

F-Secure Internet Security 2010
F-Secure Anti-Virus 2010
Benutzerhandbuch

Inhalt

Kapitel 1: Installation	9
Systemanforderungen.....	10
F-Secure-Lizenz.....	11
Vor der Installation.....	11
Installationsschritte.....	12
Haftungsausschluss.....	13
Kapitel 2: Einstieg	15
Was nach dem Installieren zu tun ist	16
Einrichten meiner E-Mail-Programme zum Spam-Filtern	16
Browsingprofile erstellen.....	16
Wie kann ich sicherstellen, dass mein Computer geschützt ist?.....	18
Was zeigt das Systemleistsymbol an?.....	18
Ansicht meines allgemeinen Schutzstatus	19
Woher weiß ich, ob mein Abonnement gültig ist?.....	21
Ausführen allgemeiner Aufgaben.....	23
Öffnen des Produktes.....	23
Erweiterte Einstellungen öffnen.....	23
Verwendung von Verknüpfungen.....	24

Mein Abonnement erneuern	28
Vollversion des Produkts kaufen.....	29
Wie erkennt man, was das Produkt geleistet hat?.....	30
Statistiken anzeigen.....	30
Was sind Benachrichtigungsfenster?.....	30
Was ist das Real Time Protection Network?	32
Datenschutzerklärung.....	32
Kapitel 3: Meinen Computer vor Malware schützen.....	33
Was sind Viren und Malware?.....	34
Viren.....	34
Spyware.....	34
Rootkits.....	35
Riskware.....	35
Wie scanne ich meinen Computer?	36
Auf Malware scannen.....	36
Zu festgelegten Zeiten scannen.....	40
Manuell scannen.....	42
Zu prüfende Dateien auswählen.....	46
Auswählen der durchzuführenden Aktion, wenn ein Virus gefunden wurde.....	50
Viren- und Spyware-Historie.....	54
Was ist DeepGuard?	55

Wie funktioniert DeepGuard?.....	55
Einschalten von DeepGuard.....	55
Programme zulassen, die von DeepGuard blockiert wurden.....	56
So schalten Sie die erweiterte Prozessüberwachung aus.....	57
Schutz gegen schädliche Systemänderungen.....	57
Anzeigen des von DeepGuard durchgeführten Vorgangs.....	59
Wie verwende ich die Quarantäne?.....	61
Unter Quarantäne gestellte Elemente anzeigen.....	61
Wiederherstellen von Elementen aus der Quarantäne.....	62
Verwendung automatischer Updates.....	64
Den Update-Status überprüfen.....	64
Meine Internetverbindungseinstellungen ändern.....	64
Kapitel 4: Netzwerkverbindungen sichern.....	67
Was ist eine Firewall?.....	68
Was sind Firewallprofile?.....	68
Was sind Firewallregeln und -dienste?.....	70
Datenverkehr im Netzwerk durch die Firewall zulassen oder blockieren	79
Was tun, wenn ein Firewall-Alarm angezeigt wird?.....	79
Firewalldienste und -regeln erstellen.....	80
So öffnen Sie einen Port durch die Firewall.....	87
Beispiele für das Erstellen von Firewallregeln.....	88

Firewallregeln ein- oder ausschalten.....	91
Firewallregeln ändern.....	92
Firewalleinstellungen.....	92
So kontrollieren Sie Netzwerkanwendungen.....	96
Was tun, wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird?.....	97
Verbindungen für Programme zulassen oder ablehnen.....	100
Popup-Fenster der Anwendungssteuerung ein- oder ausschalten.....	101
Was tun, wenn ein Programm nicht mehr funktioniert?.....	102
So wehren Sie Eindringlinge ab.....	104
Auswählen, wie Eindringversuche behandelt werden.....	104
So steuern Sie DFÜ-Verbindungen.....	106
Was tun, wenn ein Popup-Fenster der Einwahlkontrolle angezeigt wird?.....	106
Zulässige Telefonnummern bearbeiten.....	108
Programme anzeigen, die Einwahlverbindungen herstellen dürfen.....	109
DFÜ-Verbindungsversuche anzeigen.....	110
Wie gehe ich vor, wenn meine Internetverbindung nicht mehr funktioniert?.....	111
Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?.....	112
Firewall-Alarme anzeigen.....	112
Aktionsprotokoll anzeigen.....	114
Kapitel 5: Sichere Nutzung des Internets.....	121
Was ist Surfschutz.....	122

Den Surfschutz ein- oder ausschalten.....	122
Surfschutz-Sicherheitsbewertungen.....	123
Schutz gegen schädlichen Inhalt.....	125
Was tun, wenn eine Webseite blockiert wird.....	127
Sicherheitszusammenfassung für eine Webseite.....	127
Spam blockieren.....	129
Einrichten meiner E-Mail-Programme zum Spam-Filtern	129
Was passiert, wenn ich zahlreiche Spammessages erhalte?.....	137
Nachrichten von bestimmten E-Mail-Adressen zulassen oder sperren.....	140
Schutz gegen Phishing-Versuche.....	143
Kapitel 6: Den Internetaufenthalt für Kinder sicher machen.....	145
Was sind Browsingprofile?.....	146
Wozu benötige ich Eltern- und Teenagerpasswörter?.....	148
Passwörter erstellen oder ändern.....	149
Elternpasswort ändern.....	149
Teenagerpasswort ändern.....	150
Zugriff auf das Internet bei aktivierter Kindersicherung.....	151
Zwischen den verschiedenen Browsingprofilen umschalten.....	151
Webseiten freigeben und sperren.....	153
Internetzugriff für kleinere Kinder beschränken.....	153
Internetzugriff für Teenager beschränken.....	155

Wie prüfe ich nach, ob Kinder nicht auf gesperrte Webseiten zugreifen können?.....	158
Online-Zeiten festlegen.....	159
Was versteht man unter der Kindersicherungs-Uhr?.....	159
Tägliche Internetzeiten einschränken.....	159
Internetzeiten festlegen.....	160
Verlängern der Surfzeiten.....	161
Wie prüfe ich nach, ob Kinder nur während der erlaubten Zeiten zugreifen?.....	162
Wo Sie den Browser-Verlauf überprüfen können.....	163
Webseiten anzeigen, die meine Kinder besucht haben.....	165
Was tun, wenn ich mein Elternpasswort vergessen habe?.....	166

Kapitel 1

Installation

Themen:

- *Systemanforderungen*

Systemanforderungen

Bitte lesen Sie vor der Verwendung des Produkts folgende Hinweise.

Zur Installation und Verwendung des Produkts muss der Computer folgende Anforderungen erfüllen:

Systemanforderungen

Prozessor:

- Windows Vista oder Windows 7: Intel Pentium 4 2 GHz oder höher
- Windows XP: Intel Pentium III 1 GHz oder höher

Betriebssystem:

- Windows 7 32-bit oder 64-bit
- Windows Vista 32-bit oder 64-bit
- Windows XP SP2 oder höher

Arbeitsspeicher:

- Windows Vista oder Windows 7: 1 GB RAM oder mehr
- Windows XP: 512 MB RAM oder mehr

Festplattenspeicher:

800 MB freier Festplattenspeicher

Bildschirm:

- Windows Vista oder Windows 7: 16 bit oder mehr (65 000 Farben)
- Windows XP: 16 bit, 65 000 Farben oder mehr

Internetverbindung: Erforderlich für die Bestätigung der Anmeldung und zum Herunterladen von Updates



F-Secure-Lizenz

Im Folgenden erhalten Sie Informationen zur Produktlizenz.

Bei einer Lizenz für mehr als 1 PC beginnt der Gültigkeitszeitraum mit der ersten Installation.

Die Lizenzbedingungen erhalten Sie zusammen mit der Software.

Registrieren der Lizenz

Durch die Lizenzregistrierung sind Sie berechtigt, weitere Dienste in Anspruch zu nehmen, z. B. kostenlose Produktupdates und Produktunterstützung. Sie können Ihre Lizenz über das Formular unter folgender Adresse registrieren: www.f-secure.com/register

Vor der Installation

Bitte lesen Sie die folgenden Informationen, bevor Sie das Produkt installieren.

- Wenn Sie eine frühere Version von F-Secure Internet Security oder F-Secure Anti-Virus verwenden, können sie dieses Produkt direkt installieren. Befolgen Sie die Anweisungen in "Installationsschritte".
- Wenn Sie bereits die Testversion von F-Secure Internet Security 2010 oder F-Secure Anti-Virus 2010 auf Ihrem Computer installiert und die lizenzierte Version gekauft haben, können Sie sie verwenden, sobald Sie den Abonnementschlüssel eingegeben haben.

So geben Sie den Abonnementschlüssel ein:

1. Klicken Sie auf der Hauptseite auf **Aufgaben**.
2. Klicken Sie auf **Meine Anmeldung**.
3. Wählen Sie **Neuen Abonnementschlüssel eingeben...** aus.
4. Geben Sie Ihren Abonnementschlüssel in das Dialogfeld ein, und klicken Sie auf **Registrieren**.

Wenn Sie Ihren Abonnementschlüssel per E-Mail erhalten haben, können Sie den in der E-Mail enthaltenen Abonnementschlüssel kopieren und in das Feld einfügen.

Installationsschritte

Sie benötigen die Produkt-CD oder ein heruntergeladenes Installationspaket, einen gültigen Abonnementschlüssel sowie eine Internet-Verbindung. Wenn der Computer für mehrere Benutzer freigegeben ist, müssen Sie sich mit Administratorrechten anmelden, um dieses Produkt zu installieren. Für die Installation ohne CD befolgen Sie bitte die Anweisung des beigefügten Blattes "Wenn Ihr Computer über kein CD-ROM-Laufwerk verfügt".

So installieren Sie die Software:

1. Legen Sie die Installations-CD ein.

Die Installation sollte automatisch starten. Falls sie nicht automatisch gestartet wird, wechseln Sie zum Windows-Explorer, doppelklicken Sie auf das Symbol der CD-ROM, und doppelklicken Sie dann auf die Datei `f-secure2010.exe`, um die Installation zu starten.

Das erste Installationsdialogfeld wird angezeigt.

- 2.** Wählen Sie die Installationssprache aus, und klicken Sie auf **Weiter**, um fortzufahren.
- 3.** Lesen Sie die Lizenzvereinbarung. Um die Vereinbarung anzunehmen und fortzufahren, klicken Sie auf **Akzeptieren**.
- 4.** Geben Sie Ihren Abonnementschlüssel ein, und klicken Sie auf **Weiter**, um fortzufahren.



Hinweis: Wenn Sie das Produkt testen möchten, lassen Sie das Feld **Meine Anmeldeschlüssel** leer, und klicken Sie auf **Weiter**. Wählen Sie im Dialogfeld **Testoptionen** den Dienst aus, den Sie testen möchten.

- Wenn Sie das Produkt auf CD in einem Geschäft erworben haben, finden Sie den Abonnementschlüssel auf dem Deckblatt des Installationsleitfadens.
- Wenn Sie das Produkt über den F-Secure eStore bezogen haben, finden Sie den Abonnementschlüssel in Ihrem Benutzerkonto unter dem Punkt "mein Konto" --> "Meine Lizenzen".



Hinweis: Verwenden Sie nur den im Lieferumfang des Produkts enthaltenen Abonnementschlüssel. Sie können den Abonnementschlüssel für die Anzahl von Installationen

verwenden, für die Ihre Lizenz gültig ist (weitere Informationen finden Sie unter 'F-Secure-Lizenz' in diesem Handbuch). Wenden Sie sich an den technischen Support von F-Secure, wenn bei der Registrierung Probleme auftreten.

5. Wählen Sie den Installationstyp:
 - Automatische Installation: Das Produkt wird automatisch gestartet. Bereits vorhandene Sicherheitsprodukte werden möglicherweise automatisch ersetzt. Das Produkt wird im Standardverzeichnis installiert.
 - Schritt-für-Schritt-Installation: Sie können während der Installation verschiedene Auswahlen vornehmen. Sie können beispielsweise das Installationsverzeichnis ändern. Wir empfehlen jedoch, das Standardverzeichnis zu verwenden.
6. Klicken Sie auf **Weiter**.
7. Entfernen Sie die Installations-CD, nachdem die Installation abgeschlossen ist.
8. Der Computer startet automatisch neu. Um sofort neu zu starten, klicken Sie auf **Jetzt neu starten**.
9. Nach dem Neustart versucht das Produkt, eine Internetverbindung herzustellen, um die Anmeldung zu bestätigen und Updates herunterzuladen. Stellen Sie sicher, dass Sie mit dem Internet verbunden sind. Das Herunterladen dieser großen Updates kann einige Zeit in Anspruch nehmen. Sobald die Updates heruntergeladen wurden, ist der Schutz auf dem neuesten Stand. Die aktuellen Updates gewährleisten den besten Schutz.



Tipp: Für weitere Informationen zu diesem Produkt können Sie auf die Online-Hilfe zugreifen, indem Sie im Produkt auf die Taste **Hilfe** klicken. Die Online-Hilfe befindet sich ebenfalls auf der Installations-CD.

Haftungsausschluss

"F-Secure" und das Dreieckssymbol sind eingetragene Marken der F-Secure Corporation, und F-Secure-Produktnamen und -Symbole/Logos sind entweder Marken oder eingetragene Marken der F-Secure Corporation. Alle in diesem Handbuch erwähnten Produktnamen sind Marken der jeweiligen Unternehmen. F-Secure Corporation verzichtet auf Eigentumsansprüche bezüglich Marken und Namen von Dritten. Die F-Secure Corporation ist äußerst um die Genauigkeit der in diesem Handbuch aufgeführten Informationen bemüht; es wird jedoch keine Haftung für eventuelle Fehler und Auslassungen von Tatbeständen übernommen. Die F-Secure Corporation behält sich das Recht vor, in diesem Handbuch angegebene technische Daten ohne Vorankündigung zu ändern.

Sofern nicht anders angegeben, sind die in Beispielen verwendeten Unternehmen, Namen und Angaben frei erfunden. Ohne ausdrückliche schriftliche Genehmigung der F-Secure Corporation

darf kein Teil dieser Veröffentlichung auf beliebige Weise und mit beliebigen elektronischen oder mechanischen Mitteln für einen beliebigen Zweck reproduziert oder übertragen werden.

Dieses Produkt unterliegt eventuell einem oder mehreren F-Secure-Patenten, einschließlich der folgenden:

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2009 F-Secure Corporation. Alle Rechte vorbehalten.

Kapitel 2

Einstieg

Themen:

- *Was nach dem Installieren zu tun ist*
- *Wie kann ich sicherstellen, dass mein Computer geschützt ist?*
- *Ausführen allgemeiner Aufgaben*
- *Wie erkennt man, was das Produkt geleistet hat?*
- *Was ist das Real Time Protection Network?*


Was nach dem Installieren zu tun ist

Nachdem Sie das Produkt installiert haben, müssen Sie möglicherweise Ihren E-Mail-Client und Webbrowser konfigurieren, um mit dem Produkt zu arbeiten

Einrichten meiner E-Mail-Programme zum Spam-Filtern

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

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

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

Wie funktioniert das Zusammenspiel zwischen meinen eigenen Filterregeln und den E-Mail-Filterregeln?

Das E-Mail-Filtern filtert E-Mail-Nachrichten auf Grundlage eigener Filterregeln. Es filtert keine E-Mail-Nachrichten, die einer von Ihnen erstellten Regel entsprechen. Wenn Sie beispielsweise eine Regel erstellt haben, die alle E-Mail-Nachrichten von einem Webstore in den Webstore-Ordner filtert, werden sowohl Ihre Nachrichten bezüglich Auftragsbestätigungen als auch Werbematerial aus diesem Webstore aus Ihrem Posteingang entfernt und in den Webstore-Ordner verschoben.

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

Browsingprofile erstellen

Mithilfe von Profilen können Sie sicherstellen, dass kleinere Kinder und Teenager im Internet nur solche Webseiten besuchen können, die keine gesperrten oder unerwünschten Inhalte besitzen.

Wenn Sie ein Browsingprofil erstellen, müssen Sie ein Passwort festlegen. Beachten Sie beim Erstellen von Passwörtern Folgendes:

- Wählen Sie ein Passwort, das leicht zu merken, aber schwer zu erraten ist.
- Ein Passwort kann beliebige Zeichen enthalten.
- Ein Passwort muss aus 3 bis 80 Zeichen bestehen.
- Je nachdem, wie Ihr Produkt eingerichtet ist, muss Ihr Passwort eventuell eine bestimmte Zeichenanzahl übersteigen.

So erstellen Sie ein Browsingprofil:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Klicken Sie auf **Browsingprofile bearbeiten**.
Das Dialogfeld **Browsingprofil-Assistent der Kindersicherung** wird geöffnet.
4. Wählen Sie aus, ob Sie ein Browsingprofil für kleinere Kinder oder für Teenager oder beides erstellen möchten, und klicken Sie auf **Weiter**.

Sie haben die Browsingprofile erfolgreich erstellt.

Wenn Sie das Browsingprofil für kleinere Kinder erstellt haben, wird beim nächsten Öffnen Ihres Browsers die **Startseite der Kindersicherung** geöffnet. Die Liste der zugelassenen Websites auf der **Startseite der Kindersicherung** ist noch leer, nachdem Sie die Browsingprofile erstellt haben. Als Nächstes können Sie Websites und Seiten hinzufügen, auf die Ihre Kinder zugreifen dürfen.





Wie kann ich sicherstellen, dass mein Computer geschützt ist?




Sie können das Statussymbol in Ihrer Taskleiste und den Produktstatus auf der Seite **Status** überprüfen, um sicherzustellen, dass Ihr Computer geschützt ist.

Was zeigt das Systemleistungssymbol an?

Setzen Sie den Mauszeiger auf das Produktstatus-Symbol auf Ihrer Windows Systemleiste, um eine Kurzinfo anzusehen, die den aktuellen Produktstatus anzeigt.

Status-Symbole und deren Bedeutung:

Symbol	Status	Vorgehensweise
	Das Produkt funktioniert einwandfrei. Ihr Computer ist geschützt.	Sie können Ihren Computer normal verwenden.
	Ein Produktdownload wird gerade durchgeführt und Ihr Computer ist geschützt, sobald der Download abgeschlossen ist.	Das Produkt führt einen Download durch und installiert die neuesten Updates. Warten Sie, bis der Download abgeschlossen ist.
	Ein Fehler ist aufgetreten und Ihr Computer ist nicht vollständig geschützt.	Setzen Sie den Mauszeiger auf das Status-Symbol, um die Ursache des Fehlers anzuzeigen. Starten Sie Ihren Computer gegebenenfalls neu.
	Warnung: Eine Funktion des Produktes ist abgeschaltet oder das Produkt ist nicht auf dem neuesten Stand. Ihr Computer ist nicht vollständig geschützt.	Setzen Sie den Mauszeiger auf das Status-Symbol, um die Kurzinfo zum Status einzusehen. Schalten Sie die zurzeit abgeschaltete Funktion ein oder überprüfen Sie die Produkt-Updates.

Symbol Status	Vorgehensweise
	 Hinweis: Sie sehen möglicherweise dieses Symbol, wenn Sie z.B. Ihre Festplatte defragmentieren, da einige Systemfunktionen dazu führen können, dass Downloads unterbrochen werden.
 Das Produkt wurde entfernt und Ihr Computer ist nicht geschützt.	Klicken Sie mit der rechten Maustaste auf das Status-Symbol und wählen Sie Erneut laden , um das Produkt zu aktivieren.
 Das Elternprofil ist aktiv.	Sie haben uneingeschränkten Internetzugang.
Kein Symbol Das Produkt ist nicht installiert oder ein Fehler hat den Start des Produktes verhindert.	Starten Sie Ihren Computer neu. Falls das Symbol nicht angezeigt wird, installieren Sie das Produkt neu.

Ansicht meines allgemeinen Schutzstatus




Auf der Seite **Status** finden Sie einen kurzen Überblick über die installierten Produktfunktionen und deren aktuellen Status.




So öffnen Sie die Seite **Status**:

Klicken Sie auf der Startseite auf **Status**.

Die Seite **Status** wird geöffnet.

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

Status-Symbol	Statusbezeichnung	Beschreibung
	OK	Ihr Computer ist geschützt. Die Funktion ist aktiviert und funktioniert ordnungsgemäß.
	Informationen	Das Produkt informiert Sie über den besonderen Status einer Funktion. Das Symbol wird beispielsweise bei der Aktualisierung einer Funktion angezeigt.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Zum Beispiel können die Virendefinitionen veraltet sein, der Status einer Funktion erfordert Ihr Eingreifen oder die Firewall ist so konfiguriert, dass sämtlicher

Status-Symbol	Statusbezeichnung	Beschreibung
		Internetverkehr blockiert wird.
	Fehler	Ihr Computer ist nicht geschützt. In diesem Fall ist zum Beispiel Ihr Abonnement abgelaufen, Ihre Firewall wurde so konfiguriert, dass sämtlicher Datenverkehr blockiert wird, eine wichtige Funktion ist deaktiviert oder das Produkt weist einen Fehlerstatus auf.
	Aus	Eine nicht kritische Funktion ist deaktiviert.

Woher weiß ich, ob mein Abonnement gültig ist?

Der Typ und der Status Ihrer Anmeldung werden auf der Seite **Statistiken** angezeigt.

Wenn das Abonnement bald abläuft oder wenn Ihr Abonnement abgelaufen ist, ändert sich der allgemeine Schutzstatus des Produktes auf der Hauptseite, und das Datum, an dem das Abonnement ablaufen wird, wird Ihnen angezeigt.

So prüfen Sie die Gültigkeit Ihrer Anmeldung:

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

Der Status und das Ablaufdatum Ihres Abonnements werden auf der Seite **Statistiken** angezeigt. Wenn Ihr Abonnement abgelaufen ist, müssen Sie Ihr Abonnement erneuern, um weiterhin Aktualisierungen erhalten und das Produkt nutzen zu können.



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

Ausführen allgemeiner Aufgaben

Auf der Seite **Aufgaben** erfahren Sie mehr zur Verwendung des Produkts. Dort können Sie auch allgemeine Aufgaben ausführen.

So öffnen Sie die Seite **Aufgaben**:


Klicken Sie auf der Startseite auf **Aufgaben**.

