch die Browsererweiterungen des Produkts wird sichergestellt, dass alle Sicherheitsfunktionen verfügbar sind. Wenn die Erweiterungen nicht genutzt werden, funktionieren einige Schutzfunktionen möglicherweise nicht ordnungsgemäß.

Ihr Browser sollte die Erweiterung automatisch installieren und aktivieren. In manchen Fällen kann es jedoch sein, dass Sie die Erweiterung manuell erneut installieren und aktivieren müssen.

Auf der Hauptseite des Produkts wird angezeigt, wenn die Browser-Erweiterung nicht installiert oder inaktiv ist.

Zur erneuten Installation der Browser-Erweiterungen:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Browser-Erweiterungen**.
3. Klicken Sie auf **Erweiterungen erneut installieren**.
   So werden die Erweiterungen des Produkts auf allen Ihren aktuell installierten Browsern erneut installiert.
4. Wählen Sie **Erweiterungen anlassen**, wenn Sie möchten, dass das Produkt automatisch dafür sorgt, dass die Browser-Erweiterungen für Internet Explorer und Firefox aktiviert sind.

Wenn Sie die Browser-Erweiterungen manuell aktivieren möchten, müssen Sie Ihre Browser-Einstellungen bearbeiten:

- Wählen Sie in Firefox aus der Menüleiste **Extras** > **Add-ons** und klicken Sie dann neben der Erweiterung auf **Aktivieren**.
- Wählen Sie im Chrome-Menü **Einstellungen** aus, klicken Sie auf **Erweiterungen** und wählen Sie die Option **Aktivieren** neben der Erweiterung.
- Gehen Sie in Internet Explorer auf **Extras** > **Add-ons verwalten**, wählen Sie die Browser-Erweiterung aus und klicken Sie auf **Aktivieren**.

Hinweis: Wenn Sie die Erweiterungen manuell aktivieren müssen, sollten Sie die Aktivierung separat für die einzelnen Benutzerkonten auf Ihrem Computer vornehmen.

8.3 Was sind Sicherheitsbewertungen?

Sicherheitsbewertungen in den Suchergebnissen helfen bei der Vermeidung von Gefahren aus dem Internet.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.

Diese Webseite ist unseres Wissens sicher. Wir haben nichts Verdächtiges auf der Website gefunden.

Diese Seite ist verdächtig und wir empfehlen Ihnen, dass Sie vorsichtig beim Besuchen dieser Website sind. Vermeiden Sie das Herunterladen von Dateien oder die Angabe von personenbezogenen Daten.

Diese Seite ist gefährlich. Wir empfehlen Ihnen, dass Sie vermeiden, diese Website zu besuchen.

Wir haben die Website noch nicht analysiert und es liegen derzeit keine Informationen über sie vor.

Der Administrator hat Ihnen das Besuchen dieser Website erlaubt.

Der Administrator hat diese Website gesperrt und Sie können sie nicht besuchen.

8.4 Worum handelt es sich beim Browser-Schutz?

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

Der Browser-Schutz zeigt Sicherheitsbewertungen für die in den Suchmaschinenergebnissen aufgeführten Websites an. Er erkennt Websites mit Sicherheitsbedrohungen wie Malware (Viren, Würmer, Trojaner) und Phishing. So können Sie die aktuellsten Internetbedrohungen umgehen, die von herkömmlichen Virenschutzprogrammen noch nicht erkannt werden.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.

8.4.1 So aktivieren Sie den Browser-Schutz.

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

So aktivieren Sie den Browser-Schutz:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Browser-Schutz**.
3. Klicken Sie oben rechts auf die Umschalttaste.

4. Wenn Sie die Sicherheitsbewertung für Websites in Ihren Suchergebnissen (Google, Yahoo und Bing) anzeigen möchten, wählen Sie **Die Reputationsbewertung für Websites in Suchergebnissen anzeigen**.
5. Wenn Ihr Browser geöffnet sie, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

8.4.2 Was tun, wenn eine Webseite blockiert wird

Wenn Sie versuchen, auf eine Webseite zuzugreifen, die als schädlich eingestuft wurde, erscheint eine Browser-Schutz-Sperrseite.