Die Seite **Aufgaben** wird geöffnet.


Öffnen des Produktes

Durch einen Doppelklick auf das Produktstatus-Symbol auf Ihrer Windows Systemleiste öffnen Sie das Produkt.

So öffnen Sie das Produkt:

1. Wählen Sie eine der folgenden Optionen:
 - Bei Windows XP oder Vista: Klicken Sie auf das Symbol **Ausgeblendete Symbole einblenden**, um die Systemleistensymbole anzuzeigen.
 - Bei Windows 7: Klicken Sie auf den Textcursor, um die Systemleistensymbole anzuzeigen.
2. Doppelklicken Sie Sie auf das Symbol .

Die Hauptansicht öffnet sich und zeigt den aktuellen Schutzstatus.

 **Tipp:** Sie können das Produkt und die Hilfe auch im Windows-Menü **Start** öffnen oder mit dem Desktop-Symbol des Produktes.

Erweiterte Einstellungen öffnen

Bearbeiten Sie die erweiterten Einstellungen, um die Arbeitsweise des Produktes zu ändern.

Zum Öffnen der erweiterten Einstellungen

Klicken Sie auf der Startseite auf **Einstellungen**.

Das Fenster **Einstellungen** wird geöffnet.

Das linke Fenster listet Produktkomponenten gegliedert nach ihrer Funktion auf. Sie können die Produkteinstellungen im rechten Fenster ändern.

Verwendung von Verknüpfungen

Sie können im Windows Explorer Dateien und Ordner scannen und verschiedenste Aufgaben über das Menü der Taskleistensymbole ausführen.

Im Windows Explorer scannen

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

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


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

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

Aufgaben von der Systemleiste aus ausführen

Über das Produktstatussymbol in der Windows-Systemleiste lassen sich die häufigsten Aufgaben schnell ausführen.

So werden die Aufgaben ausgeführt:


1. Wählen Sie eine der folgenden Optionen:
 - Bei Windows XP oder Vista: Klicken Sie auf das Symbol **Ausgeblendete Symbole einblenden**, um die Systemleistensymbole anzuzeigen.
 - Bei Windows 7: Klicken Sie auf den Textcursor, um die Systemleistensymbole anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf das Symbol . Ein Menü mit den häufigsten Aufgaben wird geöffnet.
3. Wählen Sie die auszuführende Aufgabe im Menü aus.

Allgemeine Aufgaben:

Option	Wirkung
Öffnen	Öffnet die Benutzeroberfläche des Produkts, über die Sie den Status aller Produktkomponenten anzeigen und auf Produkteinstellungen zugreifen können, um die Schutzstufe zu ändern.
History der Benachrichtigungsfenster anzeigen	Zeigt eine Liste aller Informationsmeldungen des Produkts an. Diese Liste enthält zum Beispiel: <ul style="list-style-type: none"> • Systemkontroleignisse • Scanereignisse für Internetdatenverkehr • Artikel zu Service-News • Geplante Scanereignisse

Aufgaben im untergeordneten Menü zum Entladen:

Option	Wirkung
Entladen und mit dem aktuellen Stufe der Firewall fortfahren	Entlädt installierte Komponenten aus dem Speicher Ihres Computers. Firewallregeln werden verwendet und schützen Ihren Computer vor böswilligen Verbindungsversuchen. Das Entladen kann z. B. notwendig sein, wenn Sie bestimmte Online-Spiele spielen

Option	Wirkung
Entladen und gesamten Netzwerkverkehr zulassen	<p>oder andere Produkte installieren.</p> <p>Hiermit können Sie komplette Produkt aus dem Speicher Ihres Computers entfernen und den vollständigen Netzwerkdatenverkehr durchlassen. Alle Sicherheitsfunktionen sind währenddessen deaktiviert und Ihr Computer ist nicht geschützt.</p> <p> Hinweis: Verwenden Sie diese Option nur dann, wenn Ihr Computer nicht mit dem Internet verbunden ist.</p>

Aufgaben beim Virus- und Spyware-Scan

Option	Wirkung
Ziel scannen	Scannt eine bestimmte Datei oder einen Ordner in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Riskware</i> . Wählen Sie das Zielverzeichnis oder die Datei aus und klicken Sie auf OK , um den Scanvorgang zu starten.
Festplatten scannen	Scannt alle Dateien auf Ihren Festplatten in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Riskware</i> .
Schneller Malware-Scan	Scannt das System in Bezug auf <i>Malware</i> und <i>Riskware</i> .
Schneller Rootkit-Scan	Scannt das System in Bezug auf <i>Rootkits</i> und andere verdächtige und <i>versteckte Elemente</i> .
Computer vollständig überprüfen	Scannt den Computer in Bezug auf <i>Viren</i> , <i>Spyware</i> und <i>Rootkits</i> .

Aufgaben im untergeordneten Menü Netzwerkverbindungen:

Option	Wirkung
Gesamten Datenverkehr blockieren	Blockiert den gesamten Netzwerkdatenverkehr. Diese Option sollte nur verwendet werden, wenn Sie den Verdacht haben, dass Ihr Computer über das Netzwerk angegriffen wird.
Gesamten Datenverkehr zulassen	Lässt den gesamten Netzwerkdatenverkehr passieren. Diese Option deaktiviert die gesamte Firewall und macht den Computer ungeschützt gegenüber Netzwerkangriffen.
Alert Log anzeigen	Öffnet das Dialogfeld Firewall Alerts .

Aufgaben im untergeordneten Menü E-Mail-Filter:

Option	Wirkung
Absender zulassen	Öffnet ein Dialogfeld, in dem Sie Adressen von E-Mail-Absendern zur Liste "Zugelassene Absender" hinzufügen können. Die Liste der zugelassenen Absender enthält Adressen, die niemals durch den Spamordner gefiltert werden.
Absender filtern	Öffnet ein Dialogfeld, in dem Sie Adressen von E-Mail-Absendern zur Liste "Gesperrte Absender" hinzufügen können. Die Liste der gesperrten Absender enthält Adressen, die durch den Spamordner gefiltert werden.
E-Mail-Filterung konfigurieren	Öffnet die Einstellungen zur E-Mail-Filterung.

Aufgaben im untergeordneten Menü "Kindersicherung":

Option	Wirkung
Kindersicherung aktivieren	Aktiviert die Kindersicherung. Diese Option wird nur angezeigt,

Option	Wirkung
Erwachsener	wenn die Kindersicherung deaktiviert ist. Aktiviert das Profil für Erwachsene, nachdem Sie das Passwort für Erwachsene eingegeben und auf OK geklickt haben.
Jugendlicher	Aktiviert das Teenagerprofil, nachdem Sie das Teenagerpasswort eingegeben und auf OK geklickt haben.
Kleines Kind	Aktiviert das Kinderprofil.
Webseiten-Liste wird angezeigt	Öffnet die Website-Liste der Kindersicherung, auf der Sie zugelassene und gesperrte Webseiten hinzufügen können.

Untergeordnetes Menü "Info":

Option	Wirkung
Info	Zeigt Produktinformationen wie z. B. die Versionsnummer an.

Mein Abonnement erneuern

Wenn Ihr Abonnement bald abläuft, können Sie es online verlängern.

So verlängern Sie Ihr Abonnement:


1. Klicken Sie auf der Startseite auf **Aufgaben**.
2. Klicken Sie auf **Mein Abonnement**.
3. Wählen Sie **Online verlängern**.




Hinweis: Je nach Abonnementtyp ist diese Option möglicherweise nicht verfügbar.

Es wird eine Website geöffnet, auf der Sie Ihr Abonnement verlängern können. Befolgen Sie die Anweisungen auf dieser Seite.

4. Wenn Sie Ihren neuen Abonnementschlüssel erhalten haben, klicken Sie auf **Neuen Abonnementschlüssel eingeben**.
5. Geben Sie im sich öffnenden Dialogfeld Ihren neuen Abonnementschlüssel ein und klicken Sie auf **Registrieren**.

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

Öffnen Sie, nachdem Sie Ihren neuen Abonnementschlüssel eingegeben haben, die Seite **Statistiken**, um das neue Gültigkeitsdatum des Abonnements einzusehen.


 **Hinweis:** Wenn Ihr Abonnement abgelaufen ist, können Sie ein neues Abonnement kaufen und Ihren Abonnementschlüssel auf der Hauptseite des Produktes ändern.

Vollversion des Produkts kaufen

Wenn Sie eine Testversion des Produkts nutzen, können Sie die Vollversion online kaufen.

So kaufen Sie eine Vollversion:

1. Klicken Sie auf der Startseite auf **Aufgaben**.
2. Klicken Sie auf **Mein Abonnement**.
3. Wählen Sie **Online kaufen**.
Es wird eine Website geöffnet, auf der Sie eine Vollversion des Produkts kaufen können. Befolgen Sie die Anweisungen auf der Seite.
4. Wenn Sie den Abonnementschlüssel für die Vollversion des Produkts erhalten haben, wählen Sie **Neuen Abonnementschlüssel eingeben**.
5. Geben Sie im sich öffnenden Dialogfeld Ihren neuen Abonnementschlüssel ein, und klicken Sie auf **Registrieren**.

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

Wie erkennt man, was das Produkt geleistet hat?

Die Seite **Statistiken** zeigt an, was das Produkt geleistet hat. Sie können Funktionen, die das Produkt ausgeführt hat, um Ihren Computer zu schützen, im Benachrichtigungsfenster History ersehen.

Statistiken anzeigen

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

Zum Öffnen der Seite **Statistiken**:

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

Die Seite **Statistiken** öffnet sich.

- Unter **Letzte erfolgreiche Update-Überprüfung** können Sie einsehen, wann das letzte Update erfolgt ist.
- **Abonnement gültig bis** zeigt an, wann Ihr aktuelles Abonnement abläuft.
- Unter **Viren- und Spyware-Scanning** wird angezeigt, wie viele Dateien vom Produkt gescannt wurden und wie viele infizierte Dateien seit der Installation gefunden wurden.
- **Programme** zeigt an wie viele Programme DeepGuard seit dem Installieren erlaubt oder geblockt hat.
- Unter **E-Mail-Scanning** wird die Anzahl der gültigen E-Mail-Anhänge und die Anzahl der Anhänge angezeigt, die vom Produkt bereinigt wurden.
- Unter **E-Mail-Filterung** können Sie einsehen, wie viele E-Mails das Produkt als gültige E-Mail-Nachrichten und als Spam-Nachrichten identifiziert hat.

Was sind Benachrichtigungsfenster?

Benachrichtigungsfenster sind kurze Benachrichtigungen, die in der unteren rechten Ecke Ihres Computerbildschirms angezeigt werden.

Die Benachrichtigungsfenster informieren Sie über das, was das Produkt unternommen hat, um Ihren Computer zu schützen. Das Produkt informiert Sie beispielsweise mit Benachrichtigungsfenstern, wenn es ein möglicherweise schädliches Programm vom Start abhält. Diese Benachrichtigungsfenster dienen der Information. Ihrerseits ist keine Aktion erforderlich.

Was ist das Real Time Protection Network?

Das Realtime Protection Network von F-Secure ist ein Online-Service, der schnelle Hilfe gegen Bedrohungen aus dem Internet bietet.

Das Realtime Protection Network verwendet Zuverlässigkeitsdienste, um Informationen zu den neuesten Bedrohungen aus dem Internet einzuholen. Sie können uns bei der Entwicklung dieses Service helfen, indem Sie uns detaillierte Informationen zukommen lassen, etwa die Quellen aggressiver Programme oder Nachrichten sowie Verhaltens- und statistische Analysen zur Nutzung von Computer und Internet.

Wenn das Kontrollkästchen **Ja, ich möchte am Realtime Protection Network teilnehmen** auf der Registerkarte **Datenschutz** ausgewählt ist, werden diese Informationen an das Realtime Protection Network übermittelt.

Die Übermittlung von Informationen an das Realtime Protection Network stellt keine Gefährdung für den Datenschutz dar. Wenn Sie mehr über die Verarbeitung der übermittelten Informationen erfahren möchten, lesen Sie unsere Datenschutzerklärung. Klicken Sie hierzu auf **Lesen Sie unsere Datenschutzerklärung**.

Datenschutzerklärung

Die Übermittlung von Daten über das Realtime Protection Network stellt keine Gefährdung für den Datenschutz dar.

Obwohl die übermittelten Daten gemäß einiger Rechtsprechungen möglicherweise als persönlich angesehen werden, werden Ihre Daten während des Prozesses geschützt. Wir sorgen für eine sichere Übertragung der Daten, entfernen nicht erforderliche persönliche Angaben und verarbeiten die Daten anonym in einem aggregierten Format. So können die Angaben nicht mit Ihrer Person in Verbindung gebracht werden. Über das Realtime Protection Network werden keine Informationen zu Benutzerkonto, IP-Adresse oder Lizenz übermittelt. Die Verschlüsselung der Daten bei der Übertragung sorgt für einen zusätzlichen Schutz.

Die übermittelten Daten werden dazu genutzt, die Möglichkeiten des Schutzes, die von unseren Dienstleistungen und Produkten ausgehen, zu verbessern.

Meinen Computer vor Malware schützen

Themen:

- *Was sind Viren und Malware?*
- *Wie scanne ich meinen Computer?*
- *Was ist DeepGuard?*
- *Wie verwende ich die Quarantäne?*
- *Verwendung automatischer Updates*

Wenn Malware entdeckt wird, wird sie standardmäßig sofort deaktiviert, bevor sie Schaden anrichten kann.

Beim Viren- und Spyware-Scannen werden standardmäßig Ihre lokalen Festplatten, Wechseldatenträger (wie tragbare Festplatten oder Compact-Disks) sowie heruntergeladene Inhalte automatisch überprüft. Abhängig von Ihrer Produktkonfiguration werden auch alle E-Mails und der Webdatenverkehr gescannt. Beim Viren- und Spyware-Scannen wird Ihr Computer auch auf alle Veränderungen hin überwacht, die auf *Malware* hindeuten. Wenn gefährliche Systemveränderungen, zum Beispiel an Systemeinstellungen oder Versuche zur Veränderung wichtiger Systemprozesse entdeckt werden, verhindert DeepGuard die Ausführung dieses Programms, da es sich vermutlich um *Malware* handelt.

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 Daten sammeln.

Spyware kann persönliche Daten sammeln, wie:

- Internet-Websites, die Sie besucht haben,
- E-Mail-Adressen auf Ihrem Computer,

- Passwörter oder
- Kreditkartennummern.

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

Rootkits

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

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

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

Riskware

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

Riskware ist keine Malware im eigentlichen Sinne. Riskware-Programme führen mitunter nützliche Funktionen aus, die jedoch potenziell gefährlich sind.

Beispiele für Riskware-Programme sind:

- Programme für Instant Messaging, etwa IRC (Internet Relay Chat),
- Programme zur Übertragung von Dateien über das Internet von einem Computer auf einen anderen,
- oder Programme für die Internet-Telefonie, etwa VoIP (*Voice over Internet Protocol*).
- Software für den Remote-Zugriff, etwa VNC,
- Scareware, mit der Einzelpersonen durch Betrug oder Panikmache zum Kauf von falscher Sicherheitssoftware verleitet werden oder
- Software, mit denen die Prüfung oder der Kopierschutz von CDs umgangen wird.

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

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

Wie scanne ich meinen Computer?

Sie können Ihren Computer in Echtzeit scannen lassen oder manuelle oder zeitlich geplante Scans durchführen lassen.

Die anzuwendende Methode richtet sich nach der Leistungsstärke Ihres Computers und der gewünschten Höhe der Schutzstufe. Bei einem älteren Computer kann es zu deutlichen Leistungseinbußen kommen, wenn Sie sämtliche Funktionen zum Virus- und Spyware-Scannen aktivieren.

Auf Malware scannen

Das Scannen in Echtzeit schützt Ihren Computer, indem alle Dateien überprüft werden, sobald auf sie zugegriffen wird, und indem der Zugriff auf die Dateien blockiert wird, die *Malware* enthalten.

Das Scannen in Echtzeit funktioniert wie folgt:

1. Ihr Computer versucht, auf eine Datei zuzugreifen.
2. Die Datei wird sofort auf *Malware* überprüft, bevor dem Computer der Zugriff auf die Datei gestattet wird.
3. Wenn in einer Datei *Malware* entdeckt wird, entfernt das Echtzeit-Scannen die *Malware* automatisch, bevor sie Ihren Computer beschädigen kann.

Beeinflusst das Echtzeit-Scannen 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:

- Komprimierte Dateien, wie *.zip*-Dateien. Denken Sie daran, dass diese Dateien standardmäßig nicht gescannt werden.
- Dateien auf Wechseldatenträgern wie CDs, DVDs und tragbaren USB-Laufwerken.

Das Scannen in Echtzeit kann Ihren Computer verlangsamen, wenn:

- Sie haben einen älteren Computer oder

- Sie greifen gleichzeitig auf eine große Zahl von Dateien zu. Sie öffnen z. B. ein Verzeichnis, das viele Dateien enthält, im Windows Explorer.

Echtzeit-Scanning ein- oder ausschalten

Schalten Sie das Echtzeit-Scanning ein, um *Malware* zu stoppen, bevor sie Ihren Computer beschädigt.

So schalten Sie das Echtzeit-Scanning ein:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer ► Viren- und Spyware-Scan**.
3. Wählen Sie **Echtzeit-Scanning einschalten**.
4. Klicken Sie auf **OK**.

Meine E-mail auf Malware scannen

Das E-Mail-Scanning schützt Sie davor, *Viren* per E-Mail zu erhalten oder zu senden.

Das E-Mail-Scanning schützt Ihren Computer vor:

- Erhalt eines *Virus*, der sich in einer Datei befindet, die als E-Mail-Anhang an Sie gesendet wird,
- versehentliches Senden eines *Virus* an jemand anderen, wenn Sie eine E-Mail mit einer angehängten Datei versenden.

Wann werden E-Mail-Nachrichten und Anhänge gescannt?


E-Mail-Nachrichten und -Anhänge werden jedes Mal gescannt, wenn Ihr E-Mail-Programm E-Mail-Nachrichten an den Mail-Server sendet bzw. von ihm empfängt.

Beim E-Mail-Scannen werden folgende E-Mail-Nachrichten gescannt:


- E-Mail-Nachrichten, die über E-Mail-Programme wie Microsoft Outlook, Microsoft Outlook Express, Microsoft Mail oder Mozilla Thunderbird gesendet und empfangen werden, die als Programme unabhängig von Ihrem Webbrowser ausgeführt werden.

Beim E-Mail-Scannen werden folgende E-Mail-Nachrichten nicht gescannt:

- E-Mails in Webmail, einschließlich E-Mail-Anwendungen, die in Ihrem Webbrowser ausgeführt werden, wie Hotmail, Yahoo! mail oder Gmail.

 **Hinweis:** Sie müssen sicherstellen, dass die für die verschiedenen E-Mail-Protokolle (POP3, IMAP4, SMTP) verwendeten Ports ordnungsgemäß eingerichtet sind. E-Mail-Nachrichten, die über andere Ports empfangen und versendet werden, werden nicht gescannt.

Sie sind auch dann vor *Viren* geschützt, wenn die Ports nicht vorschriftsmäßig eingerichtet sind oder Sie Webmail verwenden. Wenn Sie den E-Mail-Anhang öffnen, erkennt das Echtzeit-Scanning, dass er einen Virus enthält, und blockiert den Virus, bevor er Schaden anrichten kann.

 **Hinweis:** Das Echtzeit-Scanning schützt nur Ihren Computer, nicht Ihre Freunde. Der Virus wird nur erkannt, wenn Sie den Dateianhang öffnen. Wenn Sie den Dateianhang nicht öffnen, wissen Sie nicht, ob die E-Mail einen *Virus* enthält und so einfach eine infizierte E-Mail an Ihre Freunde weitergeleitet werden kann.

Ausschalten des E-Mail-Scannings

Das E-Mail-Scanning lässt sich in den Einstellungen für das Echtzeit-Scanning ein- oder ausschalten.

So schalten Sie das E-Mail-Scanning ein oder aus:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer** ► **Viren- und Spyware-Scan**.
3. Wählen Sie eine der folgenden Optionen:
 - Um das E-Mail-Scanning einzuschalten, wählen Sie **E-Mails auf Viren scannen und Viren entfernen** aus.
 - Um das E-Mail-Scanning auszuschalten, deaktivieren Sie **E-Mails auf Viren scannen und Viren entfernen**.

Je nachdem, was Sie gewählt haben, ist das E-Mail-Scanning jetzt ein- oder ausgeschaltet.

Festlegen der Ports für verschiedene E-Mail-Protokolle

Wenn Ihr E-Mail-Programm keinen Standardport verwendet, müssen Sie den Port verwenden, der auf E-Mail-*Viren* überprüft wurde. Anderenfalls werden diese E-Mail-Nachrichten nicht nach *Viren* gescannt.

So legen Sie die Ports fest:

1. Starten Sie Ihre E-Mail-Anwendung und prüfen Sie, welche Ports für das Senden und Empfangen von E-Mails verwendet werden. Notieren Sie die Portnummern.
2. Öffnen Sie das Produkt.
3. Klicken Sie auf der Startseite auf **Einstellungen**.
4. Wählen Sie **Computer ► Viren- und Spyware-Scan**.
5. Klicken Sie neben **E-Mails auf Viren scannen und Viren entfernen auf Protokolle**.
6. Geben Sie die Portnummern ein, die für die einzelnen E-Mail-Protokolle verwendet werden, *POP3* , *IMAP4* oder *SMTP* .
7. Klicken Sie auf **OK**.

Web-Datenverkehr-Scanning einschalten

Scannen Sie Informationen, die Ihren Browser durchlaufen, auf *Viren*, damit Ihr Computer beim Surfen im Internet vor Viren geschützt ist.

So schalten Sie das Web-Datenverkehr-Scanning ein:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer ► Viren- und Spyware-Scan**.
3. Wählen Sie **Web-Datenverkehr auf Viren scannen und Viren entfernen** .
4. Klicken Sie auf **OK**.
5. Wenn Ihr Browser beim Ändern der Einstellung geöffnet war, müssen Sie den Browser neu starten, damit Änderung der Einstellung wirksam wird.

Beim Herunterladen einer Datei mit bösartigem oder verdächtigem Inhalt wird die Datei zwar heruntergeladen, der gefährliche Inhalt wird jedoch durch Nullen ersetzt.

Tracking Cookies blockieren

Durch das Blockieren von Tracking Cookies verhindern Sie, dass Websites verfolgen, welche Sites Sie im Internet besuchen.

Tracking Cookies sind kleine Dateien, mit denen Websites aufzeichnen, welche Websites Sie besuchen. So blockieren Sie die Installation von Tracking Cookies:

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

2. Wählen Sie **Computer** ► **Viren- und Spyware-Scan**.
3. Wählen Sie **Tracking Cookies blockieren**.
4. Klicken Sie auf **OK**.

Zu festgelegten Zeiten scannen

Sie können Ihren Computer in regelmäßigen Abständen auf *Malware* überprüfen lassen, etwa täglich, wöchentlich oder monatlich.

Das Scannen nach *Malware* ist ein intensiver Prozess. Er beansprucht die volle Leistung Ihres Computers und nimmt geraume Zeit in Anspruch. Aus diesem Grund können Sie festlegen, dass das Programm Ihren Computer dann scannt, wenn Sie ihn nicht benutzen.

Planen von Scans

Sie können festlegen, dass das Programm den Computer in regelmäßigen Abständen scannt, beispielsweise wöchentlich, täglich oder monatlich.

So planen Sie einen Scan:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer** ► **Geplanter Scan**.
3. Wählen Sie **Geplantes Scanning einschalten**.
4. Wählen Sie die Tage aus, an denen nach *Viren* und *Spyware* gescannt werden soll.

Option	Beschreibung
Täglich	Um jeden Tag zu scannen.
Wöchentlich	Um an ausgewählten Wochentagen zu scannen. Wählen Sie rechts in der Liste die Tage aus, an denen gescannt werden soll.
Monatlich	So scannen Sie an bis zu drei Tagen pro Monat. Wählen Sie die Tage aus: <ol style="list-style-type: none">1. Wählen Sie eine Option für "Tag" aus.2. Wählen Sie in der Liste neben dem ausgewählten Tag den Tag des Monats aus.3. Wiederholen Sie diesen Schritt, wenn Sie an einem anderen Tag scannen möchten.

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

Option	Beschreibung
Startzeit	Der Zeitpunkt, an dem das Scannen gestartet wird. Wählen Sie einen Zeitpunkt aus, zu dem Sie den Computer voraussichtlich nicht verwenden.
Nachdem der Computer nicht benutzt wurde für	Wählen Sie eine Inaktivitätszeit aus, nach der mit dem Scannen begonnen werden soll, wenn der Computer nicht verwendet wird.

Geplanten Scan abbrechen

Wenn Sie Ihren Computer beim Start eines geplanten Scans weiterverwenden möchten, kann es sein, dass Sie den geplanten Scan abbrechen möchten.

Geplante Scans können einen sich deutlich auf die Leistung Ihres Computers auswirken. So brechen Sie den geplanten Scan ab:

1. Klicken Sie auf den Link **Geplanter Scan wurde gestartet** im Benachrichtigungsfenster **Viren- und Spyware-Scan**.
Das Benachrichtigungsfenster bleibt ca. 15 Sekunden lang geöffnet und verschwindet dann wieder. Wenn Sie den Link im Benachrichtigungsfenster nicht anklicken, können Sie den geplanten Scanvorgang nicht mehr abbrechen.
2. Klicken Sie auf den Link **Abbrechen** im Fenster **Viren- und Spyware-Scan**.
3. Klicken Sie auf den Link **Schließen** aus.

Der geplante Scan wurde abgebrochen. Der nächste geplante Scan wird wie gewohnt ausgeführt.

Ergebnisse geplanter Scans anzeigen

Sobald ein geplanter Scan fertiggestellt ist, können Sie überprüfen, ob *Malware* gefunden wurde.

So überprüfen Sie die Ergebnisse eines geplanten Scans:

1. Klicken Sie auf **Geplanter Scan fertiggestellt** im Benachrichtigungsfenster **Viren- und Spyware-Scan**.

2. Klicken Sie auf **Bericht anzeigen** , um anzuzeigen, was während des Scanvorgangs passiert ist.



Hinweis: Wenn Sie das Dialogfeld über das Dialogfeld **Historie des Fensters** öffnen, ist die Schaltfläche **Bericht anzeigen** deaktiviert. Sie können die Ergebnisse früherer geplanter Scans nicht anzeigen.

3. Klicken Sie auf **Schließen** , um das Dialogfeld zu schließen.

Manuell scannen


Sie können Ihren Computer manuell scannen, wenn Sie den Verdacht haben, dass sich *Malware* auf Ihrem Computer befindet.

Art des manuellen Scans auswählen

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

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

So starten Sie das Scannen Ihres Computers manuell:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das Symbol  in der Taskleiste von Windows.

Wenn Sie das Symbol nicht finden können, ist es möglicherweise ausgeblendet. Klicken Sie zum Einblenden ausgeblendeter Symbole

in der Taskleiste auf das Symbol .

2. Wählen Sie **Viren- und Spyware-Scan** .
3. Wählen Sie den Scan-Typ.

Der **Scan-Assistent** wird geöffnet.

Scantypen

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

Dies sind die verschiedenen Scantypen:

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
Vollständiger Scan	Ihr gesamter Computer (interne und externe Festplatten) auf Viren, Spyware und Riskware	Wenn Sie absolut sicher sein wollen, dass keine Malware oder Riskware auf Ihrem Computer ist. Diese Art des Scannens dauert am längsten. Sie kombiniert den schnellen Malware-Scan und den Festplattenscan. Außerdem sucht sie nach Elementen, die unter Umständen durch ein Rootkit verborgen sind.
Ziel scannen	Eine spezielle Datei, ein spezieller Ordner oder ein spezielles Laufwerk für Viren, Spyware und Riskware	Wenn Sie den Verdacht haben, dass sich an einem bestimmten Speicherort Ihres Computers Malware befindet, weil sich dort Downloads von potenziell gefährlichen Quellen, wie Peer-to-Peer File Sharing-Netzwerken, befinden. Wie lange der Scan dauert, hängt von der Größe des zu scannenden Ziels ab. Der Scan wird beispielsweise schnell abgeschlossen, wenn Sie einen Ordner mit nur ein paar kleinen Dateien scannen.
Festplatten scannen	Alle internen Festplatten auf Ihrem Computer auf Viren, Spyware und Riskware	Dabei werden alle Festplatten des Computers gescannt. Im Gegensatz zum schnellen Malware-Scan werden bei diesem Scantyp nicht nur gezielt die Teile Ihres Systems mit installierten Programmdateien durchsucht, sondern auch alle Datendateien wie Dokumente, Musik, Bilder und Videos. Diese Art des Scannens ist langsam und wird nur dann empfohlen, wenn der schnelle Malware-Scan keine Malware entdeckt hat, Sie aber sicher gehen möchten, dass die

Scantyp	Was wird gescannt?	Wann dieser Typ verwendet werden sollte
		übrigen Teile Ihres Computer keine schädlichen Dateien enthalten.
Schneller Malware-Scan	Teile Ihres Computers auf Viren, Spyware und Riskware	Diese Art des Scannens ist weitaus schneller als ein vollständiger Scan. Es werden nur die Teile Ihres Systems durchsucht, die installierte Programmdateien enthalten. Dieser Scantyp wird empfohlen, wenn Sie rasch überprüfen möchten, ob Ihr Computer sauber ist, da Sie mit dieser Funktion aktive Malware auf Ihrem Computer rasch entdecken können.
Schnelles Rootkit-Scanning	Wichtige Systembereiche, wo verdächtige Elemente zu einem Sicherheitsproblem werden können. Scant nach verborgenen Dateien, Ordnern, Laufwerken oder Prozessen	Wenn Sie vermuten, dass auf Ihrem Computer ein Rootkit installiert ist. Beispielsweise, wenn vor kurzem auf Ihrem Computer Malware entdeckt wurde und Sie sichergehen möchten, dass dabei kein Rootkit installiert wurde.

Malware automatisch bereinigen

Wenn während des Scannens *Malware* gefunden wird, kann das Programm automatisch entscheiden, wie sie von Ihrem Computer entfernt wird. Oder Sie treffen diese Entscheidung für jedes Element selbst.

1. Wählen Sie eine Option aus:

Option

Automatisches Verfahren (empfohlen)

Was passieren soll

Das Programm entscheidet, wie die jeweilige *Malware* behandelt wird, um Ihren Computer automatisch zu bereinigen.

Option

Benutzer entscheidet abhängig vom jeweiligen Element


Was passieren soll

Das Programm fragt Sie bei jedem *Malware* -Element, wie Sie verfahren möchten.

2. Klicken Sie auf **Weiter**.

Ergebnisse manueller Scans anzeigen

Nachdem der Scan abgeschlossen ist, können Sie einen Bericht der Scan-Ergebnisse anzeigen.


-  **Hinweis:** Sie sollten diesen Bericht anzeigen, da es sich bei der von Ihnen ausgewählten Aktion nicht immer um die durchgeführte Aktion handelt. Wenn Sie beispielsweise eine infizierte bereinigen, der *Virus* jedoch nicht aus ihr entfernt werden konnte, kann das Produkt auch eine andere Aktion für die Datei durchgeführt haben.

So zeigen Sie den Bericht an:

1. Klicken Sie auf **Bericht anzeigen**.

Der Bericht enthält:

- Die Anzahl gefundener *Malware*.
- Der Typ der gefundenen *Malware* und Links zu Beschreibungen der *Malware* im Internet.
- Die bei den einzelnen *Malware* -Elementen durchgeführten Aktionen.
- Alle Elemente, die vom Scannen ausgeschlossen wurden.
- Die Scanning Engines, die für die Überprüfung auf *Malware* verwendet wurden.

-  **Hinweis:** Die Anzahl der gescannten Dateien kann unterschiedlich sein, je nachdem, ob Dateien in Archiven in den Scanvorgang einbezogen wurden. Wurden bereits archivierte Dateien gescannt, können sich die Scan-Ergebnisse im Cachespeicher befinden.

2. Klicken Sie auf **Fertig stellen**, um **Scan-Assistent** zu schließen.

Zu prüfende Dateien auswählen

Sie können die Dateitypen und die Bereiche Ihres Computers auswählen, die bei manuellen und geplanten Scans geprüft werden.



Hinweis: Bearbeiten Sie die Einstellungen für das manuelle Scannen, um Dateien und Ordner auszuwählen, die beim geplanten Scan überprüft werden sollen.

Die in Echtzeit auf *Viren* gescannten Dateien werden durch zwei Typen von Listen festgelegt:

- Die Liste der gescannten Dateitypen enthält entweder alle Dateien oder eine definierte Liste mit Dateitypen.
- Mit Listen von Dateien, die vom Scannen ausgeschlossen wurden, werden Ausnahmen hinsichtlich der Liste der gescannten Dateitypen definiert. Dateitypen oder Speicherorte, die sich auf der Liste der ausgeschlossenen Dateien befinden, werden auch dann nicht gescannt, wenn sie sich auf der Liste der gescannten Dateitypen befinden.

Über die Listen der gescannten Dateitypen und der ausgeschlossenen Dateien können Sie auf unterschiedliche Art definieren, welche Teile Ihres Computers gescannt werden:

- Sie können alle Dateien einschließen und dann optional die Ausschlussliste verwenden, um Laufwerke, Verzeichnisse oder Dateien auszuschließen, von denen Sie wissen, dass sie sicher sind, und nicht gescannt werden müssen.
- Sie können eine Liste von Dateitypen definieren, die gescannt werden sollen, damit nur diese Dateitypen gescannt werden.

Einbeziehen von Dateien

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

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer** ► **Manueller Scan**.
3. Weilen Sie unter **Scan-Optionen** eine der folgenden Optionen aus:

**Nur bekannte
Dateitypen scannen
(schneller)**

Um nur die am ehesten infizierten Dateitypen, wie ausführbare Dateien, zu scannen. Diese Option beschleunigt zugleich den Scanvorgang.

**In komprimierten
Dateien scannen (ZIP,
RAR etc.)**

Um Archivdateien und -ordner zu scannen.

**Erweiterte
Heuristiken
verwenden
(langsamer)**

Um alle verfügbaren Heuristiken während des Scans zu verwenden, damit neue oder unbekannte Malware besser gefunden werden kann.



Hinweis: Wenn Sie diese Option auswählen, nimmt das Scanning mehr Zeit in Anspruch und kann zu mehr falschen Positiven führen (harmlose Dateien, die als verdächtig gemeldet werden).

4. Klicken Sie auf **OK**.

Die von Ihnen ausgewählten Optionen unter **Scan-Optionen** legen fest, welche Dateien in künftige manuelle und geplante Scans einbezogen werden.



Hinweis: Die Dateitypen oder -speicherorte in der Ausschlussliste heben die hier definierten Einstellungen auf. Die Dateitypen in der Ausschlussliste werden nicht gescannt, selbst wenn Sie sie hier als zu scannend ausgewählt haben.

Ausschließen bestimmter Dateitypen

Sie können Dateien nach Dateityp von Echtzeit- und manuellen Scans ausschließen.

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Führen Sie einen der folgenden Schritte durch:
 - Wählen Sie **Computer** ► **Viren- und Spyware-Scan**.
 - Wählen Sie **Computer** ► **Manuelles Scanning**.

3. Klicken Sie auf **Ausschlussliste öffnen**.
4. So schließen Sie einen Dateityp aus:
 - a) Wählen Sie die Registerkarte **Dateitypen** aus.
 - b) Wählen Sie **Dateien mit diesen Erweiterungen ausschließen**.
 - c) Geben Sie eine Dateierweiterung, die den Typ der Dateien angibt, die Sie ausschließen möchten, in das Feld neben der Schaltfläche **Hinzufügen** ein.


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

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

Die ausgewählten Dateitypen sind von künftigen Echtzeit- und manuellen Scans ausgeschlossen.

Ausschließen von Dateien nach Speicherort


Sie können eine Liste der Ordner und Laufwerke definieren, die Sie nicht in Echtzeit oder manuell auf *Viren* scannen möchten.

 **Hinweis:** Dateien in Ordnern oder auf Laufwerken, die vom Scanvorgang ausgeschlossen sind, werden auch dann nicht gescannt, wenn ihr Dateityp in der Liste der zu scannenden Dateitypen enthalten ist.

So definieren Sie eine Liste mit Dateien, Ordnern oder Laufwerken für den Ausschluss nach Speicherort:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Führen Sie einen der folgenden Schritte durch:
 - Wählen Sie die Option **Computer** ► **Viren- und Spyware-Scan**.
 - Wählen Sie die Option **Computer** ► **Manuelles Scanning**.

3. Klicken Sie auf **Ausschlussliste öffnen**.
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 Virenskan 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 sind von künftigen Echtzeit- und manuellen Scans ausgeschlossen.

Anzeigen von ausgeschlossenen Anwendungen

Sie können sich die Anwendungen, die Sie aus künftigen Echtzeit-, manuellen und geplanten Scans ausgeschlossen haben, anzeigen lassen, sie aus der Ausschlussliste entfernen und somit in künftige Scans einbeziehen.

So zeigen Sie vom Scanvorgang ausgeschlossene Anwendungen an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Führen Sie einen der folgenden Schritte durch:
 - Wählen Sie **Computer** ► **Viren- und Spyware-Scan**.
 - Wählen Sie **Computer** ► **Manuelles Scanning**.
3. Klicken Sie auf **Ausschlussliste öffnen**.
4. Wählen Sie die Registerkarte **Anwendungen**.

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

5. So stellen Sie ein, dass eine Anwendung bei zukünftigen manuellen oder geplanten Scans einbezogen wird:
 - a) Wählen Sie die Anwendung aus, die erneut in den Scan einbezogen werden soll.
 - b) Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**, um das Dialogfeld **Vom Scanning ausschließen** anzuzeigen.
7. Klicken Sie zum Beenden auf **OK**.

In komprimierten Dateien und Ordnern scannen


Sie können nach *Viren* scannen, die sich in komprimierten Dateien verbergen.

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer** ► **Manueller Scan**.
3. Wenn Sie Archivdateien oder -ordner scannen möchten, etwa *.zip*-Dateien, wählen Sie **In komprimierten Dateien scannen (ZIP, RAR etc.)**.

Bei komprimierten Dateien und Ordnern dauert der Scanvorgang ein wenig länger.
4. Klicken Sie auf **OK**.

Auswählen der durchzuführenden Aktion, wenn ein Virus gefunden wurde

Wenn *Viren* gefunden wurden und Sie keine automatische Bearbeitung von *Viren* durch das Programm festgelegt haben, können Sie jetzt auswählen, ob die Dateien, in denen ein Virus gefunden wurde, bereinigt, gelöscht, unter Quarantäne gestellt oder nur blockiert werden sollen.

 **Hinweis:** Dieser Schritt des **Scan-Assistenten** wird übersprungen, wenn Sie festgelegt haben, dass das Programm *Viren* während eines manuellen oder geplanten Scans immer automatisch behandeln soll, oder wenn Sie festgelegt haben, dass während des Scans gefundene *Malware* automatisch behandelt werden soll.

Eine Liste der infizierten Dateien und der *Viren*, die in diesen Dateien gefunden wurden. So entfernen Sie diese *Viren* von Ihrem Computer:


1. Für weitere Informationen über die *Viren* und deren Gefährlichkeit klicken Sie auf die Links in der Spalte **Infektion**, die zu weiteren Angaben zu den
2. Wählen Sie die Aktion aus, die für infizierte Dateien durchgeführt werden soll.
3. Prüfen Sie die Aktionen, die für die infizierten Dateien ausgewählt sind. Sie können alle Aktionen noch ändern.
4. Klicken Sie auf **Weiter**, um die Aktionen durchzuführen.
5. Klicken Sie auf **Weiter**.

Wenn *Spyware* gefunden wird, macht der **Scan-Assistent** mit dem Schritt zur Bereinigung von *Spyware* weiter.

Bei infizierten Dateien zu ergreifende Aktionen

Das Produkt **Durchzuführende Aktion** wird Ihnen angezeigt, welche Aktionen Sie beim Echtzeit-, manuellen oder geplanten Scannen an den infizierten Dateien vornehmen können.

Die folgenden Aktionen können an infizierten Dateien durchgeführt werden:


 **Hinweis:** Die Infektion wird unter Umständen nicht nur in der Datei, sondern auch in einem Eintrag in der Registrierung oder in einem Prozess entdeckt

Durchzuführende Aktion	Was mit der infizierten Datei passiert
Dateien bereinigen	Wenn möglich, wird der <i>Virus</i> aus der infizierten Datei entfernt. Anschließend können die Dateien sicher verwendet werden
Dateien löschen	Die infizierten Dateien werden gelöscht.
Dateien in Quarantäne stellen	Die infizierten Dateien werden in Quarantäne gestellt, wo sie Ihren Computer nicht beschädigen können. Sie können die Datei später bei Bedarf aus der Quarantäne zurückholen.
Datei nur blockieren	Der Zugriff auf die infizierte Datei ist blockiert.

Standardaktionen beim Echtzeit-scannen

Das Produkt **Standardaktion** wird Ihnen angezeigt, welche Standardaktionen Sie beim Echtzeit-Scannen für infizierte Dateien auswählen können.


Sie können festlegen, dass eine der folgenden Standardaktionen durchgeführt wird, wenn Malware entdeckt wird:



Standardaktion	Was passiert, wenn Malware gefunden wurde
Mich immer fragen	Wenn bei einem manuellen Scan Malware gefunden wird, fragt Sie das Programm, was getan werden soll.  Hinweis: Bei geplanten Scans funktioniert diese Option genauso wie die Option zum Bereinigen von Dateien,
Mich bei Unklarheit fragen	Wenn das Programm die Malware nicht identifizieren kann, fragt es Sie, was damit geschehen soll.

Standardaktionen beim manuellen und geplanten Scannen

Das Produkt **Standardaktion** wird Ihnen angezeigt, welche Standardaktionen Sie im manuellen und geplanten Scannen für infizierte Dateien auswählen können.

Sie können festlegen, dass eine der folgenden Standardaktionen durchgeführt wird, wenn Malware entdeckt wird:

Standardaktion	Was passiert, wenn Malware gefunden wurde
Mich immer fragen	Wenn bei einem manuellen Scan Malware gefunden wird, fragt Sie das Programm, was getan werden soll.  Hinweis: Bei geplanten Scans funktioniert diese Option genauso wie die Option zum Bereinigen von Dateien.
Dateien bereinigen	Das Programm versucht, die Viren in infizierten Dateien, die während eines manuellen oder geplanten Scans entdeckt wurden, automatisch zu bereinigen.Spyware

Standardaktion	Was passiert, wenn Malware gefunden wurde
	<p>und Riskware werden automatisch in Quarantäne gestellt.</p> <p> Hinweis: Nicht immer kann ein Virus in einer Datei bereinigt werden. Wenn dies nicht möglich ist, wird die Datei in Quarantäne gestellt (sofern sie nicht im Netzwerk oder auf Wechseldatenträgern gefunden wurde), damit die Datei Ihren Computer nicht beschädigen kann.</p>
Dateien löschen	Das Programm löscht automatisch alle während eines manuellen oder geplanten Scans gefundenen infizierten Dateien.
Dateien in Quarantäne stellen	Das Programm verschiebt automatisch alle während eines manuellen oder geplanten Scans gefundenen infizierten Dateien in die Quarantäne, wo diese auf dem Computer keinen Schaden anrichten können.
Nur Bericht	<p>Das Programm lässt infizierte Dateien, die während eines manuellen oder geplanten Scans gefunden werden, im bisherigen Zustand und trägt die entdeckte Malware in den Scanbericht ein.</p> <p> Hinweis: Wenn das Echtzeit-Scannen nicht aktiviert ist und Sie diese Option auswählen, kann Malware Ihren Computer beschädigen.</p>

Standardaktionen bei DeepGuard

Das Produkt **Standardaktion** wird Ihnen angezeigt, welche Standardaktionen Sie für DeepGuard auswählen können.