Wenn eine Browser-Schutz-Sperrseite erscheint:

1. Wenn Sie die Webseite trotzdem aufrufen möchten, klicken Sie auf **Webseite zulassen**.
   Die Benutzerzugangssteuerung von Windows fordert Sie dazu auf, diese Aktion zu bestätigen.
2. Geben Sie, wenn nötig, die Daten Ihres Administratorkontos ein und bestätigen Sie dann die Änderung.

8.5 Sicheres Online-Banking

Der Banking-Schutz schützt Sie vor schädlichen Aktivitäten beim Zugriff auf Ihre Online-Bank oder beim Durchführen von Online-Transaktionen.

Der Banking-Schutz erkennt automatisch sichere Verbindungen zu Online-Banking-Websites und blockiert alle Verbindungen, die nicht zur gewünschten Seite führen. Wenn Sie eine Online-Banking-Website öffnen, sind lediglich Verbindungen zu Online-Banking-Websites oder zu Websites, die als sicher für Online-Banking eingestuft werden, zulässig.

Banking-Schutz unterstützt derzeit die folgenden Browser:

- Internet Explorer 9 oder höher
- Firefox 13 oder höher
- Google Chrome

8.5.1 Aktivieren des Banking-Schutzes

Wenn der Banking-Schutz aktiviert ist, sind Ihre Online-Banking-Sitzungen und -Transaktionen geschützt.

So aktivieren Sie den Banking-Schutz:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und wählen Sie **Einstellungen**.
   Die Seite **Einstellungen** wird geöffnet.

   Hinweis: Sie benötigen Administratorrechte, um auf diese Seite zuzugreifen.
3. Wählen Sie **Banking-Schutz**.
4. Klicken Sie auf den Schalter rechts oben, um den Banking-Schutz an- und auszuschalten.
5. Wählen Sie **OK**.
   Der Banking-Schutz ist nun für das ausgewählte Benutzerkonto aktiviert.
6. Wenn Ihre aktuellen Verbindungen offen bleiben sollen, wählen Sie **Meine aktiven Internetverbindungen nicht unterbrechen**.

   Wenn Sie die Website Ihrer Bank aufrufen oder Online-Zahlungen durchführen, wird der Banking-Schutz aktiviert und blockiert alle für Online-Banking nicht notwendige Verbindungen. Das bedeutet, dass auch alle Ihre aktuellen Internetverbindungen getrennt werden, es sei denn, Sie wählen diese Einstellung.

8.5.2 Verwenden des Banking-Schutzes

Wenn der Banking-Schutz aktiviert ist, erkennt er automatisch, wenn Sie eine Online-Banking-Website aufrufen.

Wenn Sie eine Online-Banking-Webseite in Ihrem Browser öffnen, wird die Benachrichtigung **Banking-Schutz** oben auf Ihrem Bildschirm angezeigt. Während die Banking-Schutz-Sitzung geöffnet ist, sind alle anderen Verbindungen blockiert.

Tipp: Wenn Sie Ihre anderen aktiven Verbindungen während des Online-Banking nicht unterbrechen möchten, klicken Sie **Einstellungen ändern** auf der Benachrichtigung, um die Produkteinstellungen für Ihr Benutzerkonto zu ändern.

So beenden Sie die Banking-Schutz-Sitzung und stellen Ihre anderen Verbindungen wieder her:

Klicken Sie in der Benachrichtigung **Banking-Schutz** auf **Beenden**.

8.6 Zugriff auf Webinhalte wird begrenzt.

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: Der eingeschränkte Zugriff auf Online-Inhalte schützt Ihre Benutzerkonten vor Chat- und E-Mail-Programmen, die in Ihrem Webbrowser ausgeführt werden.

Sie können die Webseiten einschränken, die angezeigt werden können. Darüber hinaus können Sie die Zeit beschränken, die online verbracht werden kann. Sie können auch verhindern, dass Links zu nicht jugendfreien Inhalten in Suchmaschinenergebnissen angezeigt werden. Diese Einschränkungen werden auf die Windows-Benutzerkonten angewandt, d. h. immer wenn sich jemand mit seinem Benutzerkonto anmeldet, gelten die eingerichteten Beschränkungen.

8.6.1 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. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Inhaltssperre**.
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie die Option **Nur ausgewählte Websites zulassen**.
5. Klicken Sie auf **Hinzufügen**, um Websites zur Liste **Zugelassene Websites** hinzuzufügen.
6. Wenn Sie alle Websites, die Sie zulassen möchten, hinzugefügt haben, klicken Sie auf **OK**.