Sie können festlegen, dass eine der folgenden Standardaktionen durchgeführt wird, wenn DeepGuard einen Versuch erkennt, Änderungen am System vorzunehmen.

Standardaktion	Was passiert, wenn Malware gefunden wurde
Mich immer fragen	DeepGuard fragt Sie, ob Sie alle überwachten Aktionen zulassen oder blockieren wollen, selbst wenn die Anwendung als sicher eingestuft wurde.

Standardaktion	Was passiert, wenn Malware gefunden wurde
Mich bei Unklarheit fragen	Nur wenn die Anwendung nicht als sicher oder unsicher eingestuft werden kann, fragt DeepGuard Sie, ob Sie alle überwachten Aktionen zulassen oder blockieren wollen,
Automatisch handhaben	DeepGuard blockiert unsichere Anwendungen und lässt sichere Anwendungen zu, ohne Sie zu fragen.

Viren- und Spyware-Historie

Die Viren- und Spyware-Historie zeigt an, welche Aktionen vom Programm im Hinblick auf gefundene Viren und Spyware durchgeführt wurden.

So rufen Sie die Historie auf:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer ► Viren- und Spyware-Scan**.
3. Klicken Sie auf **Viren- und Spyware-Historie anzeigen** aus.

Die Viren- und Spyware-Historie wird geöffnet.

Was ist DeepGuard?

DeepGuard analysiert den Inhalt von Dateien und das Verhalten von Programmen und blockiert neue und unentdeckte *Viren*, *Würmer* und andere bösartige Programme, die versuchen, schädliche Veränderungen an Ihrem Computer vorzunehmen.

Zu den möglicherweise gefährlichen Systemänderungen gehören:

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

DeepGuard beobachtet permanent solche Veränderungen und überprüft jedes Programm, das versucht, Änderungen am System vorzunehmen.

Wie funktioniert DeepGuard?

Wenn DeepGuard erkennt, dass ein Programm versucht, potenziell schädliche Veränderungen am System vorzunehmen, lässt es die Ausführung des Programms in einer Sicherheitszone zu, sofern Sie das Programm nicht ausdrücklich zugelassen oder blockiert haben.

In der Sicherheitszone kann das Programm Ihrem Computer keinen Schaden zufügen. DeepGuard analysiert, welche Veränderungen das Programm vornehmen wollte und entscheidet aufgrund dessen, wie wahrscheinlich es ist, dass es sich bei dem Programm um *Malware* handelt.

DeepGuard übernimmt entweder die automatische Zulassung oder Blockierung des Programms oder fragt Sie, ob das Programm zugelassen oder blockiert werden soll. Dies hängt von folgenden Faktoren ab:

- wie wahrscheinlich es ist, dass das Programm *Malware* ist, und
- Welche Aktion DeepGuard nach Ihren Vorgaben durchführen soll, wenn es einen möglicherweise bösartigen Versuch entdeckt, Änderungen am System vorzunehmen.

Einschalten von DeepGuard

Wenn DeepGuard aktiviert ist, können verdächtige Programme daran gehindert werden, an Ihrem Computer schädliche Systemänderungen vorzunehmen.

Wenn Sie Windows XP haben, stellen Sie vor dem Einschalten von DeepGuard sicher, dass Sie Service Pack 2 installiert haben.

So schalten Sie DeepGuard ein:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer ► DeepGuard**.
3. Wählen Sie **DeepGuard einschalten**.
4. Klicken Sie auf **OK**.

Programme zulassen, die von DeepGuard blockiert wurden

Sie können einem Programm, das von DeepGuard blockiert wurde, erlauben Systemänderungen vorzunehmen.

Es kann vorkommen, dass DeepGuard das Ausführen eines sicheren Programms verhindert, auch wenn Sie das Programm verwenden möchten und wissen, dass es sicher ist. Die passiert, weil das Programm versucht, Systemänderungen durchzuführen, die potenziell schädlich sein können. Es ist auch möglich, dass Sie ein Programm unabsichtlich blockiert haben, als ein DeepGuard Pop-up-Fenster eingeblendet wurde. Sie können ein blockiertes Programm zulassen, indem Sie seine Berechtigung in der Liste der Anwendungen ändern.

So lassen Sie ein Programm zu, das von DeepGuard blockiert wurde:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer ► DeepGuard**.
3. Klicken Sie neben Echtzeit-Scanning auf **Offene Liste der überwachten Programme**.
Die Liste der Anwendungen wird angezeigt.
4. Klicken Sie auf die Spalte **Berechtigung**, damit die Liste nach zugelassenen und abgelehnten Programmen sortiert wird.
5. Wählen Sie das Programm aus, das Sie zulassen möchten, und klicken Sie auf **Details**.
6. Wählen Sie unter **Berechtigung** die Option **Zulassen**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Schließen**.

Das von Ihnen gewählte Programm kann jetzt ausgeführt werden und darf Systemänderungen vornehmen.

So schalten Sie die erweiterte Prozessüberwachung aus

Zu Ihrer maximalen Sicherheit ändert DeepGuard Programme vorübergehend während deren Ausführung.

Infolge dieser erweiterten Prozessüberwachung funktionieren gewisse Programme wie Online-Spiele und Anti-Cheating Tools möglicherweise nicht. Dies ist bei Programmen der Fall, die ihre eigene Integrität prüfen. Anti-Cheating-Tools setzen in der Regel Integritätsprüfungen ein, um herauszufinden, ob sie dahingehend geändert wurden, dass sie Anderes ausführen als das, wozu sie entwickelt wurden.

So schalten sie die erweiterte Prozessüberwachung aus:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Computer** ► **DeepGuard**.
3. Schalten Sie **Erweiterte Prozessüberwachung verwenden** aus.
4. Klicken Sie auf **OK** aus.

Schutz gegen schädliche Systemänderungen

Entdeckt DeepGuard ein Programm, das möglicherweise schädliche Systemänderungen vorzunehmen versucht, und es kann nicht ermitteln, ob das Programm sicher oder unsicher ist, wird ein Dialogfeld zu einem **Systemänderungsversuch** angezeigt.

Das Dialogfeld "Systemänderungsversuch" wird angezeigt, wenn Sie eine der folgenden Aktionen ausgewählt haben, die DeepGuard beim Erkennen eines möglicherweise schädlichen Systemänderungsversuchs durchführen soll:

- **Immer nachfragen** oder
- **Wenn unklar, nachfragen**.

DeepGuard zeigt das Dialogfeld möglicherweise an, wenn Sie gerade Software installieren.

So entscheiden Sie, ob das Programm, das versucht, Systemänderungen durchzuführen, vertrauenswürdig ist:

1. Wenn Sie unsicher sind, aus welcher Quelle der Änderungsversuch stammt, klicken Sie auf **Details >>**, damit weitere Informationen über das Programm angezeigt werden.

Im Bereich der technischen Details sehen Sie:

- den Namen des Programms, das die Änderung durchführen möchte,
- den Speicherort des Programms,
- die Änderung, die das Programm durchführen möchte und
- eine *Risikobewertung*, die angibt, wie hoch die Wahrscheinlichkeit ist, dass es sich bei dem Programm um *Malware* handelt:
 - eine niedrige Bewertung weist auf ein Programm hin, das wahrscheinlich unbedenklich ist
 - eine hohe Risikobewertung weist auf ein Programm hin, bei dem es sich wahrscheinlich um *Malware* handelt.,

2. Wählen Sie eine der folgenden Optionen aus:

Wählen Sie...

Wenn Sie...

Ich vertraue der Anwendung.
Fortfahren zulassen.

denken, dass das Programm sicher ist. Das Programm ist wahrscheinlich sicher, wenn:

- es eine geringe *Risikobewertung* hat,
- das Dialogfeld aufgrund einer von Ihnen durchgeführten Aktion angezeigt wurde
- Sie das Programm erkennen oder
- Sie das Programm von einer sicheren Quelle erhalten haben.

Ich vertraue der Anwendung nicht.
Diesen Vorgang blockieren.

befürchten, dass das Programm unsicher ist. Das Programm ist wahrscheinlich unsicher, wenn:

- es eine hohe *Risikobewertung* hat,
- Sie das Programm nicht kennen oder
- Sie das Programm kennen und es für verdächtig halten.

3. Wählen Sie **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen**, wenn Sie möchten, dass DeepGuard Ihre Entscheidung für dieses Programm bei künftigen Systemänderungsversuchen durch das Programm anwendet. Diese Option wird nur angezeigt, wenn Sie **Immer nachfragen** als Aktion für Systemänderungsversuche ausgewählt haben. Wenn DeepGuard dasselbe Programm das nächste Mal entdeckt, fragt es Sie nicht, wie Sie vorgehen möchten, sondern wendet Ihre letzte Entscheidung an.
4. Wenn Sie eine Probe eines Programms senden möchten, das versucht hat, Systemänderungen durchzuführen, gehen Sie wie folgt vor:
- Klicken Sie auf **Eine Probe senden...**
Ein Dialogfeld wird geöffnet, das die Einreichungsbedingungen erläutert.
 - Lesen Sie die Bedingungen sorgfältig durch, und klicken Sie auf **Akzeptieren**, wenn Sie damit einverstanden sind und die Probe einreichen möchten.

Sie möchten eventuell eine Probe senden:

- wenn DeepGuard ein Programm automatisch blockiert, von dem Sie wissen, dass es sicher ist oder
- wenn ein Dialogfeld zu einem **Systemänderungsversuch** angezeigt wird und Sie den Verdacht haben, dass es sich bei dem Programm um *Malware* handeln könnte.

Das System sendet der F-Secure Corporation eine elektronische Kopie des Programms, das als mögliche Sicherheitsbedrohung erkannt wurde.

Anzeigen des von DeepGuard durchgeführten Vorgangs

Wenn DeepGuard automatisch ein Programm daran hindert, Systemänderungen vorzunehmen, wird ein kleines Benachrichtigungsfenster angezeigt.

Benachrichtigungsfenster sind kurze Benachrichtigungen, die in der unteren rechten Ecke Ihres Computerbildschirms angezeigt werden. Sie werden beispielsweise dann eingeblendet, wenn DeepGuard die Verwendung eines Programms verweigert hat. Diese Benachrichtigungsfenster dienen der Information, es ist keine Aktion Ihrerseits erforderlich. Im Verlauf der Benachrichtigungsfenster werden alle Benachrichtigungsfenster angezeigt.

Wenn ein Programm, das Sie zu installieren oder auszuführen versuchen, nicht funktioniert, kann das daran liegen, dass DeepGuard dieses Programm daran hindert, Systemänderungen vorzunehmen. In diesem Fall können Sie sich von DeepGuard ein kleines Benachrichtigungsfenster anzeigen lassen, wenn DeepGuard automatisch ein Programm blockiert. So wissen Sie, warum das Programm nicht richtig funktioniert hat.

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.

Sie können *Malware*, *Spyware* und *Riskware* unter Quarantäne stellen und sie so unschädlich machen. Sie können Anwendungen oder Dateien zu einem späteren Zeitpunkt aus der Quarantäne entlassen, wenn Sie sie benötigen.

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

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

Unter Quarantäne gestellte Elemente anzeigen

Sie können weitere Informationen zu Elementen unter Quarantäne anzeigen.

So zeigen Sie detaillierte Informationen zu Elementen unter Quarantäne an:

1. Klicken Sie auf der Startseite auf **Aufgaben**.
2. Klicken Sie auf der Seite **Aufgaben** auf **Eine entfernte Datei oder ein entferntes Programm wiederherstellen**. Das Dialogfeld **Quarantäne** wird geöffnet.

3. Durchsuchen Sie die Kategorien *Virus*, *Spyware* und *Riskware*, um alle unter Quarantäne gestellten Elemente anzuzeigen.
 - In der Liste der unter Quarantäne gestellten Elemente (*Viren*) werden der Name des isolierten Elements sowie der Installationspfad der Datei angezeigt. Hat das unter Quarantäne gestellte Element mehrere Dateien installiert, erfolgt die Anzeige in der Liste wie folgt: *Systeminfektion*.
 - Die Liste der unter Quarantäne gestellten *Spyware* zeigt den *Spyware* -Typ und eine Liste von Anwendungen an, bei denen bekannt ist, dass sie *Spyware* enthalten.
 - Die Liste der unter Quarantäne gestellten *Riskware* zeigt den Dateipfad und den Namen der Elemente an.
4. Um weitere Informationen zu dem unter Quarantäne gestellten Element anzuzeigen, sind folgende Optionen verfügbar:
 -

Klicken Sie auf die Registerkarte



Icon neben dem Quarantäne-Element.

- Klicken Sie auf **Eigenschaften**, um zusätzliche Informationen zu dem Element unter Quarantäne anzuzeigen.
5. Um das unter Quarantäne stehende Element zu löschen, wählen Sie es aus und klicken auf **Löschen**.

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.

1. Klicken Sie auf der Startseite auf **Aufgaben**.
2. Wählen Sie in der Liste **Aufgaben**-Liste auf **Dateien wiederherstellen**. Das Dialogfeld **Quarantäne** wird geöffnet.

3. Durchsuchen Sie die Quarantänekategorien und wählen Sie das Element aus, das Sie wiederherstellen möchten. Sie können mehrere Elemente auswählen, die wiederhergestellt werden sollen.



Hinweis: Beachten Sie beim Auswählen von Dateien, dass die Namen der Dateien als Verknüpfung zur Beschreibung des Elements in der Online-Datenbank dienen.

4. Klicken Sie auf **Wiederherstellen**.
Das Produkt stellt das ausgewählte Element am Originalspeicherort auf der Festplatte wieder her und entfernt das Element aus der Quarantäneliste.

Verwendung automatischer Updates

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

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

Den Update-Status überprüfen

Datum und Uhrzeit der letzten Aktualisierung anzeigen.

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

So prüfen Sie, ob Sie die neuesten Updates besitzen:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Sonstige Einstellungen** ► **Automatische Updates**.
3. **Letzte Update-Prüfung** zeigt den Zeitpunkt des letzten Updates an.
4. Klicken Sie auf **Jetzt prüfen**.
Das Produkt stellt eine Verbindung mit dem Internet her und sucht nach den neuesten Updates. Falls der Schutz nicht aktuell ist, ruft es die neuesten Updates ab.



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

Meine Internetverbindungseinstellungen ändern



Sie können konfigurieren, wie Ihr Computer eine Verbindung mit dem Internet herstellt, um Updates automatisch zu empfangen.

So ändern Sie Ihre Internetverbindungseinstellungen:



Hinweis: Normalerweise ist es nicht erforderlich, die Standardeinstellungen zu ändern.

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Sonstige Einstellungen** ► **Verbindung**.

3. Wählen Sie in der Liste **Internetverbindung** aus, wie Ihr Computer mit dem Internet verbunden ist.
 - Wählen Sie **Ständige Verbindung voraussetzen**, wenn Sie eine permanente Netzwerkverbindung haben.
 -  **Hinweis:** Falls Ihr Computer keine ständige Netzwerkverbindung besitzt und bei Bedarf eine DFÜ-Verbindung herstellt, kann die Option **Ständige Verbindung voraussetzen** zu mehreren Einwahlversuchen führen.
 - Wählen Sie **Verbindung erkennen**, um Updates nur dann abzurufen, wenn das Produkt eine aktive Netzwerkverbindung erkennt.
 - Wählen Sie **Datenverkehr erkennen**, um Updates nur dann abzurufen, wenn das Produkt anderen Netzwerkverkehr erkennt.
 -  **Tipp:** Falls Sie eine ungewöhnliche Hardwarekonfiguration besitzen, die dafür sorgt, dass mit der Einstellung **Verbindung erkennen** auch dann eine aktive Netzwerkverbindung erkannt wird, wenn keine vorhanden ist, wählen Sie stattdessen **Datenverkehr erkennen**.

4. Wählen Sie in der Liste **HTTP-Proxy** aus, ob Ihr Computer für die Internetverbindung einen *Proxy-Server* verwendet.
 - Wählen Sie **Kein HTTP-Proxy** aus, wenn Ihr Computer direkt mit dem Internet verbunden ist.
 - Wählen Sie **HTTP-Proxy manuell konfigurieren** aus, um die *HTTP-Proxy*-Einstellungen zu konfigurieren.
 - Wählen Sie **HTTP-Proxy des Browsers verwenden** aus, um die *HTTP-Proxy*-Einstellungen zu verwenden, die in Ihrem Browser konfiguriert sind.

Netzwerkverbindungen sichern

Themen:

- *Was ist eine Firewall?*
- *Datenverkehr im Netzwerk durch die Firewall zulassen oder blockieren*
- *So kontrollieren Sie Netzwerkanwendungen*
- *So wehren Sie Eindringlinge ab*
- *So steuern Sie DFÜ-Verbindungen*
- *Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?*

Das Produkt

- Schützt Sie vor Eindringlingen, die versuchen, ohne Ihre Genehmigung auf Ihren Computer zuzugreifen. Diese können z. B. versuchen, Ihre persönlichen Daten zu stehlen - Dateien, Passwörter oder Kreditkartennummern.
- Blockiert schädlichen Internetdatenverkehr wie *Trojaner*. Diese können z. B. Dateien auf Ihrem Computer zerstören, Ihren Computer zum Absturz bringen oder *Ports* öffnen, damit Hacker auf Ihren Computer zugreifen können.
- Blockiert schädlichen Internetdatenverkehr wie *Spyware*. *Spyware* kann z. B. Informationen über Ihre E-Mail-Adressen, Passwörter oder Kreditkartennummern abrufen.
- Verhindert, dass bösartige *Dialer*programme Ihre Modem- oder ISDN-Verbindung verwenden, um kostenpflichtige Telefonnummern mit hohen Minutenpreisen anzuzahlen.

Sobald das Produkt installiert ist, werden Ihre Netzwerkverbindungen automatisch geschützt.

Was ist eine Firewall?

Die *Firewall* schützt Ihren Computer, indem Sie sicheren Internetdatenverkehr passieren lässt und unsicheren Datenverkehr blockiert.

In der Regel lässt die *Firewall* den Datenverkehr von Ihrem Computer in das Internet zu, blockiert aber den gesamten Datenverkehr aus dem Internet auf Ihren Computer, sofern Sie diesen nicht ausdrücklich zulassen. Indem eingehender Datenverkehr blockiert wird, verhindert die *Firewall*, dass *schädliche Software*, z. B. *Würmer*, auf Ihren Computer gelangen oder dass Eindringlinge auf Ihren Computer zugreifen können. Je nach den gewählten Einstellungen werden Popup-Fenster mit *Alarmmeldungen* zu den jeweiligen Aktionen der *Firewall* angezeigt.

Ihr Computer wird durch die vordefinierten *Firewalleinstellungen* geschützt. Diese brauchen Sie in der Regel nicht anzupassen. Unter Umständen müssen Sie jedoch die Einstellungen verändern, wenn Sie ein sehr strenges *Firewallprofil* verwenden oder wenn Sie Ihre eigenen *Firewallregeln* oder -dienste hinzugefügt haben.



Vorsicht: Schalten Sie *Firewall* nicht ab. Wenn Sie dies tun, ist Ihr Computer allen Netzwerkangriffen ungeschützt ausgeliefert. Wenn ein Programm auf Ihrem Computer nicht mehr funktioniert, da es keine Verbindung zum Internet herstellen kann, ändern Sie *Firewallregeln* bzw. die Einstellungen für die Anwendungssteuerung, anstatt *Firewall* abzuschalten.

Was sind Firewallprofile?

Im *Firewallprofil* wird die Sicherheitsstufe auf Ihrem Computer festgelegt.

Jedes *Firewallprofil* enthält eine vordefinierte Gruppe von *Firewallregeln*, die wiederum festlegen, welche Art von Datenverkehr von Ihrem Computer zugelassen oder abgewiesen wird. Einigen Profilen können Sie auch selbst erstellte Regeln hinzufügen.

Außerdem definieren Firewallprofile

- wenn Internetverbindungen automatisch für alle Anwendungen zugelassen sind oder
- wenn Sie jeden Verbindungsversuch in einem Popup-Fenster der Anwendungssteuerung separat zulassen oder ablehnen können.

Es gibt mehrere vordefinierte *Firewallprofile*, von sehr strengen bis zu sehr lockeren:

- Ein sehr strenges *Firewallprofil* (**Alle blockieren**) blockiert in der Regel den meisten Netzwerkdatenverkehr. Dies kann dazu führen, dass Sie einige auf Ihrem Computer installierten Programme nicht verwenden können.
- Ein mittleres Profil (**Normal**) lässt in der Regel den gesamten von Ihrem Computer ausgehenden Datenverkehr ins Internet zu. Die mittlere Stufe lehnt eventuell Das mittlere Profil weist unter Umständen einige eingehende Dienste ab und generiert *Alarmer* für diese.
- Ein sehr lockeres Profil (**Alle zulassen**) lässt in der Regel den gesamten Netzwerkdatenverkehr zu, eingehenden wie ausgehenden, und erzeugt keine *Alarmmeldungen*. Da bei diesem Profil Ihr Computer nicht geschützt ist, sollten Sie es nur in Ausnahmefällen einsetzen.



Hinweis: Abhängig vom verwendeten Produkt können sich die Namen der Firewallprofile unterscheiden.

Ihre Computer ist durch das vordefinierte *Firewallprofil* geschützt. B. Ihren Laptop außerhalb Ihres Hauses verwenden und das Internet über eine *WLAN*-Verbindung öffnen.

Sie können eigene *Firewallprofile* definieren und diesen wiederum eigene Regelgruppen hinzufügen. Allerdings sollten nur erfahrene Benutzer eigene Firewallprofile erstellen.

In welchem Verhältnis stehen Firewallprofile zu Firewallregeln und -diensten?

Ein *Firewallprofil* besteht aus mehreren *Firewallregeln*. Eine *Firewallregel* umfasst verschiedene *Firewalldienste*. Dienste werden durch die *Protokolle* und *Ports* definiert, die sie verwenden.

Die Sicherheitsstufe **Mobil** besitzt eine Regel namens **Websuche**. Diese Regel erlaubt die Suche im Web. Die Regel enthält die Dienste, die für die Suche im Web erforderlich sind, wie den Dienst **HyperText Transfer Protocol (HTTP)**. Dieser Service verwendet *TCP* und *Port* Nummer 80.

Firewallprofil ändern

Wenn Sie die Schutzebene auf Ihrem Computer ändern möchten, müssen Sie das *Firewallprofil* ändern.

So ändern Sie das *Firewallprofil* :

1. Klicken Sie auf der Startseite auf **Status**.
2. Klicken Sie neben **Firewall** auf den Link, der das aktuelle Firewallprofil zeigt.
Das Dialogfeld **Firewallprofil ändern** wird geöffnet.
3. Lesen Sie die Beschreibungen des *Firewallprofils* sorgfältig durch.
4. Wählen Sie das geeignete Profil aus der Liste aus, und klicken Sie auf **OK**.

Auf der Seite **Status** wird nun das neue *Firewall-Profil* angezeigt. Die *Firewall-Regeln* und die Einstellungen der Anwendungssteuerung ändern sich entsprechend dem ausgewählten *Firewall-Profil*.

Was sind Firewallregeln und -dienste?

In Firewallregeln und -diensten wird definiert, wie die Firewall Ihre Netzwerkverbindungen schützt.

Was sind Firewallregeln?

Firewallregeln definieren, welche Art von Internetdatenverkehr zugelassen oder blockiert ist.

Zu jedem *Firewallprofil* gehört eine vordefinierte Gruppe von *Firewallregeln*, die nicht geändert werden können. Sie können lediglich bei einigen der Profile neue Regeln hinzufügen. Bei einigen Profilen können Sie keine eigenen Regeln hinzufügen. Unter Umständen ist auch ein Profil ohne vordefinierte Regeln vorhanden, dem Sie Ihre eigene Regelgruppe hinzufügen können. Vom ausgewählten Firewallprofil hängt auch ab, welche Priorität Ihre eigenen Regeln in Bezug auf die vordefinierten Regeln erhalten.

Eine *Firewall-Regel* kann auf Datenverkehr aus dem Internet auf Ihren Computer (eingehend) oder von Ihrem Computer in das Internet (ausgehend) angewendet werden. Eine Regel kann auch auf beide Richtungen gleichzeitig angewendet werden.

Eine *Firewallregel* enthält *Firewall dienste*, die den Typ des Datenverkehrs und die *Ports* festlegen, die dieser Typ von Datenverkehr verwendet. Eine Regel namens **Websuche** verwendet z. B. einen Dienst namens **HTTP**, der TCP und den *Port* Nummer 80 verwendet.

Durch *Firewallregeln* wird außerdem definiert, ob Popup-Fenster mit *Alarmmeldungen* der Firewall angezeigt werden, in denen Sie über den Datenverkehr, der die *Firewallregeln* erfüllt, informiert werden.

Wann muss eine neue *Firewallregel* hinzugefügt werden?

Möglicherweise müssen Sie eine neue Firewallregel hinzufügen, wenn Sie mit der Verwendung eines neuen Programms beginnen oder ein neues Gerät an Ihren Computer anschließen, wie z. B. ein WLAN-Gerät oder eine IP-Kamera.

Indem alle Dienste, die das Programm oder das Gerät benötigt, zu derselben Regel hinzugefügt werden, ist es einfach:

- die Regel später ein- oder ausschalten oder
- die Regel entfernen, wenn das Programm deinstalliert oder das Gerät entfernt wird.

Sie müssen außerdem eine neue Regel hinzufügen, wenn Sie einen bestimmten Datenverkehrstyp abgelehnt haben, diesen aber für bestimmte IP-Adressen zulassen möchten. In diesem Fall besitzen Sie bereits eine allgemeine *Firewallregel*, die den Datenverkehr ablehnt. Um den Datenverkehr für bestimmte IP-Adressen zuzulassen, müssen Sie eine etwas spezifischere Zulassungsregel erstellen.

Wenn die allgemeine Regel z. B. den gesamten ausgehenden *FTP*-Datenverkehr ablehnt, dann möchten Sie möglicherweise den *FTP*-Datenverkehr zur Website Ihres Internet Service Providers dennoch zulassen, um Ihre Webseiten aktualisieren zu können. Dies erreichen Sie, indem Sie eine spezifischere Regel hinzufügen, die den *FTP*-Datenverkehr zur

IP-Adresse Ihres Internet Service Providers zulässt, und indem Sie dieser Regel eine höhere Priorität zuweisen als die der allgemeinen Ablehnungsregel.

Firewallregeln anzeigen




Sie können die gerade aktiven *Firewallregeln* anzeigen, um herauszufinden, wie die *Firewall* den Datenverkehr auf Ihrem Computer zulässt oder blockiert.

Jedes *Firewallprofil* hat seinen eigenen Satz aktiver *Firewallregeln*. So zeigen Sie die Regeln an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Wählen Sie neben **Aktuelles Firewallprofil** das gewünschte Firewallprofil aus.

Sie können eine Regelliste anzeigen, die folgende Informationen enthält:

Feld	Beschreibung
Wird benutzt	Wenn das Kontrollkästchen aktiviert ist, ist die Regel aktuell aktiv. Wenn das Kontrollkästchen leer ist, ist die Regel aktuell deaktiviert.
Name	Name der Regel. Es gibt zwei Typen von Regeln: <ul style="list-style-type: none"> • Vordefinierte Regeln: Diese Regeln werden grau dargestellt. Sie wurden für das derzeit ausgewählte <i>Firewallprofil</i> vordefiniert. • Ihre eigenen Regeln: Wenn Sie Ihre eigenen Regeln hinzugefügt haben, werden diese über der Zeile Ihre Regeln werden hier hinzugefügt in Schwarz dargestellt.

Feld	Beschreibung
Typ	Regeltyp: <ul style="list-style-type: none"> •  : Diese Regel lässt den Datenverkehr zu. •  : Diese Regel lehnt den Datenverkehr ab. •  : Diese Regel generiert Alarme im Alarmprotokoll und zeigt möglicherweise ein Alarm-Popup an, wenn die Regel Netzwerkdatenverkehr zulässt oder ablehnt.
Remote-Host	<i>IP-Adressen</i> und Netzwerke, für die die Regel gilt. Wenn die Regel für alle <i>IP-Adressen</i> gilt, enthält dieses Feld einen der folgenden Werte: <ul style="list-style-type: none"> • 0.0.0.0/0, ::/0: Die Regel gilt für alle <i>IPv4</i>- und <i>IPv6</i>-Adressen. • 0.0.0.0/0: Die Regel gilt für alle <i>IPv4</i>-Adressen. • ::/0: Die Regel gilt für alle <i>IPv6</i>-Adressen.

5. Um die Einzelheiten einer Regel anzuzeigen, wählen Sie in der Liste eine Regel aus und klicken Sie auf **Details**.
- Wenn die Regel vordefiniert wurde, wird das Dialogfeld **Regeldetails** geöffnet, auf dem die vordefinierte Regel angezeigt wird. Klicken Sie auf **Beenden**, nachdem Sie die Details gelesen haben.
 - Wenn Sie die Regel selbst hinzugefügt haben, wird das Dialogfeld **Regeldetails** geöffnet. Klicken Sie auf **Weiter >**, bis das Dialogfeld mit der Zusammenfassung der Regel angezeigt wird. Klicken Sie auf **Abbrechen**, nachdem Sie die Details gelesen haben.

Einzelheiten der Firewallregeln

Zu den Einzelheiten der *Firewallregel* gehören der Name und der Typ der Regel, die *IP-Adressen* und Dienste, für die die Regel gilt, sowie die Alarmeinstellungen.

Das Dialogfeld **Einzelheiten der Regel** enthält folgende Informationen:

Feld	Beschreibung
Name	Name der Regel.
Typ	Typ der Regel, der definiert, ob die Regel den Netzwerkdatenverkehr zulässt oder ablehnt.
Remote-Adresse	<p><i>IP-Adressen</i> und Netzwerke, für die die Regel gilt. Wenn die Regel für alle <i>IP-Adressen</i> gilt, enthält das Feld einen der folgenden Werte:</p> <ul style="list-style-type: none"> • 0.0.0.0/0, ::/0: Die Regel gilt für alle <i>IPv4</i>- und <i>IPv6</i>-Adressen. • 0.0.0.0/0: Die Regel gilt für alle <i>IPv4</i>-Adressen. • ::/0: Die Regel gilt für alle <i>IPv6</i>-Adressen.
Dienste	<p>Die Spalte Dienst enthält die <i>Firewalldienste</i>, die in der Regel enthalten sind.</p> <p>Die Spalte Richtung zeigt an, ob die Regel für eingehende Dienste (ein), ausgehende Dienste (aus) oder für beide gilt.</p>
Alarmausgabe	Zeigt, ob die Regel Alarmmeldungen generiert und Alarm-Popups einblendet.
Alarmtext	Wenn die Regel Alarme generiert, ist dies der Alarmtext, der im Alarmprotokoll sowie im Popup-Fenster angezeigt wird.

Was sind Firewalldienste?

Firewalldienste definieren den Typ des Datenverkehrs, für den eine *Firewallregel* gilt.

Netzwerkdienste, wie Websuche, *Dateifreigabe* oder *Remote-Konsolen-Zugriff*, sind Beispiele für *Firewalldienste*.

Ein Dienst verwendet ein bestimmtes *Protokoll* und einen bestimmten *Port*. Der HTTP-Dienst verwendet z. B. das *TCP-Protokoll* und den *Port* Nummer 80.

Ein *Firewalldienst* verwendet zwei Arten von *Ports*:

- *Ausgangspartei-Port*: der *Port* auf dem Computer, der die Verbindung initiiert.
- *Antwortpartei-Port*: der *Port* auf dem Computer, bei dem die Verbindung ankommt.

Ob es sich bei dem *Port* auf Ihrem eigenen Computer um einen *Ausgangspartei-Port* oder um einen *Antwortpartei-Port* handelt, hängt von der Richtung des Datenverkehrs ab:

- Wenn der *Firewalldienst* für ausgehenden Datenverkehr zuständig ist, dann ist der *Ausgangspartei-Port* der *Port* auf Ihrem Computer. Der *Antwortpartei-Port* ist dann der *Port* auf einem Remote-Computer.
- Wenn der *Firewalldienst* für eingehenden Datenverkehr zuständig ist, ist der *Ausgangspartei-Port* der *Port* auf einem Remote-Computer. Der *Antwortpartei-Port* ist dann der *Port* auf Ihrem eigenen Computer.

Die *Antwortpartei-Ports* werden in der Regel in der *Softwaredokumentation* angegeben. *Ausgangspartei-Port* kann in der Regel jeder *Port* über 1023 sein. Für einige Spiele müssen Sie jedoch gegebenenfalls bestimmte *Ausgangspartei-Ports* definieren. In diesem Fall werden auch diese in der *Softwaredokumentation* angegeben.

Wenn Sie eine neue *Firewallregel* erstellen, stehen Ihnen einige vordefinierte Dienste zur Verfügung, die Sie zu Ihrer Regel hinzufügen können. Sie können auch eigene Dienste erstellen und hinzufügen, falls Sie den benötigten Dienst nicht in der *Dienstliste* finden.

Firewalldienste anzeigen

Die vorhandenen *Firewalldienste* können Sie auf der Registerkarte **Dienste** anzeigen.

So zeigen Sie die Dienste an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Dienste**.
Folgende Informationen sind verfügbar:

Feld	Beschreibung
Name	Name des Dienstes.
Verwendet in Regel	Name der Firewallregel und wo der Dienst verwendet wird.

- Um die Details eines Dienstes anzuzeigen, wählen Sie den Dienst in der Liste aus, und klicken Sie auf **Details**.
Das Dialogfeld **Dienstdetails** wird geöffnet.
- Klicken Sie nach der Ansicht der Dienstdetails auf **Schließen**.

Was sind dynamische *Firewallregeln*?

Dynamische *Firewallregeln* werden für Verbindungen von Remote-Computern zu Serverprogrammen auf Ihrem Computer erstellt.

Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird und Sie dort eine eingehende Verbindung zulassen - z. B. zu einem Peer-to-Peer-Serverprogramm auf Ihrem Computer -, erstellt die *Firewall* eine temporäre, dynamische *Firewallregel*. Diese Regel wird auf der Registerkarte **Aktivität** zur Liste der dynamischen Regeln hinzugefügt. Die Regel öffnet einen *Port* für dieses Programm und hält diesen so lange geöffnet, wie das Programm an diesem *Port* auf eingehende Verbindungen wartet.

Wenn das Programm den *Port* nicht mehr überwacht, greift die Option *Regel schließt den Port*, und die dynamische Regel wird aus der Liste der dynamischen Regeln entfernt. Abhängig von den Einstellungen für die Je nach den gewählten Einstellungen werden die Popup-Fenster zur Anwendungssteuerung nicht bei allen Programmen angezeigt. Wenn das Popup-Fenster nicht angezeigt wird, wird die dynamische Firewall-Regel automatisch für dieses Programm erstellt.

Dynamische *Firewallregeln* anzeigen

Die Registerkarte **Aktivität** zeigt die dynamischen *Firewallregeln* an, die gerade aktiv sind.

Dynamische *Firewallregeln* werden für Verbindungen von Remote-Computern zu *Serverprogrammen* auf Ihrem Computer erstellt.

So zeigen Sie die dynamischen Firewallregeln an:

- Klicken Sie auf der Startseite auf **Einstellungen**.
- Wählen Sie **Netzwerkverbindung ► Firewall**.
- Klicken Sie auf die Registerkarte **Aktivität**.

Folgende Informationen sind verfügbar:

- **Anwendung:** Der Dateiname des *Server*programms auf Ihrem Computer, das gerade einen *Port* auf eingehende Verbindungen überwacht.
- **Abhörport:** Der *Port*, den die dynamische *Firewallregel* geöffnet hat. Das *Server*programm überwacht diesen *Port* auf eingehende Verbindungen.
- **Remote-Adresse:** Das *Server*programm überwacht den *Port* auf Verbindungen für folgende *IP-Adressen*:
 - **0.0.0.0/0** : Alle *IPv4* - Adressen.
 - **::/0** : Alle *IPv6*- Adressen.

Wie funktioniert die Prioritätenreihenfolge der Firewallregeln?

Firewallregeln haben eine Prioritätsreihenfolge, die festlegt, in welcher Reihenfolge die Regeln auf den Netzwerkdatenverkehr angewendet werden.

Firewallregeln werden auf der Registerkarte **Regeln** als Liste angezeigt. Die *Regeln* werden von oben nach unten angewendet, wobei die erste Regel, die mit dem Datenverkehr übereinstimmt, alle nachfolgenden Regeln überschreibt. Das Hauptprinzip besteht darin, nur den erforderlichen Datenverkehr zuzulassen und den Rest zu blockieren. Daher ist die letzte Regel einer *Firewallprofil* die Regel **Alles andere sperren**. Diese blockiert den gesamten Datenverkehr, den die vor ihr stehenden Regeln nicht explizit zugelassen haben.

Dynamische *Firewallregeln* werden in einer separaten Liste auf der Registerkarte **Aktivität** angezeigt. Die Priorität der dynamischen Regeln ist niedriger als die Priorität der normalen *Firewallregeln*. Dies bedeutet, dass eine dynamische Regel einen bestimmten Datenverkehr nicht zulassen kann, wenn eine *Firewallregel* diesen ablehnt. Die Priorität der dynamischen Regeln ist jedoch höher als die Priorität der vordefinierten Regel **Alles andere sperren**.

Ein Beispiel für die Funktionsweise der Prioritätenreihenfolge

- Sie haben eine Regel hinzugefügt, die den gesamten ausgehenden *FTP*-Datenverkehr ablehnt. In der Regelliste fügen Sie vor dieser

Regel eine andere Regel hinzu, die eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers zulässt. Durch diese Regel ist es möglich, eine *FTP*-Verbindung mit dieser IP-Adresse herzustellen.

- Sie haben eine Regel hinzugefügt, die eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers zulässt. Vor dieser Regel fügen Sie in der Regelliste eine Regel hinzu, die den gesamten *FTP*-Datenverkehr ablehnt. Diese Regel verhindert, dass eine *FTP*-Verbindung zur IP-Adresse Ihres Internet Service Providers hergestellt werden kann (oder zu einer beliebigen anderen IP-Adresse).

Datenverkehr im Netzwerk durch die Firewall zulassen oder blockieren

Sie können Datenverkehr im Netzwerk mit Hilfe von Firewallregeln zulassen oder blockieren.

Was tun, wenn ein Firewall-Alarm angezeigt wird?

Ein Popup-Fenster mit einem Firewall-Alarm wird auf Ihrem Computerbildschirm angezeigt, wenn die *Firewall* verdächtigen Netzdatenverkehr auf Ihrem Computer erkennt.

Ein Popup wird angezeigt, wenn:

- der Datenverkehr passt zu einer der aktuellen *Firewallregeln* und für die Regel wurde die Alarmmeldung aktiviert oder
- auf Ihrem Computer hat ein Eindringversuch stattgefunden, und die Alarmmeldung für den Eindringenschutz wurde eingeschaltet.

Es ist nicht unbedingt erforderlich, dass Sie etwas unternehmen, da die Firewall verdächtigen Datenverkehr automatisch blockiert und Eindringungsversuche blockiert (wenn **Blockieren und Versuch protokollieren** in den Einstellungen des Schutzes gegen Eindringlinge eingeschaltet wurde).

Verfahren Sie wie folgt, wenn ein Alarm-Popup angezeigt wird:

1. Lesen Sie die Alarminformation.
2. Klicken Sie auf **Details >>**, um die Alarmdetails anzuzeigen.
3. Wenn Sie nicht möchten, dass die Popup-Fenster mit den Firewall-Alarmen angezeigt werden, aktivieren Sie das Kontrollkästchen **Alarmdialogfeld nicht mehr anzeigen**.
4. Für Informationen über die Remote-*IP-Adresse* klicken Sie auf **DNS-Name**.
Zeigt, welcher *Domainname* zur *IP-Adresse* gehört, z. B. **www.beispiel.com**. Wenn der *Domainname* nicht aufgelöst werden kann, wird die Schaltfläche **DNS-Name** deaktiviert und es wird kein Domainname angezeigt.
5. Sie können für den Datenverkehr, der den Alarm ausgelöst hat, eine neue *Firewallregel* erstellen.

Diese Regel kann diese Art von Datenverkehr in Zukunft entweder zulassen oder ablehnen. Klicken Sie auf **Regel erstellen** und geben Sie die Regelinformationen ein.

6. Um das Dialogfeld **Firewall-Alarm** zu schließen, klicken Sie auf **Schließen**.

Sie können Ihren Computer jetzt wieder ganz normal verwenden.

Firewall-Alarme ein- oder ausschalten

Sie können auswählen, ob Popups mit Firewall-Alarmen angezeigt werden sollen oder nicht.

So schalten Sie Alarm-Popups ein oder aus:


1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
4. Klicken Sie auf **Alarmprotokoll anzeigen**.
5. Um die Popup-Nachrichten einzuschalten, aktivieren Sie das Kontrollkästchen **Alarm-Popups anzeigen**. Um die Popups auszuschalten, deaktivieren Sie das Kontrollkästchen.
6. Klicken Sie auf **Schließen**.

Wenn Sie die Popup-Nachrichten eingeschaltet haben, wird ein Popup-Fenster angezeigt, sobald Datenverkehr mit den aktuellen Firewallregeln übereinstimmt. Dies gilt nur für Regeln, für die die Alarmprotokollierung und Popups aktiviert sind. Wenn Sie die Popup-Nachrichten abgeschaltet haben, werden diese nicht mehr angezeigt.

Firewalldienste und -regeln erstellen

Sie können eigene *Firewalldienste* und -regeln erstellen, wenn Sie bestimmten Internetdatenverkehr zulassen oder ablehnen möchten.

Bevor Sie mit der Erstellung einer Regel beginnen, wählen Sie das *Firewallprofil* aus, dem Sie diese Regel hinzufügen möchten.

 **Hinweis:** Es kann sein, dass Sie Ihre eigenen Regeln nicht zu allen *Firewallprofilen* hinzufügen können.

Einen *Firewalldienst* erstellen

Sie müssen möglicherweise einen neuen *Firewalldienst* erstellen, wenn Sie z. B. ein neues Programm einsetzen, das eine Verbindung mit dem Internet benötigt und für das kein vordefinierter Dienst vorhanden ist.

Der Dienst definiert die *Protokolle* und *Ports*, die das Programm verwendet. Diese Informationen finden Sie in der Dokumentation des Programms.

So erstellen Sie einen *Firewalldienst*:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Dienste**.
4. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Neuen Dienst hinzufügen** wird geöffnet.
5. Geben Sie im Feld **Name** einen Namen für den Dienst ein. Verwenden Sie einen möglichst aussagekräftigen Namen.
6. Wählen Sie in der Liste **Protokoll** das *Protokoll* für den Dienst aus:
 - *ICMP* (1)
 - *TCP* (6)
 - *UDP* (17)

Wenn Sie ein anderes *IP-Protokoll* verwenden möchten, geben Sie die *Protokollnummer* (0-255) in das Feld ein.

7. Wenn der Dienst das *TCP-* oder das *UDP-Protokoll* verwendet, legen Sie die *Ausgangspartei-Ports* für den Dienst fest.

Wenn in der Dokumentation des Programms keine *Ausgangspartei-Ports* angegeben sind, können Sie in der Regel eine beliebige *Port*-Nummer über 1023 verwenden.

- a) Klicken Sie neben dem Feld **Ausgangspartei-Ports** auf **Bearbeiten**.
- b) Fügen Sie die *Ports* hinzu:
 - Um einen einzelnen *Port* anzugeben, geben Sie die *Port* Nummer in das Feld **Einzel** ein, beispielsweise 1024.
 - Um einen *Port* anzugeben, fügen Sie die niedrigste und die höchste *Port* -Zahl des **Bereichs** den Feldern hinzu, z. B., 1024 - 65535.
- c) Klicken Sie auf **Zur Liste hinzufügen**.