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.

8.6.2 Webseiten anhand ihres Inhalts sperren

Sie können den Zugang zu Websites mit ungeeigneten Inhalten blockieren.

So wählen Sie die zu blockierenden Inhaltstypen aus:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.

2. Wählen Sie **Inhaltssperre**.
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie **Webinhalte blockieren**.
5. Wählen Sie die Inhaltstypen aus, die Sie blockieren möchten.
6. Wenn Sie alle Inhaltstypen, die Sie blockieren möchten, ausgewählt haben, klicken Sie auf **OK**.

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.

8.6.3 Zugelassene und blockierte Websites bearbeiten

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

Hinweis: Abhängig von der verwendeten Produktversion kann es sein, dass Sie den Zugang zu Websites entweder erlauben oder blockieren können, nicht jedoch beides.

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. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Inhaltssperre**.
3. Klicken Sie auf **Website-Ausnahmen anzeigen**.

   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 die Adresse der Website ein, die Sie hinzufügen möchten, und klicken Sie auf **OK**.
   d) Klicken Sie im Dialogfeld **Website-Ausnahmen** auf **Schließen**.
4. Klicken Sie auf **OK**, 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**.

8.6.4 Suchergebnisfilter verwenden

Sie können den Suchergebnisfilter aktivieren, um explizite Inhalte aus den Suchergebnissen zu blockieren.

Der Suchergebnisfilter blendet nicht-jugendfreie Inhalte aus, indem sichergestellt wird, dass Google, Yahoo und Bing das SafeSearch-Level "streng" verwenden. Dadurch können unangemessene und explizite Inhalte zwar nicht völlig aus den Suchergebnissen blockiert werden, aber das meiste Material dieser Art wird vermieden.

So aktivieren Sie den Suchergebnisfilter:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.

Das Dialogfeld **Einstellungen** wird geöffnet.

2. Wählen Sie **Kindersicherung** > **Suchergebnisfilter**.
3. Klicken Sie oben rechts auf die Umschalttaste.

Wenn der Suchergebnisfilter aktiviert ist, werden die Einstellungen von SafeSearch für Websites für alle überschrieben, die über dieses Windows-Benutzerkonto eingeloggt sind.

8.7 Zeitlimits werden festgelegt.

Sie können festlegen, wann und wie lange dieser Computer genutzt werden kann.

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

- Wenn jemand den Computer nutzen oder im Internet surfen darf, können Sie beispielsweise festlegen, dass der Zugang nur vor 8 Uhr abends möglich ist.
- Wie lange jemand den Computer nutzen oder im Internet surfen darf. Sie können beispielsweise festlegen, dass der Zugang auf eine Stunde täglich begrenzt ist.

Hinweis: Wenn Sie die Zeitbeschränkungen für einen Nutzer entfernen, dann dieser jederzeit den Computer nutzen oder im Internet surfen.

So richten Sie die erlaubten Zeiten ein:

1. Wählen Sie auf der Hauptseite das Windows-Benutzerkonto aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen**.
   Das Dialogfeld **Einstellungen** wird geöffnet.
2. Wählen Sie **Zeitlimits**.
3. Klicken Sie oben rechts auf die Umschalttaste.
4. Wählen Sie, welche Zugangsart Sie einschränken möchten:
   - Wenn Sie den allgemeinen Zugang zum Computer einschränken möchten, wählen Sie **Den Computer sperren**.
   - Wenn Sie das Surfen im Internet einschränken möchten, wählen Sie **Nur das Surfen blockieren**.
5. Legen Sie die erlaubten Zeiten für jeden Wochentag in der Tabelle *erlaubte Zeiten* fest.
   Wenn Sie den Zugang nicht auf bestimmte Zeiten einschränken wollen, vergewissern Sie sich, dass alle Zellen in der Tabelle ausgewählt sind.
6. Wählen Sie die maximale Anzahl an erlaubten Stunden pro Tag.
   Wenn Sie die Zeit, in der der Computer genutzt werden darf, nicht begrenzen möchten, stellen Sie sicher, dass die Zahl der erlaubten Stunden auf **Max.** gestellt ist.
7. Klicken Sie auf **OK**.

Diese Zeitlimits gelten nun für jeden, der das ausgewählte Windows-Nutzerkonto verwendet.