- d) Wiederholen Sie die Schritte a-c, um alle erforderlichen Ports hinzuzufügen.
 - e) Klicken Sie auf **OK**.
- 8.** Wenn der Dienst das *TCP*- oder das *UDP-Protokoll* verwendet, legen Sie die *Antwortparti-Ports* für den Dienst fest.
- Die *Antwortparti-Ports* werden in der Regel in der Dokumentation des Programms angegeben.
- a) Klicken Sie neben dem Feld *Antwortparti-Ports* auf **Bearbeiten**.
 - b) Fügen Sie die *Ports* hinzu:
 - Um einen einzelnen *Port* anzugeben, geben Sie die *Port*-Nummer in das Feld **Einzeln** ein.
 - Um einen *Portbereich* anzugeben, geben Sie den niedrigsten und den höchsten *Port* des **Bereichs** in die Felder **Bereich** ein.
 - c) Klicken Sie auf **Zur Liste hinzufügen**.
 - d) Wiederholen Sie die Schritte a-c, um alle erforderlichen Ports hinzuzufügen.
 - e) Klicken Sie auf **OK**.
- 9.** Wenn der Dienst das *ICMP-Protokoll* verwendet, definieren Sie den *ICMP-Typ* und den Code für den Dienst. Klicken Sie auf **Bearbeiten** und den **Typ** für den Dienst. Klicken Sie auf **Code** und geben Sie die Werte in die Felder **Typ** und **Code** ein. Zulässig sind die Werte 0-255.
- 10.** Wenn Sie diesen Dienst verwenden möchten, um eingehenden Datenverkehr zuzulassen, können Sie festlegen, ob Sie außerdem Broadcast- und Multicast-Datenverkehr zulassen wollen.
- Diese Art des Datenverkehrs wird von Streaming-Programmen, wie etwa Webradio oder Web-TV erstellt. Um diese Dienste zuzulassen, aktivieren Sie die Kontrollkästchen **Broadcasts zulassen** und **Multicasts zulassen**. Normalerweise können Sie diese Kontrollkästchen deaktiviert lassen.
- 11.** Klicken Sie im Dialogfeld **Neuen Dienst hinzufügen** auf **OK**.

Ihr neuer Dienst wird jetzt auf der Registerkarte **Dienste** in der Dienstliste angezeigt. Um den durch den Dienst definierten Datenverkehr zuzulassen oder abzulehnen, müssen Sie den Dienst zu einer *Firewallregel* hinzufügen, die ausgehende Internetverbindungen zulässt.

Erstellung einer Regel starten

Geben Sie einen Namen für die Regel ein und wählen Sie aus, ob die *Firewallregel* den Datenverkehr zulässt oder ablehnt.

So erstellen Sie eine Regel:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Neue Regel hinzufügen** wird geöffnet.
5. Geben Sie im Feld **Name** einen Namen für die Regel ein. Verwenden Sie einen möglichst aussagekräftigen Namen.
6. Wählen Sie **Ablehnen** oder **Zulassen**, um den Datenverkehr abzulehnen oder zuzulassen.
7. Um eine Regel zu erstellen, die nur gilt, wenn eine aktive DFÜ-Verbindung besteht, wählen Sie **Diese Regel nur auf DFÜ-Verbindungen anwenden**.

Diese Option ist nur dann relevant, wenn Sie Ihre Internetverbindung über ein Modem oder einen ISDN-Anschluss herstellen. Diese Option können Sie z. B. auswählen, wenn Sie einen Laptop außerhalb Ihres Heimnetzwerks verwenden und über ein Modem oder einen ISDN-Anschluss auf das Internet zugreifen. Außerhalb Ihres Hauses ist der Laptop nicht durch die Firewall des Routers geschützt, daher möchten Sie eventuell eine strengere Regel erstellen, die den gesamten unnötigen eingehenden Datenverkehr ablehnt, und diese Regel außerhalb anwenden. Normalerweise müssen Sie keine Regel erstellen. Außerdem schützt das Standard-Firewallprofil Ihren Computer sowohl innerhalb als auch außerhalb Ihres Hauses.

8. Klicken Sie auf **Weiter**.

IP-Adressen auswählen

Wenden Sie die Regel auf alle Netzwerkverbindungen an oder geben Sie die *IP-Adressen* und Netzwerke an, für die die neue Regel gilt.



Hinweis: Die IPv6-bezogenen Optionen stehen nur zur Verfügung, wenn Sie als Betriebssystem Microsoft Windows Vista oder Windows 7 verwenden.

So wählen Sie die *IP-Adressen* aus:

1. Wählen Sie eine der folgenden Optionen aus:

- Um die Regel sowohl auf *IPv4*- als auch auf *IPv6*-Adressen anzuwenden, wählen Sie **Beliebige IP-Adresse**.
- Damit die Regel auf alle *IPv4*-Adressen angewendet wird, wählen Sie **Beliebige IPv4-Adresse**.
- Damit die Regel auf alle *IPv6*-Adressen angewendet wird, wählen Sie **Beliebige IPv6-Adresse**.
- Damit die Regel auf bestimmte *IP-Adressen* und Netzwerke angewendet wird, wählen Sie **Benutzerdefiniert**, und klicken Sie auf **Bearbeiten**. Das Dialogfeld **Adressen** wird geöffnet.

1. Wählen Sie im Dialogfeld **Adressen** eine der folgenden Optionen der Liste **Typ** aus:

Typ	Address example
<i>IP-Adresse</i>	192.168.5.16
<i>DNS -Name</i>	www.example.com
<i>IP Bereich</i>	192.168.1.1-192.168.1.63
<i>IP- Subnetz</i>	192.168.88.0/29
<i>MyDNS</i>	[mydns]
<i>MyNetwork</i>	[mynetwork]
<i>IPv6-Adresse</i>	2001:db8:5a3b:d3:1319:8a2e:370:733
<i>IPv6-Bereich</i>	2001:db8:1234:: - 2001:db8:1234:ffff:ffff:ffff:ffff:ffff
<i>IPv6Subnetz</i>	2001:db8:1234::/48

2. Geben Sie die **Adresse** in das Feld Adresse ein.
3. Damit die Adresse zur Adressliste hinzugefügt wird, klicken Sie auf **Zur Liste hinzufügen**.
4. Wiederholen Sie die Schritte a-c, um alle erforderlichen Adressen zur Adressliste hinzuzufügen.
5. Klicken Sie auf **OK**.

2. Klicken Sie auf **Weiter**.**Wie wird ein *IP-Subnetz* definiert?**

Wenn Sie ein *IP- Subnetz* definieren möchten, verwenden Sie eine *Classless Inter-Domain Routing* -(CIDR)-Notation. Dies ist eine

Standardnotation, die aus einem *Netzwerkadresse* und einem *Subnetzmaske* besteht. Beispiel:

Netzwerkadresse	Subnetzmaske	CIDR-Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

Wählen Sie die Dienste und die Richtung aus:

Wählen Sie die Dienste aus, für die die *Firewall- regel* gilt, sowie die Richtung des Datenverkehrs.



So wählen Sie die Dienste und die Richtung aus:

1. Wählen Sie die Dienste aus, auf die Sie die Regel anwenden möchten:

- Wenn Sie die Regel auf sämtlichen IP-Verkehr anwenden möchten, wählen Sie in der Liste **Gesamter IP-Verkehr** aus.
- Wenn sich der benötigte Dienst nicht in der Liste befindet, müssen Sie ihn zuerst erstellen.

Das Symbol  ?  wird in der Spalte **Richtung** für die ausgewählten Dienste angezeigt.

2. Wählen Sie für alle Dienste die Richtung des Datenverkehrs aus, auf die die Regel angewendet wird.

Die Richtung  ?  verläuft von Ihrem Computer in das Internet oder umgekehrt. Um die Richtung auszuwählen, klicken Sie auf das Symbol **Richtung** in der Spalte Richtung.

Richtung Erklärung



Der Dienst wird in beide Richtungen zugelassen oder abgelehnt.



Der Dienst wird zugelassen oder abgelehnt, wenn er aus dem Internet auf Ihren Computer verläuft (eingehend).



Der Dienst wird zugelassen oder abgelehnt, wenn er von Ihrem eigenen Computer ins Internet verläuft (ausgehend).

3. Klicken Sie auf **Weiter**.

Alarmoptionen auswählen

Wählen Sie aus, wie das Produkt Sie benachrichtigt, wenn die *Firewallregel* Datenverkehr zulässt oder ablehnt.

So wählen Sie die Alarmoption aus:

1. Wählen Sie eine der folgenden Optionen:
 - Wenn Sie nicht benachrichtigt werden möchten, wählen Sie **Kein Alarm**. Es werden keine *Alarme* in das Protokoll der *Alarme* eingetragen und keine *Alarm*-Popups angezeigt. Diese Option sollten Sie auswählen, wenn Sie eine Regel erstellen, die Datenverkehr zulässt.
 - Wenn das Produkt *Alarme* in das Protokoll der *Alarme* eintragen soll, wählen Sie **Protokoll**.
 - Wenn das Produkt *Alarme* in das Protokoll der *Alarme* eintragen und *Alarm*-Popups anzeigen soll, wählen Sie **Protokoll und Popup**. Denken Sie daran, dass Sie die *Alarm*-Popups außerdem im Dialogfeld **Firewall-Alarme** einschalten müssen.
 - Geben Sie im Feld **Alarm-Text** eine Beschreibung ein, die im Protokoll der *Alarme* und in den Popups angezeigt wird.

2. Klicken Sie auf **Weiter**.

Regeln prüfen und übernehmen

Prüfen und übernehmen Sie die neue Regel.

Gehen Sie wie folgt vor:

1. Prüfen Sie die Zusammenfassung der Regel. Falls Sie die Regel bearbeiten müssen, klicken Sie auf **Zurück**.
2. Wenn Sie mit Ihrer neuen Regel zufrieden sind, klicken Sie auf **Fertig stellen**.

Ihre neue Regel wird jetzt auf der Registerkarte **Regeln** angezeigt. Sie ist automatisch aktiviert. Wenn Sie mehrere Regeln erstellt haben, können Sie nun die Reihenfolge ihrer Priorität festlegen.

Prioritätenfolge der *Firewallregeln* definieren

Wenn Sie mehrere neue *Firewallregeln* erstellt haben, müssen Sie deren Prioritätsreihenfolge festlegen.

Dies kann auch dann erforderlich sein, wenn z. B. eine Regel Datenverkehr ablehnt, den Sie zulassen möchten. In diesem Fall müssen Sie eine neue zulassende Regel erstellen und diese vor die ablehnende Regel verschieben. So wird die zulassende Regel zuerst auf den Datenverkehr angewendet. Sie können lediglich die Prioritätsreihenfolge der Regeln verändern, die Sie selbst erstellt haben.

So legen Sie die Prioritätsreihenfolge fest:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Klicken Sie mit der rechten Maustaste auf die Regel, die Sie verschieben möchten, halten Sie die Maustaste gedrückt, und ziehen Sie die Regel an die neue Position in der Tabelle.

Die Regeln werden jetzt in ihrer neuen Prioritätsreihenfolge auf den Datenverkehr angewendet.

So öffnen Sie einen Port durch die Firewall

Sie können einen Port durch die Firewall öffnen, wenn Sie einen Teil des Internetverkehrs zulassen möchten und die Portnummer wissen, die Sie öffnen möchten.

Es kann sein, dass Sie nicht alle Ihre eigenen Regeln zu allen Firewallprofilen hinzufügen können. Wählen Sie das *Firewallprofil* aus, zu dem Sie die neue Regel hinzufügen möchten, bevor Sie den Port öffnen.

Wenn Sie einen Port durch eine Firewall öffnen, erstellen Sie eine neue Firewallregel und zwei neue Dienste.

1. Klicken Sie auf der Startseite auf **Aufgaben**.
2. Klicken Sie auf **Firewallport öffnen**.
3. Geben Sie im Feld **Name** einen Namen für die neue Firewallregel ein.

4. Legen Sie im Feld **Port-Adresse** den Antwortport für die Regel fest. Der Antwortport wird normalerweise in der Produktdokumentation erwähnt.
5. Klicken Sie auf **OK**.

Die neue Regel wird der Liste mit Firewallregeln hinzugefügt und zwei neue Dienste werden auf der Firewalldienstliste für TCP- und UDP-Protokolle mit der angegebenen Portnummer erstellt.

Beispiele für das Erstellen von Firewallregeln


Eine neue Firewallregel erstellen Sie, wenn Sie ein neues Netzwerkspiel spielen oder Dateien in Ihrem Heimnetzwerk freigeben möchten.

Regeln für ein Netzwerkspiel erstellen

Dieses Beispiel zeigt, wie Sie *Firewalldienste* und eine *Firewallregel* für ein imaginäres Netzwerkspiel namens `Game_1` erstellen.

Um die *Firewalldienste* zu erstellen, müssen Sie wissen, welche *Protokolle* das Spiel verwendet. Sie müssen außerdem wissen, welche *Ports* das Spiel für eingehende Verbindungen vom Spiele-Server an Ihren Computer verwendet. In diesem Fall liegen folgende Daten vor:

Protokoll	Porttyp	Standort	Ports
UDP	Ausgangspartei	Game-Server	1024
UDP	Antwortpartei	Eigener Computer	8889, 9961
TCP	Ausgangspartei	Spiele-Server	1025
TCP	Antwortpartei	Eigener Computer	17475, 9961

 **Hinweis:** Sie müssen keine Firewalldienste oder eine Firewallregel für ausgehende Verbindungen von Ihrem Computer zum Spiele-Server erstellen.

So erstellen Sie die Dienste und eine Regel für die eingehenden Verbindungen:



1. Fügen Sie den neuen Dienst wie folgt hinzu:

Schritt	Beispiel
Geben Sie einen Namen für den ersten Dienst ein	<code>Service_Game_1_UDP</code>

Schritt	Beispiel
Wählen Sie das <i>Protokoll</i> aus	UDP
Geben Sie die <i>Ausgangspartei-Port</i> ein	1024
Geben Sie die <i>Antwortpatei-Ports</i> ein	8889, 9961
Geben Sie einen Namen für den zweiten Dienst ein	Service_Game_1_TCP
Wählen Sie das zweite <i>Protokoll</i> aus	TCP
Geben Sie die <i>Ausgangspartei-Port</i> ein	1025
Geben Sie die <i>Antwortpatei-Ports</i> ein	17475, 9961

Nachdem Sie die Dienste hinzugefügt haben, werden diese in der Diensteliste angezeigt.

2. Fügen Sie eine neue *Firewallregel* wie folgt hinzu:

Schritt	Beispiel
Geben Sie einen Namen für die Regel ein	Rule_Game_1
Wählen Sie den Regeltyp aus	Zulassen
Wählen Sie die <i>IP-Adressen</i> aus	Beliebige Adresse
Wählen Sie die Dienste aus	Service_Game_1_UDP, Service_Game_1_TCP
Wählen Sie die Richtung aus	 ←  (vom Internet an Ihren Computer)
Wählen Sie den <i>Alarmtyp</i> aus	Kein Alarm

Nachdem Sie die Regel hinzugefügt haben, wird diese aktiv und in der Regelliste angezeigt.

Regeln für die Dateifreigabe auf einem Heimnetzwerk erstellen

In diesem Beispiel wird eine neue *Firewallregel* für die Windows-Dateifreigabe erstellt, um Dateien auf den Computern eines Heimnetzwerks gemeinsam zu nutzen.

Wenn Sie in Ihrem Netzwerk einen *Router* verwenden, prüfen Sie die DHCP-Einstellungen (Dynamic Host Configuration Protocol) Ihres Routers, um den IP-Adressbereich zu ermitteln, der Ihrem Heimnetzwerk zugewiesen ist. Weitere Informationen finden Sie in der Dokumentation Ihres Routers.

Der Bereich für die *IP-Adresse* für Heimnetzwerke ist in der Regel 192.168.1.1 - 192.168.1.254. Wenn Sie Dateien auf all Ihren Computern freigeben möchten, müssen Sie auf allen Computern dieselbe Regel erstellen.

So erstellen Sie die Regel:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie einen Namen ein und wählen Sie den Regeltyp aus:


Schritt	Beispiel
Geben Sie einen Namen für die Regel ein	FileSharing
Wählen Sie den Regeltyp aus	Zulassen

6. Wählen Sie die *IP-Adressen* aus:

Schritt	Beispiel
1. Klicken Sie auf Benutzerdefiniert .	192.168.1.1 -
2. Klicken Sie auf Bearbeiten .	192.168.1.254
3. Wählen Sie IP- Bereich und geben Sie die Adressen Ihrer Computer in das Feld ein.	
4. Klicken Sie auf Zur Liste hinzufügen .	

7. Wählen Sie die Dienste und die Richtung aus:

Schritt	Beispiel
Wählen Sie die von der Windows-Dateifreigabe verwendeten Dienste aus	<ul style="list-style-type: none"> • SMB über TCP/IP (TCP) • SMB über TCP/IP (UDP) • Windows-Dateifreigabe und Netzwerkdrucker • Windows-Netzwerksuche

Schritt	Beispiel
	<ul style="list-style-type: none"> ICMP / Internet Control Message Protocol
Wählen Sie für beide Dienste die Richtung aus	 (vom Internet auf Ihren Computer)

8. Wählen Sie den Alarmtyp aus:

Schritt	Beispiel
Wählen Sie den Alarmtyp aus	Kein Alarm

9. Prüfen Sie die Zusammenfassung der Regel und klicken Sie auf **Fertig stellen**.

Ihre neue Regel wird auf der Registerkarte **Regeln** in der Regelliste angezeigt. Sie ist automatisch aktiviert.

10. Prüfen Sie, ob die Regel funktioniert.

Verwenden Sie hierbei die Windows-Dateifreigabe, um einen Ordner oder eine Datei freizugeben, und prüfen Sie, ob Sie von allen Computern auf die Datei oder den Ordner zugreifen können.



Tipp: Wenn Sie den Drucker in Ihrem Heimnetzwerk freigeben möchten, dann erstellen Sie eine ähnliche Regel. In diesem Fall müssen Sie lediglich eine Regel erstellen, die auf dem Computer, an dem der Drucker angeschlossen ist, eingehenden Datenverkehr zulässt.

Firewallregeln ein- oder ausschalten

Sie können eine *Firewallregel* vorübergehend ausschalten, um Datenverkehr zuzulassen, den die Regel ablehnt.

Sie können die Regeln ein- bzw. ausschalten, die Sie selbst erstellt haben.

So schalten Sie eine Regel ein oder aus:

- Klicken Sie auf der Startseite auf **Einstellungen**.
- Wählen Sie **Netzwerkverbindung** ► **Firewall**.
- Klicken Sie auf die Registerkarte **Regeln**.
- Führen Sie einen der folgenden Schritte durch:

- Wenn Sie eine Regel abschalten möchten, müssen Sie das Häkchen in der Spalte **Wird benutzt** entfernen.
- Wenn Sie die Regel einschalten möchten, aktivieren Sie das Kontrollkästchen.

Abhängig von Ihrer Auswahl ist die Firewallregel nun ein- bzw. ausgeschaltet.

Firewallregeln ändern

Sie können nur eine *Firewallregel* ändern, die Sie selbst erstellt haben.

So ändern Sie eine Regel:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Wählen Sie die Regel aus und klicken Sie auf **Details**.
Das Dialogfeld **Regeldetails** wird geöffnet.
5. Nehmen Sie schrittweise die erforderlichen Änderungen vor. Klicken Sie auf **Weiter**, um zum jeweils nächsten Schritt zu gelangen.
6. Prüfen Sie im Dialogfeld **Regeldetails** Ihre Änderungen.
7. Wenn die Regel in Ordnung ist, klicken Sie auf **Fertig stellen**.

Ihre Änderungen werden auf die Regel angewendet.

Firewalleinstellungen

Auf der Registerkarte **Einstellungen** können Sie die *IPv6*-Einstellungen und die Alarmstufe ändern sowie den gesamten Datenverkehr zwischen Computern in einem Heimnetzwerk zulassen.


Die Registerkarte **Einstellungen** enthält außerdem das Feld **IP-Fragmente blockieren, die kürzer sind als** angezeigt. Die Registerkarte *Firewall* blockiert *IP-Paketfragmente*, die kürzer sind als der in diesem Feld angezeigte Grenzwert. Kurze *IP-Paketfragmente* weisen möglicherweise auf einen *Fragmentationsangriff* hin, der Ihren Computer zum Absturz bringen kann. Sie sollten den in diesem Feld angegebenen Grenzwert möglichst nicht ändern.

IPv6-Einstellungen ändern

Auf der Registerkarte **Einstellungen** können Sie festlegen, wie die *Firewall* den *IPv6*-Datenverkehr behandelt.

Wenn Sie als Betriebssystem Microsoft Windows Vista oder Windows 7 verwenden, können Sie entweder den gesamten *IPv6*-Datenverkehr sperren oder normale *Firewallregeln* auf den Datenverkehr anwenden. Wenn Sie ein anderes Betriebssystem einsetzen, können Sie den gesamten *IPv6*-Datenverkehr entweder blockieren oder zulassen.

So ändern Sie die *IPv6*-Einstellungen:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
 2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
 3. Klicken Sie auf die Registerkarte **Einstellungen**.
 4. Um festzulegen, wie die *Firewall* den *IPv6*-Datenverkehr behandelt, wählen Sie in der Liste **Filteroptionen für IPv6-Datenverkehr auswählen** eine der folgenden Optionen aus:
 - Wenn Sie Microsoft Windows Vista oder Windows 7 verwenden:
 - **Blockieren**: Blockiert den gesamten *IPv6*-Datenverkehr. Es empfiehlt sich, diese Option aktiviert zu lassen.
 - **Normal**: Normale *Firewallregeln* definieren, ob der *IPv6*-Datenverkehr zugelassen oder blockiert ist. Diese Option können Sie auswählen, wenn Sie auf Ihrem Computer das *IPv6*-Protokoll verwenden.
 - Wenn Sie ein anderes Betriebssystem einsetzen:
 - **Blockieren**: Der gesamte *IPv6*-Datenverkehr wird blockiert. Es empfiehlt sich, diese Option aktiviert zu lassen.
 - **Zulassen**: Lässt den gesamten *IPv6*-Datenverkehr zu. Diese Option können Sie auswählen, wenn Sie auf Ihrem Computer das *IPv6*-Protokoll einsetzen.
-  **Hinweis:** Den gesamten *IPv6*-Datenverkehr zuzulassen, stellt ein Sicherheitsrisiko dar, weil auf den *IPv6*-Datenverkehr keine *Firewallregeln* angewendet werden.
5. Klicken Sie auf **OK**.