Was ist Safe Search?

Themen:

Safe Search zeigt die Sicherheit von Websiten in den Suchergebnissen an und verhindert, dass Sie unabsichtlich auf gefährliche Websites zugreifen.

Safe Search ermittelt Websites, die Sicherheitsbedrohungen enthalten, wie z. B. Malware (Viren, Würmer,Trojaner) oder versuchen Ihre sensiblen Daten, wie z. B. Benutzernamen und Passwörter zu stehlen.

9.1 Was sind Sicherheitsbewertungen?

Sicherheitsbewertungen in den Suchergebnissen helfen bei der Vermeidung von Gefahren aus dem Internet.

Die Sicherheitsbewertungen basieren auf Informationen aus mehreren Quellen, wie Malware-Analysten und Partnern von F-Secure.


Diese Webseite ist unseres Wissens sicher. Wir haben nichts Verdächtiges auf der Website gefunden.


Diese Seite ist verdächtig und wir empfehlen Ihnen, dass Sie vorsichtig beim Besuchen dieser Website sind. Vermeiden Sie das Herunterladen von Dateien oder die Angabe von personenbezogenen Daten.


Diese Seite ist gefährlich. Wir empfehlen Ihnen, dass Sie vermeiden, diese Website zu besuchen.


Wir haben die Website noch nicht analysiert und es liegen derzeit keine Informationen über sie vor.


Der Administrator hat Ihnen das Besuchen dieser Website erlaubt.


Der Administrator hat diese Website gesperrt und Sie können sie nicht besuchen.

9.2 Safe Search in Ihrem Webbrowser einrichten

Safe Search unterstützt die folgenden Internetbrowser:

- Internet Explorer 8 für Windows XP SP3
- Internet Explorer, zwei zuletzt veröffentlichte Versionen für Windows Vista, Windows 7 und Windows 8
- Firefox, zwei zuletzt veröffentlichte Versionen
- Google Chrome, zwei zuletzt veröffentlichte Versionen.

9.2.1 Verwenden von Safe Search mit Internet Explorer

Sie können Safe Search als Ihre Standard-Startseite, es als einen Suchanbieter hinzufügen und die Suchleiste installieren, wenn Sie Internet Explorer verwenden.

Befolgen Sie diese Anweisungen, um Safe Search mit Internet Explorer zu verwenden:

1. Internet Explorer öffnen.
2. Wenn Internet Explorer eine Nachricht anzeigt, dass das Toolbar-Add-On jetzt verwendet werden kann, klicken Sie auf **Aktivieren**. Wenn stattdessen in einem Dialogfenster angezeigt wird **Mehrere Add-Ons können jetzt verwendet werden.**, klicken Sie zunächst auf **Add-Ons auswählen**.

   
   Hinweis: In Internet Explorer 8 ist die Toolbar automatisch bereit zur Verwendung.

   
   Hinweis: Diese Nachricht erscheint nicht, wenn Sie die Suchleiste während der Installation nicht installiert haben.

3. So legen Sie Safe Search als Ihren Standard-Suchanbieter fest:
   a) > Wählen Sie ExtrasInternetoptionen aus.
   b) Klicken Sie unter **Suche** auf **Einstellungen**.
   c) Klicken Sie mit der rechten Maustaste in der Liste **Suchanbieter** auf Safe Search und wählen Sie **Als Standard festlegen**.

9.2.2 Verwenden von Safe Search mit Firefox

Sie können Safe Search als Ihre Standard-Startseite festlegen, es als einen Suchanbieter hinzufügen und die Suchleiste installieren, wenn Sie Firefox verwenden.

Hinweis: Wenn Ihre Firefox-Konfiguration die Änderung der Startseite und des Standard-Suchanbieters verhindert, kann auch Safe Search diese Einstellungen nicht ändern.

Folgen Sie diesen Anweisungen, um die Safe Search-Suchleiste mit Firefox zu verwenden, nachdem Sie das Produkt installiert haben.

1. Firefox öffnen.
2. Gehen Sie zum Reiter **Add-on installieren**.
3. Stellen Sie sicher, dass es sich beim zu installierenden Add-on um *Safe Search* handelt.
4. Markieren Sie das Kontrollkästchen **Diese Installation zulassen**.
5. Klicken Sie auf **Fortfahren**.
6. Klicken Sie auf **Firefox neu starten**.