Ihre Änderungen der *IPv6*-Einstellungen sind jetzt aktiv.

Was zu tun ist, wenn Sie eine Internetverbindung mit dem Heimnetzwerk verwenden möchten

Wenn Sie eine Internetverbindung Ihres Computers mit Ihrem restlichen Heimnetzwerk verwenden möchten, müssen Sie dem gesamten Datenverkehr zwischen diesen Computern gestatten, die Firewall zu passieren.



Hinweis:

Lassen Sie den gesamten Datenverkehr nur dann die Firewall passieren, wenn Sie die Gemeinsame Internetnutzung von Windows verwenden. Wenn Sie andere Ressourcen freigeben möchten - wie Laufwerke, Dateien oder Drucker - sollten Sie hierfür neue Firewallregeln erstellen.

Sie können den gesamten Datenverkehr durch die Firewall passieren lassen, indem Sie die Verbindung zwischen dem Heimnetzwerk und dem Computer mit der Internetverbindung als vertrauenswürdig definieren. Sie können eine *Vertrauenswürdige Netzwerkschnittstelle* definieren, wenn:

- Sie haben einen Computer mit einer Internetverbindung.
- Dieser Computer besitzt zwei *Netzwerkkarten*: Eine für die Internetverbindung und die andere für die Verbindung mit dem Heimnetzwerk.
- Sie haben auf dem Computer, der die Internetverbindung besitzt, in Windows die Gemeinsame Nutzung der Internetverbindung aktiviert.
- Sie haben unser Produkt mit einer Firewall auf all Ihren Computern installiert. So können Sie sicher sein, dass Sie kein Risiko eingehen, wenn Sie zwischen Ihren Computern eine vertrauenswürdige Schnittstelle definieren.

Um die vertrauenswürdige Netzwerkschnittstelle zu definieren, müssen Sie die Netzwerkkarte (Adapter) auswählen, über die der Computer mit dem Heimnetzwerk verbunden ist.

So wählen Sie die Netzwerkkarte auf dem Computer mit der Internetverbindung aus:

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

2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
4. Wählen Sie in der Liste **Vertrauenswürdiger Netzwerkadapter** die **Netzwerkkarte** (Adapter) aus, über die Ihr Computer mit dem Heimnetzwerk verbunden ist. Die **IP-Adresse** des Computers wird im Feld **IP-Adresse** angezeigt.



Hinweis: Da die *Firewall* den Datenverkehr über die ausgewählte Netzwerkschnittstelle zulässt, müssen Sie sicherstellen, dass Sie nicht die Internetschnittstelle als vertrauenswürdig auswählen. Andernfalls schützt die Firewall Ihren Computer nicht mehr.

5. Klicken Sie auf **OK**.

Die *Firewall* lässt nun den gesamten Datenverkehr zwischen dem Computer mit der Internetverbindung und Ihrem Heimnetzwerk zu. Sie können das Internet jetzt von allen Computern aus nutzen.

Wie sieht es bei Verwendung einer digitalen TV-Karte aus?

Wenn Sie eine digitale TV-Karte verwenden und das Fernsehbild friert ein, dann müssen Sie auch die Schnittstelle zum Fernseher als vertrauenswürdig definieren.

So kontrollieren Sie Netzwerkanwendungen


Die Anwendungssteuerung verhindert, dass schädliche Programme eine Verbindung mit dem Internet herstellen.

Die Anwendungssteuerung schützt Sie hauptsächlich vor ausgehenden Bedrohungen, die durch Programme auf Ihrem Computer verursacht werden. Im Normalfall öffnet die Anwendungssteuerung ein Popup-Fenster, sobald ein Programm versucht, eine Verbindung zum Internet herzustellen. In diesem Popup-Fenster können Sie die Verbindung dann zulassen oder ablehnen:

- Wenn Sie darauf vertrauen, dass das Programm sicher ist, können Sie die Verbindung zulassen. Sie können z. B. davon ausgehen, dass das Programm sicher ist, wenn Sie es gerade selbst gestartet haben. Wenn Sie die Verbindung zulassen, öffnet die *Firewall* für das Programm einen *Port* und lässt die Verbindung so lange zu, wie das Programm gestartet ist. Wenn Sie das Programm beenden, schließt die Firewall den *Port*.
- Wenn Sie dem Programm nicht vertrauen, müssen Sie die Verbindung ablehnen. Ein Programm kann z. B. unsicher sein, wenn Sie es nicht kennen oder nicht selbst installiert haben.

Je nach den gewählten Einstellungen werden bei Programmen, die DeepGuard als sicher einstuft, keine Popup-Fenster zur Anwendungssteuerung angezeigt. Diese Programme sind berechtigt, automatisch eine Verbindung zum Internet herzustellen.

Die Anwendungssteuerung fragt Sie außerdem, ob Sie Verbindungen aus dem Internet zu den Programmen auf Ihrem Computer zulassen möchten. Dies ist z. B. der Fall, wenn Sie Skype verwenden.

 **Hinweis:** Schalten Sie die Anwendungssteuerung nicht aus, wenn ein Programm auf Ihrem Computer nicht funktioniert. Dies reduziert die Schutzstufe Ihres Computers. Ändern Sie stattdessen die Einstellungen der Anwendungssteuerung oder die *Firewallregeln*.

Was ist der Unterschied zwischen Firewall und Anwendungssteuerung?

Eine Firewall bietet grundlegenden Schutz auf Netzwerkebene, wohingegen Sie mithilfe der Anwendungskontrolle die Verwendung bestimmter Programme steuern können. Die Firewall schützt Sie vor Bedrohungen,

die durch Verbindungen aus dem Internet mit Ihrem Computer verursacht werden (eingehende Verbindungen). Die Firewall gestattet bzw. verweigert Verbindungen auf der Grundlage der von den Verbindungen verwendeten IP-Adressen.

Die Anwendungssteuerung schützt Sie in erster Linie vor Bedrohungen, die durch Verbindungen von Ihrem Computer ins Internet verursacht werden (ausgehende Verbindungen). Die Anwendungssteuerung gestattet bzw. verweigert Verbindungen auf der Grundlage der Programme, die die Verbindungen erstellen.

Was tun, wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird?

Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt wird, müssen Sie entscheiden, ob Sie den Verbindungsversuch für das im Popup angegebene Programm zulassen oder ablehnen möchten.

Popups der Anwendungssteuerung können auf schädliche Aktivitäten hinweisen, wie auf *Trojaner*, *Würmer* oder *Spyware*. Andererseits werden auch Popups angezeigt, wenn Sie die Programme auf Ihrem Computer normal verwenden.

So lassen Sie einen Verbindungsversuch zu oder lehnen diesen ab:

1. Prüfen Sie im Popup-Fenster die Informationen über den Verbindungsversuch.
2. Um die Details des Verbindungsversuchs anzuzeigen - wie den Namen des Programms und die IP-Adresse des Remote-Computers - klicken Sie auf **Details**.
3. Wenn Sie möchten, das für das aktuelle Programm in Zukunft keine Popups mehr angezeigt werden, aktivieren Sie das Kontrollkästchen **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen**.
4. Lassen Sie die Verbindung entweder zu oder lehnen Sie sie ab:
 - Klicken Sie auf **Zulassen**, wenn Sie sicher sind, dass der Verbindungsversuch sicher ist. Sie können die Verbindung in den folgenden Fällen zulassen:

Popup-Typ	Beschreibung	Klicken Sie auf Zulassen wenn...
Neuer Verbindungsversuch (ausgehend)	Ein <i>Client</i> -Programm auf Ihrem Computer versucht, eine Verbindung zum Internet herzustellen.	Sie haben dieses Programm zum ersten Mal selbst gestartet.
Geänderte Anwendung (ausgehend)	Ein <i>Client</i> -Programm auf Ihrem Computer versucht, eine Verbindung zum Internet herzustellen, es wurde aber seit der letzten Verbindung geändert.	Sie haben das Programm seit seiner letzten Verwendung auf Ihrem Computer aktualisiert.
Neue Serveranwendung (e eingehend)	Ein Programm auf Ihrem Computer versucht als <i>Server</i> zu agieren und möchte anfangen, eingehende Verbindungen zu erwarten.	Sie haben das <i>Server</i> programm selbst auf Ihrem Computer gestartet.
Geänderte Anwendung (e eingehend)	Ein <i>Server</i> programm auf Ihrem Computer möchte auf eingehende Verbindungen warten, es wurde aber seit dem letzten Verbindungsversuch geändert.	Sie haben das <i>Server</i> programm seit der letzten Verwendung auf Ihrem Computer aktualisiert.

- Klicken Sie auf **Ablehnen**, wenn Sie nicht sicher sind, ob der Verbindungsversuch sicher ist.

Abhängig von der ausgewählten Aktion wird die Verbindung entweder zugelassen oder abgelehnt. Wenn Sie das Kontrollkästchen **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen** aktiviert haben, wird das Programm auf der Registerkarte **Anwendungen** zur Liste der zugelassenen bzw. abgelehnten Programme hinzugefügt. Es werden für dieses Programm keine Popup-Fenster über Verbindungsversuche mehr angezeigt.

Sichere und unsichere Programme und Verbindungsversuche

Bevor Sie in einem Popup-Fenster der Anwendungssteuerung eine Verbindung zulassen, sollten Sie prüfen, ob das Programm sicher ist.

Welche Programme und Verbindungsversuche können als sicher angesehen werden?

- Ein bekanntes Programm, das Sie selbst gestartet haben.
- Microsoft Windows-Betriebssystem, das für die Updatedienste eine Verbindung zum Internet herstellt.

Welche Programme und Verbindungsversuche sollten als unsicher angesehen werden?

- Alle Programme, die Sie von einer unbekanntem Quelle erhalten haben.
- Alle Programme, die Sie nicht selbst installiert haben oder die Sie nicht kennen.
- Alle Programme, die Sie als sicher ansehen, die aber versuchen, eine Verbindung zum Internet herzustellen oder als *Server* zu agieren, ohne dass Sie sie gestartet haben.

Verbindungen für Programme zulassen oder ablehnen

Sie können Internetverbindungen für Programme auf der Registerkarte **Anwendungen** zulassen oder ablehnen.

Sie können z. B. eine Verbindung für ein Programm zulassen, die Sie versehentlich im Popup-Fenster der Anwendungssteuerung abgelehnt haben.

Standardmäßig enthält die Registerkarte **Anwendungen** die folgenden Programme:

- Wenn die Option **Bei neuen Programmen fragen** aktiviert ist: Programme, die Sie zugelassen oder abgelehnt haben und für die Sie im Popup-Fenster der Anwendungssteuerung die Option **Dieses Dialogfeld zukünftig nicht mehr für dieses Programm anzeigen** gewählt haben.
- Wenn die Option **Zulassen und zur Programmliste hinzufügen** aktiviert ist: zugelassene Programme.
- Das Programm, das Sie auf dieser Registerkarte manuell zur Liste der Programme hinzugefügt haben.

Diese Registerkarte zeigt nicht automatisch die zugelassenen Betriebssystemprogramme an, die DeepGuard als sicher ansieht.

So lassen Sie die Verbindung für ein Programm zu oder lehnen diese ab:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Systemmenü des Programms**.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie das Programm aus und klicken Sie auf **Details**. Das Dialogfeld **Anwendungsdetails** wird geöffnet.
5. Wählen Sie unter **Client-Verbindung (ausgehend)** eine passende Option:
 - **Ablehnen**: Wenn Sie ablehnen möchten, dass das Programm eine Verbindung mit dem Internet herstellt, wenn es das nächste Mal gestartet wird.

- **Zulassen:** Wenn Sie zulassen möchten, dass das Programm eine Verbindung mit dem Internet herstellt, wenn es das nächste Mal gestartet wird.
 - **Auffordern:** Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt werden soll, wenn das Programm das nächste Mal versucht, eine Verbindung mit dem Internet herzustellen. In diesem Popup-Fenster können Sie die Verbindung entweder zulassen oder ablehnen.
6. Wählen Sie unter **Server-Verbindung (eingehend)** eine geeignete Option:
- **Ablehnen:** Wenn Sie Verbindungen aus dem Internet zu dem Programm ablehnen möchten.
 - **Zulassen:** Wenn Sie Verbindungen aus dem Internet zu dem Programm zulassen möchten.
 - **Auffordern:** Wenn ein Popup-Fenster der Anwendungssteuerung angezeigt werden soll, wenn das nächste Mal versucht wird, eine Verbindung aus dem Internet zu dem Programm herzustellen. In diesem Popup-Fenster können Sie die Verbindung entweder zulassen oder ablehnen.
7. Klicken Sie auf **OK**.



Tipp: Sie können Internetverbindungen für ein neues Programm bereits ablehnen oder zulassen, bevor Sie beginnen, es zu verwenden. Hierzu klicken Sie auf die Schaltfläche **Hinzufügen** und wählen die Programmdatei aus. Anschließend können Sie für das Programm eingehende oder ausgehende Verbindungen entweder zulassen oder ablehnen.

Popup-Fenster der Anwendungssteuerung ein- oder ausschalten

Sie können die Popup-Fenster der Anwendungssteuerung ein- bzw. ausschalten.

Wenn Sie die Popup-Fenster der Anwendungssteuerung ausschalten, lässt das Produkt automatisch Verbindungen für alle Programme zu.

So schalten Sie die Popup-Fenster der Anwendungssteuerung ein oder aus:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Systemmenü des Programms**.
3. Klicken Sie auf die Registerkarte **Einst.**
4. Wählen Sie eine der folgenden Optionen:
 - **Zulassen und zur Liste der Programme hinzufügen** : Wählen Sie diese Option, wenn Sie die Popup-Fenster der Anwendungssteuerung ausschalten möchten.
 - **Bei neuen Programmen fragen** : Wählen Sie diese Option, wenn Sie die Popup-Fenster der Anwendungssteuerung einschalten möchten. Sobald ein neues Programm zum ersten Mal versucht, eine Verbindung herzustellen, wird ein Popup-Fenster eingeblendet.
5. Wenn Sie nicht möchten, dass die Popups der Anwendungssteuerung bei Programmen angezeigt werden, die DeepGuard für sicher hält, wählen Sie **Bei bekannten Programmen nicht fragen**.
Lassen Sie dieses Kontrollkästchen möglichst aktiviert.
6. Klicken Sie auf **OK**.

Abhängig von Ihrer Auswahl sind die Popup-Fenster der Anwendungssteuerung nun entweder ein- oder ausgeschaltet.

Was tun, wenn ein Programm nicht mehr funktioniert?

Wenn Sie ein neues Programm zum ersten Mal einsetzen, z. B. ein Netzwerkspiel, funktioniert es möglicherweise nicht, wenn es keine Verbindung zum Internet herstellen kann.

Dies kann z. B. aus folgenden Gründen passieren:

- Ihr aktuelles *Firewallprofil* ist sehr streng und verwehrt Internetverbindungen für die meisten Programme, einschließlich des Netzwerkspiels, das Sie gerade verwenden.
- Sie haben ein Popup-Fenster der Anwendungssteuerung übersehen und das Popup ist noch im Hintergrund aktiv.
- Sie haben die Verbindung in dem Popup versehentlich abgelehnt.

Gehen Sie wie folgt vor, um sicherzustellen, dass das Programm eine Verbindung mit dem Internet herstellen kann:

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


2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Aktivieren Sie auf der Registerkarte **Regeln** das aktuelle *Firewallprofil*.
Wenn es sich dabei um ein sehr strenges Profil handelt, ändern Sie es zu einem weniger strengen, und klicken Sie auf **OK**.
4. Starten Sie das Programm und prüfen Sie, ob es jetzt funktioniert.
5. Wenn das Programm nicht funktioniert, schalten Sie die Popups der Anwendungssteuerung vorübergehend aus, um sämtliche Verbindungen für neue Programme zuzulassen.
6. Wählen Sie **Netzwerkverbindung** ► **Systemmenü des Programms**.
7. Wählen Sie auf der Registerkarte **Einstellungen** die Option **Zulassen und zur Liste der Programme hinzufügen**, und klicken Sie dann auf **OK**.
8. Starten Sie das Programm und prüfen Sie, ob es jetzt funktioniert.
9. Wenn das Programm funktioniert, schalten Sie die Popups der Anwendungssteuerung wieder ein.
10. Wählen Sie **Netzwerkverbindung** ► **Systemmenü des Programms**.
11. Wählen Sie auf der Registerkarte **Einstellungen** die Option **Bei neuen Programmen fragen**, und klicken Sie auf **OK**.

So wehren Sie Eindringlinge ab

Intrusion Prevention schützt Sie vor Netzwerkangriffen, die sich gegen offene *Ports* Ihres Computers richten.

Intrusion Prevention verwendet vordefinierte Regeln, mit denen Netzwerkangriffe erkannt werden. Diese Regeln enthalten Informationen über bekannten böartigen Datenverkehr. Wenn die Intrusion Prevention Datenverkehr erkennt, der mit einer Regel übereinstimmt, wird der Datenverkehr blockiert (sofern die Option **Blockier. und protok** aktiviert ist) und generiert eine Alarmmeldung im Protokoll der Firewall-Alarmmeldungen. Je nach den gewählten Einstellungen wird im Firewall-*Alarm*protokoll des Internet-Schutzschilds ein Alarm erzeugt. Sofern Sie entsprechende Einstellungen vorgenommen haben, wird außerdem ein Alarm-Popup des Internet-Schutzschilds angezeigt.

Intrusion Prevention erkennt und verhindert böartigen Datenverkehr der durch Netzwerkwürmer wie den Wurm Sasser verursacht wird. Der Wurm Sasser infiziert ungeschützte Systeme, indem er am TCP-Port 445 böartigen Datenverkehr an den Microsoft-Dienst für die Netzwerkfreigabe sendet. Dieser Dienst wird für die Freigabe von Druckern in einem Netzwerk verwendet. Der Wurm öffnet eine TCP-Verbindung zu dem Pot und sendet böartigen Datenverkehr über den Port. Der Datenverkehr verursacht einen Overflow und sorgt unter Umständen dafür, dass das gesamte System abstürzt.

 **Hinweis:** Schalten Sie die Intrusion Prevention nicht ab. Sonst verringert sich die Schutzstufe Ihres Computers.

Worin besteht der Unterschied zwischen Firewall und Intrusion Prevention?

Im Unterschied zur Firewall blockiert Intrusion Prevention nur Datenverkehr, der als böartig eingestuft wird, und lässt den übrigen Datenverkehr den Port passieren. Die Firewall lässt entweder den gesamten Datenverkehr über den Port zu oder blockiert ihn.

Auswählen, wie Eindringversuche behandelt werden

Auf der Registerkarte **Schutz vor Eindringlingen** können Sie auswählen, wie Eindringungsversuche behandelt werden.

Die Eindringungsversuche können entweder automatisch blockiert und protokolliert oder lediglich protokolliert werden.

So wählen Sie aus, wie Eindringungsversuche behandelt werden:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung ► Eindringenschutz**.
3. Wählen Sie eine der folgenden Optionen:
 - **Blockieren und Versuch protokollieren:** Wählen Sie diese Option, wenn Sie Eindringversuche sowohl blockieren als auch protokollieren möchten. Die Versuche werden blockiert, und die Informationen zu den Versuchen werden im Dialogfeld **Firewall-Alarme** angezeigt.
 - **Protokollieren:** Wählen Sie diese Option aus, wenn Sie nur die Eindringversuche protokollieren möchten. Die Informationen über die Versuche werden im Dialogfeld **Firewall-Alarme** angezeigt.
4. Wenn Sie möchten, dass ein Popup-Fenster mit einem **Firewall-Alarm** angezeigt wird, wenn ein Eindringungsversuch vermutet wird, wählen Sie **Alarm anzeigen, wenn ein Eindringversuch vermutet wird**.
5. Klicken Sie auf **OK**.

Die Einstellung zum Schutz vor Eindringlingen wurde jetzt geändert.

So steuern Sie *DFÜ-Verbindungen*

Der *Dialerschutz* verhindert, dass böswillige Dialerprogramme Verbindungen zu kostenpflichtigen Telefonnummern mit einem hohen Minutenpreis herstellen.

Böswillige *Dialerprogramme* versuchen möglicherweise, Ihre Internetverbindung zu schließen und eine neue *DFÜ-Verbindung* zu einer anderen Telefonnummer herzustellen. Die Verbindung zu dieser Nummer kann sehr teuer sein und kommt dem Hersteller des *Dialerprogramms* zugute.

Durch den Einsatz des *Dialerschutzes* können Sie verhindern, dass diese böswilligen Dialerprogramme Verbindungen beenden und neue herstellen. Der *Dialerschutz* verhindert außerdem, dass versehentlich falsche oder mit hohen Kosten verbundene Nummern angewählt werden. Sie können sicherstellen, dass *DFÜ-Verbindungen* sicher sind, indem Sie folgende Definitionen vornehmen:

- die Nummern, zu denen Programme eine *DFÜ-Verbindung* herstellen können und
- die Programme, die berechtigt sind, *DFÜ-Verbindungen* zu beenden.



Hinweis: Der *Dialerschutz* ist für Benutzer, die für ihre Internetverbindung ein Modem oder eine *ISDN-Verbindung* verwenden.

Das Virus- und Spyware-Scannen erkennt böswillige *Dialerprogramme* als *Spyware* und kann sie von Ihrem Computer entfernen. Wenn ein neues böswilliges *Dialerprogramm* nicht erkannt wird, verhindert der *Dialerschutz*, dass dieses Dialerprogramm *DFÜ-Verbindungen* herstellt.

Wenn Sie den Verdacht haben, dass sich auf Ihrem Computer ein nicht erkannter *Dialer* befindet, können Sie die *Dialerdatei* als Muster an F-Secure schicken. Anschließend aktualisiert F-Secure die *Viren- und Spyware-Definitionsdatenbanken* und Sie können Ihren Computer erneut scannen. Der *Dialer* wird dann erkannt und kann von Ihrem Computer entfernt werden.

Was tun, wenn ein Popup-Fenster der Einwahlkontrolle angezeigt wird?