9.2.3 Verwenden von Safe Search mit Chrome

Sie können Safe Search als Ihren Standard-Suchanbieter festlegen und die Suchleiste installieren, wenn Sie Chrome verwenden.

Wenn Sie Chrome als Standardbrowser verwenden, können Sie durch die Installation des Produkts auch die Suchleiste installieren und Safe Search automatisch als Suchanbieter hinzufügen.

So legen Sie Safe Search als Ihren Standard-Suchanbieter fest:

1. Öffnen Sie die **Einstellungen** im Chrome-Menü.
2. Finden Sie die Einstellungen zu **Suche**.
3. Klicken Sie auf **Suchmaschinen verwalten**.
4. Klicken Sie auf der Safe Search-Reihe auf **Als Standard festlegen**.

9.3 Safe Search entfernen

9.3.1 Safe Search aus Internet Explorer entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Internet Explorer zu entfernen:

1. Öffnen Sie die Windows Systemsteuerung.
2. Öffnen Sie **Netzwerk und Internet** > **Internetoptionen**.
   Das Fenster **Interneteigenschaften** wird geöffnet.
3. Um Safe Search als Standard-Homepage zu deaktivieren, befolgen Sie diese Anweisungen:
   a) In **Interneteigenschaften** öffne den Reiter **Allgemein**.
   b) Unter **Homepage** klicken Sie auf **Standardeinstellung verwenden**.
4. In **Interneteigenschaften** öffnen Sie den Reiter **Programme**.
5. Klicken Sie auf **Add-ons verwalten**.
   Das Fenster **Add-ons verwalten** wird geöffnet.
6. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anweisungen:
   a) In **Add-ons verwalten** wählen Sie **Suchanbieter**.
   b) Wählen Sie *Safe Search*.
   c) Klicken Sie auf **Entfernen**.
7. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:
   a) In **Add-ons verwalten** wählen Sie **Symbolleisten und Erweiterungen**.
   b) Wählen Sie *Safe Search*.
   c) Klicken Sie auf **Deaktivieren**.

Hinweis: Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.

9.3.2 Safe Search aus Firefox entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Firefox zu entfernen.

1. Um Safe Search als Standard-Homepage zu deaktivieren, befolgen Sie diese Anweisungen:
   a) Gehen Sie zu **Extras** > **Einstellungen**.
   a) Im Fenster **Optionen** öffnen Sie den Reiter **Allgemein**.
   b) Klicken Sie **Auf Standard zurücksetzen** unter dem Feld **Homepage**.
2. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anwendungen.
   a) Klicken Sie auf das Symbol Suchanbeiter im Suchfeld, um das Menü Suchmaschine zu öffnen.
   b) Klicken Sie auf **Suchmaschinen verwalten**.
   c) Wählen Sie *Safe Search* aus der Liste und klicken Sie auf **Entfernen.**
   d) Klicken Sie auf **OK**.
3. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:
   a) Gehen Sie zu **Extras** > **Add-ons**.
   b) Im Fenster **Add-ons-Manager** öffnen Sie den Reiter **Erweiterungen**.
   c) Klicken Sie auf **Deaktivieren** in der Zeile Safe Search-Erweiterung.
   d) Starten Sie Ihren Browser neu, um die Symbolleiste zu entfernen.

Hinweis: Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.

9.3.3 Safe Search aus Chrome entfernen

Befolgen Sie diese Anweisungen, um Safe Search aus Chrome zu entfernen.

1. Um Safe Search nicht mehr als Suchanbieter zu verwenden, befolgen Sie diese Anweisungen:
   a) Öffnen Sie die **Einstellungen** im Chrome-Menü.
   b) Finden Sie die Einstellungen zu **Suche**.
   c) Klicken Sie auf **Suchmaschinen verwalten**.
   d) Klicken Sie auf **X** am Ende der Safe Search-Zeile.
2. Um die Safe Search-Symbolleiste zu entfernen, befolgen Sie diese Anweisungen:
   a) Rechtsklicken Sie auf das Symbol für die Safe Search-Symbolleiste.
   b) Wählen Sie **Aus Chrome-Browser entfernen**.

Hinweis: Deinstallieren Sie Safe Search, um die Safe Search-Suchmaschine und die Symbolleiste vollständig zu entfernen.