Wenn das Popup-Fenster "Neuer Einwahlversuch" angezeigt wird, können Sie die *DFÜ-Verbindung* entweder zulassen oder ablehnen.

So lassen Sie eine *DFÜ-Verbindung* zu oder lehnen diese ab:

1. Prüfen Sie den Namen des Programms.
2. Prüfen Sie die Telefonnummer.
3. Lassen Sie die *DFÜ-Verbindung* entweder zu oder lehnen Sie sie ab:
 - Wenn die Nummer in Ordnung ist (der Ihres Service Providers entspricht) und das Programm von Ihnen selbst gestartet wurde:
 1. Wählen Sie **Diese Einstellung für die Zukunft speichern**.
 2. Klicken Sie auf **Zulassen**.
 - Wenn die Nummer falsch ist oder wenn die Verbindung automatisch hergestellt wurde:
 1. Wählen Sie **Diese Einstellung für die Zukunft speichern**.
 2. Klicken Sie auf **Ablehnen**.

Die Verbindung wird auf der Grundlage der von Ihnen getroffenen Entscheidung zugelassen oder abgelehnt. Die Nummer und die Informationen über das Programm werden auf der Registerkarte **Nummernliste** zur Liste hinzugefügt. Anschließend:

- Wenn Sie die Verbindung zugelassen haben, wird kein Popup mehr angezeigt, wenn erneut ein Programm versucht, eine *DFÜ-Verbindung* zu dieser Nummer herzustellen.
- Wenn Sie die Verbindung abgelehnt haben und ein Programm versucht, eine *DFÜ-Verbindung* zu dieser Nummer herzustellen, wird das Popup **Abgelehnter Einwahlversuch** angezeigt. Schließen Sie das Popup-Fenster, indem Sie auf **Schließen** klicken.

Hinweis:

Möglicherweise wird ein Popup **Verbindung schließen** angezeigt, wenn ein Programm versucht, eine *DFÜ-Verbindung* zu schließen. Wenn es sich bei dem Programm um das handelt, das Sie selbst beendet haben, können Sie das Schließen der *DFÜ-Verbindung* zulassen. Klicken Sie hierzu auf **Zulassen**. Wenn es sich nicht um das Programm handelt, das Sie selbst beendet haben, müssen Sie das Schließen ablehnen, indem Sie auf **Ablehnen** klicken. Das Ablehnen des Beendigungsversuchs stellt sicher, dass kein

schädliches *Dialer*programm Ihre Internetverbindung beendet und eine neue Verbindung zu einer anderen Nummer herstellt.

Zulässige Telefonnummern bearbeiten

Zu der Liste der Telefonnummern auf der Registerkarte **Nummernliste** können Sie Nummern hinzufügen, wenn Sie *DFÜ-Verbindungen* zu diesen Nummern zulassen oder ablehnen möchten.

So fügen Sie eine neue Nummer zur Liste hinzu:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Einwahlkontrolle**.
3. Klicken Sie auf die Registerkarte **Nummernliste**.
4. Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Nummer/Bereich hinzufügen** wird geöffnet.
5. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Nummer ein.
6. Geben Sie im Feld **Nummer** die Telefonnummer ein:
 - Folgende Zeichen dürfen verwendet werden: #*1234567890.
 - Sie können eine Vorwahl und eine Landesvorwahl verwenden, z. B. 040-1234567, 00 358 9 123 4567.
 - Sie können andere Zeichen, wie Leerzeichen oder Bindestriche verwenden, um die Nummern zu strukturieren. Der Dialerschutz ignoriert jedoch andere als die oben aufgeführten Zeichen. Er behandelt z. B. 09-1234567 als dieselbe Nummer wie 091234567.
 - Mithilfe der folgenden Platzhalter können Sie einen Nummernbereich eingeben:
 - "?" ersetzt eine einzelne Zahl. Um z. B. die *DFÜ-Verbindung* zu bestimmten Servicenummern abzulehnen, geben Sie 0900?234567 ein.
 - "X" oder "x" ersetzt eine oder mehrere Zahlen. Sie können diese Platzhalter verwenden, wenn Sie z. B. *DFÜ-Verbindungen* ins Ausland ablehnen möchten. Wenn Sie normalerweise eine Auslandsverbindung mit "00" beginnen, geben Sie "00x" ein, um alle *DFÜ-Verbindungen* ins Ausland abzulehnen.
7. Wählen Sie aus, ob Sie die *DFÜ-Verbindungsversuche* ablehnen oder zulassen möchten:

- Wählen Sie **Abgelehnt**, um alle Versuche, eine *DFÜ-Verbindung* zu der eingegebenen Nummer herzustellen, abzulehnen.
 - Wählen Sie **Zugelassen**, um *DFÜ-Verbindungen* mit der eingegebenen Nummer zuzulassen.
8. Klicken Sie auf **OK**.
Auf der Registerkarte **Nummernliste** werden die Telefonnummer bzw. der Nummernbereich sowie die ausgewählte Aktion angezeigt:
- Wenn Sie eine Nummer zulassen, wird vor der Nummer das Symbol ✓ angezeigt.
 - Wenn Sie die Nummer abgelehnt haben, wird vor der Nummer das Symbol × angezeigt.
9. Wenn Sie die Prioritätsreihenfolge der Nummern ändern möchten, klicken Sie auf eine Nummer in der Liste, halten Sie die Maustaste gedrückt, und ziehen sie die Nummer an die neuen Position in der Tabelle.



Hinweis: Auf der Registerkarte **Nummernliste** befinden sich möglicherweise einige vordefinierte Nummern, falls Ihr Service Provider *DFÜ-Verbindungen* zu bestimmten Nummern abgelehnt oder zugelassen hat. Diese Nummern können Sie nicht entfernen.

Programme anzeigen, die *Einwahlverbindungen* herstellen dürfen

Auf der Registerkarte **Einstellungen** können Sie die sicheren Programme anzeigen, die berechtigt sind

Diese Registerkarte zeigt folgende Programme:

- Sichere Programme, die jederzeit berechtigt sind, *DFÜ-Verbindungen* zu beenden, wie z. B. der von Ihnen verwendete Webbrowser.
- Programme, bei denen Sie gefragt werden, ob Sie das Beenden der *DFÜ-Verbindung* zulassen oder ablehnen möchten. Die Registerkarte zeigt die Programme, bei denen Sie zugelassen haben, dass sie *DFÜ-Verbindungen* beenden.

Diese Registerkarte zeigt nicht die abgelehnten Programme an. Wenn Sie das Beenden der Verbindung für eine Anwendung in einem Popup-Fenster abgelehnt haben, kann die Verbindung erst dann getrennt werden, wenn

Sie den Computer neu starten. Wenn Sie die Trennung der DFÜ-Verbindung durch eine Anwendung zugelassen haben, kann die Anwendung die Verbindung jederzeit trennen. Sie müssen diese Option nicht erneut auswählen.

So zeigen Sie die Programme an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Einwahlkontrolle**.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
Diese Registerkarte zeigt eine Liste der Programme, die berechtigt sind, *DFÜ-Verbindungen* zu beenden.

DFÜ-Verbindungsversuche anzeigen

Wenn Sie die Protokollierung des Dialerschutzes aktivieren, können Sie die Versuche, eine *DFÜ-Verbindung* herzustellen, sehen, die das Produkt erkannt hat.

Die Protokollierung des Dialerschutzes ist standardmäßig deaktiviert.

So schalten Sie die Protokollierung ein:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Einwahlkontrolle**.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
4. Wählen Sie **Protokoll der Einwahlkontrolle aktivieren**, um die Protokollierung einzuschalten.
5. Klicken Sie auf **Protokoll anzeigen**, um das erstellte Protokoll anzuzeigen.

Sie können folgende Informationen anzeigen:

- Versuche, *DFÜ-Verbindungen* herzustellen oder zu beenden.
- Ob die Versuche zugelassen oder abgelehnt wurden.
- Gewählte Telefonnummern.

Wie gehe ich vor, wenn meine Internetverbindung nicht mehr funktioniert?

Wenn die *DFÜ-Verbindung* zu Ihrem Internet Service Provider (oder einer anderen Telefonnummer) nicht mehr funktioniert, überprüfen Sie, ob Sie nicht versehentlich die Verbindungen zu dieser Nummer abgelehnt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Einwahlkontrolle**.
3. Klicken Sie auf die Registerkarte **Nummernliste**.
4. Prüfen Sie, ob sich die Nummer, die Sie anwählen möchten, in der Liste befindet. Wenn dies der Fall ist und wenn die Nummer abgelehnt wird (das Symbol × steht davor), verfahren Sie wie folgt:
 - a) Wählen Sie die Nummer aus.
 - b) Klicken Sie auf **Bearbeiten**.
 - c) Wählen Sie **Zugelassen**.
 - d) Klicken Sie auf **OK**.
Das Symbol vor der Nummer wurde in ✓ geändert.

Testen Sie, ob die Verbindung zu der Nummer jetzt hergestellt werden kann.

Wo finde ich die Alarmmeldungen und Protokolldateien der Firewall?

Anhand der Alarmmeldungen und Protokolldateien der Firewall können Sie feststellen, wie die Netzwerkverbindungen Ihres Computers geschützt sind.

Firewall-Alarme anzeigen

Sie können eine Liste aller erzeugten Firewall-Alarme anzeigen.

Die Liste enthält Alarme, die von der Firewall und dem Schutz gegen Eindringlinge ausgelöst wurden.

So zeigen Sie die Liste an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Firewall**.
3. Klicken Sie auf die Registerkarte **Regeln**.
4. Klicken Sie auf **Alarmprotokoll anzeigen**.
Das Dialogfeld **Firewall-Alarme** wird geöffnet und zeigt folgende Informationen an:

Feld	Beschreibung
Zeit	Zeitpunkt des Alarms.
Remote-Adresse	<i>IP-Adresse</i> des Computers, von dem Datenverkehr empfangen wurde bzw. an den Datenverkehr gesendet wurde.
Treffer	Zeigt, wie oft ein ähnlicher Alarm erzeugt wurde.
Beschreibung	Ein Alarmtext, der für die <i>Firewallregel</i> hinzugefügt wurde. Wenn der Alarm wegen eines Eindringungsversuchs ausgelöst wurde, enthält das Feld eine Information über das <i>Muster</i> des Eindringungsversuchs.

5. Um Alarmdetails anzuzeigen, wählen Sie den Alarm aus und klicken Sie auf **Details**.

6. Um zum vorherigen oder zum nächsten Alarm zu gelangen, klicken Sie auf die Schaltfläche **Zurück** oder **Weiter**.
7. Klicken Sie nach der Ansicht der Details auf **Schließen**, um das Dialogfeld mit den Details der **Firewall-Alarme** zu schließen.
8. Klicken Sie auf **Schließen**, um das Dialogfeld mit der Liste der **Firewall-Alarme** zu schließen.

Informationen in den Alarmmeldungen der Firewall

Die Alarmmeldungen der Firewall enthalten Informationen über den Datenverkehr, der die Meldung ausgelöst hat.

Eine Alarmmeldung der Firewall enthält die folgenden Informationen:

Feld	Beschreibung
Beschreibung	Ein Alarmtext, der für die <i>Firewallregel</i> hinzugefügt wurde. Wenn der Alarm durch einen Eindringungsversuch ausgelöst wurde, zeigt der Alarm Informationen über das <i>Muster</i> des Eindringungsversuchs an.
Aktion	Zeigt, was passiert ist, z. B., dass die <i>Firewall</i> den Datenverkehr blockiert oder zugelassen hat.
Zeit	Das Datum und den Zeitpunkt, zu dem der Alarm generiert wurde.
Richtung	Zeigt, ob der Datenverkehr eingehend oder ausgehend ist (von einem Remote-Computer an Ihren Computer oder umgekehrt).
Protokoll	Das verwendete <i>IP-Protokoll</i> .
Dienste	Zeigt die <i>Firewalldienste</i> , mit denen der Datenverkehr übereinstimmte.
Remote-Adresse	Die <i>IP-Adresse</i> des Remote-Computers.
Remote-Port	Der <i>Port</i> auf dem Remote-Computer.
Lokale Adresse	Die <i>IP-Adresse</i> Ihres eigenen Computers.
Lokaler Port	Der <i>Port</i> auf Ihrem eigenen Computer.

Aktionsprotokoll anzeigen

Wenn ein Programm, beispielsweise ein Netzwerkspiel, nicht funktioniert, können Sie im Aktionsprotokoll prüfen, ob die Anwendungssteuerung das Programm daran gehindert hat, eine Internetverbindung herzustellen.

Das *Aktionsprotokoll* ist eine Textdatei (*action.log*) die automatisch Daten über die Netzwerkverbindungen erfasst. Die Maximalgröße der Datei beträgt 10 MB. Sobald die Datei voll ist, werden die alten Protokolleinträge gelöscht.

So zeigen Sie das *Aktionsprotokoll* an:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung ► Protokollfunktion**.
3. Klicken Sie auf **Aktionsprotokoll anzeigen**.

Das *Aktionsprotokoll* wird im standardmäßigen Texteditor oder in einem Anzeigeprogramm wie z. B. Notepad geöffnet.

Aktionsprotokoll – Beispiele

Das *Aktionsprotokoll* enthält Informationen über geöffnete Verbindungen und Änderungen der *Firewallregeln*.

Öffnen einer Verbindung

Das folgende Beispiel zeigt einen Protokolleintrag, der erstellt wird, wenn Sie den Internet Explorer starten und eine Verbindung zu einem *HTTP-Server* herstellen:

```
2009-03-07 T13:07:15+02:00 Info
C:\PROGRA~1\INTERN~1\iexplore.exe zulass nach außen
verbinden 6 10.0.1.14 80
```

1. Datum
2. Zeit
3. Typ
4. Interner Grund
5. Programm

6. Steuerung
7. Netzwerkaktion
8. Protokoll
9. Remote IP Adresse
10. Remote Port

Verbindung wird empfangen

Das folgende Beispiel zeigt einen Protokolleintrag, der erzeugt wird, wenn ein Programm auf Ihrem Computer als *Server* für andere Computer agiert. Diese anderen Computer können über den von der Anwendungssteuerung auf Ihrem Computer geöffneten *Port* eine Verbindung zu diesem *Server*-Programm herstellen (dynamische *Firewallregel*):

```
2009-03-04 T13:08:15+02:00 Info appl control unbekannt  
zulassen empfangen 17 10.0.1.146 138
```

1. Datum
2. Zeit
3. Typ
4. Interner Grund
5. Programm
6. Steuerung
7. Netzwerkaktion
8. Protokoll
9. Remote IP Adresse
10. Lokaler Port

Hinzufügen und Entfernen einer dynamischen *Firewallregel*

Das folgende Beispiel zeigt zwei *Firewallregel*-Protokolleinträge:

- Der erste Eintrag zeigt, dass die Anwendungssteuerung eine dynamische *Firewallregel* hinzugefügt hat. Diese Regel erlaubt eine temporäre, eingehende Verbindung für ein Programm.
- Der zweite Eintrag zeigt, dass die Anwendungssteuerung die dynamische *Firewallregel* entfernt hat und dass die Verbindung beendet wurde.

2009-03-05 T13:06:59+02:00 Info dynamische Regel hinzugefügt 0.0.0.0
255.255.255.0 0 65535 371 371 zulassen

2009-03-05 T13:07:23+02:00 Info dynamische Regel entfernt 0.0.0.0
255.255.255.0 0 65535 371 371 zulassen

1. Datum
2. Zeit
3. Warnungstyp
4. Regeltyp
5. Aktion
6. Minimaler Adressbereich für Remote-Adresse
7. Maximaler Adressbereich für Remote-IP-Adresse
8. Remote-Port-Bereich (von)
9. Remote-Port-Bereich (bis)
10. Lokaler Port -Bereich (von)
11. Lokaler Port -Bereich (bis)
12. Regelaktion

Datenverkehr im Netzwerk mit Paketprotokollierung überwachen

Sie können bei Bedarf die Paketprotokollierung starten, um Informationen über den *IP*-Datenverkehr im Netzwerk aufzuzeichnen.

Wie funktioniert die Paketprotokollierung?

Das *Paketprotokoll* sammelt Informationen zum *IP*-Netzwerkdatenverkehr.

Standardmäßig ist die Paketprotokollierung ausgeschaltet. Die Paketprotokollierung richtet sich in erster Linie an erfahrene Benutzer, die mit Computernetzwerken vertraut sind.

Sie können die Paketprotokollierung wieder einschalten, wenn Sie Ihre eigenen *Firewallregeln* erstellt haben und überprüfen wollen, wie diese den Datenverkehr blockieren. Sie können dies auch tun, wenn Sie schädliche Netzwerkaktivitäten vermuten.

Die Informationen werden in 10 Dateien gesammelt (`packetlog.0`-`packetlog.9`). Jedes Mal, wenn Sie die Protokollierung einschalten, wird das *Paketprotokoll* in einer neuen Datei gespeichert. Wenn die zehnte Datei voll ist, wird das Protokoll wieder in der ersten Datei gespeichert. So können Sie sich die vorhergehenden Protokolle ansehen, während ein neues Protokoll erstellt wird.

Zusätzlich zum *IP*-Datenverkehr sammelt das *Paketprotokoll* auch Informationen über andere Typen von Netzwerkdatenverkehr, z. B. über die *Protokolle*, die Ihr *lokales Netzwerk* (LAN) benötigt. Zu diesen Informationen gehören z. B. die *Routing*-Daten.

Das *Paketprotokoll* ist im *Hexadezimalformat* und unterstützt das *tcpdump*-Format. So können Sie die *Protokolldateien* auch in einem Programm für die *Paketprotokollierung* öffnen, das nicht ihr standardmäßiger Viewer für das *Paketprotokoll* ist. Sie können außerdem ein Programm zur Netzwerk-Protokoll-Analyse verwenden, um die Inhalte weiter zu analysieren.

Paketprotokollierung starten

Wenn Sie den Verdacht haben, dass bösartige Netzwerkaktivitäten stattfinden, oder wenn z. B. ein Netzwerkspiel nicht mehr funktioniert, können Sie die Paketprotokollierung starten.

So starten Sie die Protokollierung:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Netzwerkverbindung** ► **Protokollfunktion**.
3. Verwenden Sie die vorgeschlagenen Werte für die **Protokollzeit** und die Dateigröße der Felder **Protokollzeit** und **Maximalgröße der Protokolldatei** und geben Sie die Werte in die Felder **Typ** und **Code** ein. Wenn Sie möchten, können Sie die Werte auch ändern.
4. Klicken Sie auf **Protokollierung starten**. Zur Liste der Protokolldateien wird eine neue Datei hinzugefügt. Die Größe der Datei steigt an, je mehr Informationen gesammelt werden. Wenn die Liste bereits 10 Protokolldateien enthält, wird das nächste Protokoll in eine vorhandene Datei geschrieben.

- Um die Protokollierung manuell zu stoppen, klicken Sie auf **Protokollierung starten**. Die Protokollierung wird automatisch nach Ablauf der vorgegebenen Protokollzeit beendet bzw. wenn die Maximalgröße der Protokolldatei erreicht ist.

Eine neue Protokolldatei wird erzeugt und zur Liste der Protokolldateien hinzugefügt.

Paketprotokoll anzeigen

Nachdem Sie ein *Paketprotokoll* erstellt haben, können Sie es öffnen und anzeigen.

So zeigen Sie das *Paketprotokoll* an:

- Klicken Sie auf der Startseite auf **Einstellungen**.
- Wählen Sie **Netzwerkverbindung** ► **Protokollfunktion**.
- Wählen Sie das *Paketprotokoll* aus, das Sie anzeigen möchten, und klicken Sie auf **Details**.
Der standardmäßige *Paketprotokoll*-Viewer wird geöffnet. Im oberen Fensterbereich werden alle protokollierten Verbindungen angezeigt.

Sie können folgende Informationen anzeigen:

Feld	Beschreibung
Zeit	Zeit in Sekunden ab dem Augenblick, in dem die Protokollierung begann. Wenn die definierte Protokollierungszeit 60 Sekunden beträgt, liegt die Startzeit für das erste <i>Paket</i> nahe bei 0 Sekunden, und die Startzeit für das letzte <i>Paket</i> nahe bei 60 Sekunden.
Verwerfen (Verz.)	Zeigt an, ob die <i>Firewall</i> das <i>Paket</i> durchgelassen oder verworfen hat, und zeigt die Richtung des <i>Pakets</i> an: <ul style="list-style-type: none"> • Nein : Zugelassen: <i>Paket</i>. • Ja : Verwarf <i>Paket</i>.

Feld	Beschreibung
	<ul style="list-style-type: none"> • Eingehend : Eingehendes <i>Paket</i>. • Ausgehend : Ausgehendes <i>Paket</i>. <p>Diese Informationen sind nicht verfügbar, wenn Sie die Datei in einem anderen Paketprotokollierungsprogramm anzeigen als dem standardmäßigen <i>Paketprotokoll -Viewer</i>.</p>
Protokoll	Das verwendete <i>IP-Protokoll</i> .
Ursprung	Ursprungs- <i>IP-Adresse</i> des <i>Pakets</i> .
Ziel	Ziel- <i>IP-Adresse</i> des <i>Pakets</i> .
ID	<i>IP</i> <i>Paket</i> -Kopfzeileninformationen: Kennung des <i>Pakets</i> .
TTL	<i>IP</i> <i>Paket</i> -Kopfzeileninformationen: Der Wert <i>Lebensdauer</i> des <i>Pakets</i> definiert die Anzahl der Netzwerkgeräte, die das <i>Paket</i> durchlaufen kann, bevor es abgeworfen wird.
Len	<i>IP</i> <i>Paket</i> Header-Informationen: Gesamtlänge des <i>Pakets</i> .
Beschreibung	Beschreibung des <i>Pakets</i> .

Im rechten Fensterbereich werden die Datenverkehrstypen und die zugehörigen Definitionen angezeigt.

Im unteren Fensterbereich werden die Informationen in den Formaten *Hexadezimal* und *ASCII* angezeigt.

Wenn Sie alle Arten von Netzwerkverkehr anzeigen möchten (und nicht nur *IP*-Datenverkehr), müssen Sie das Kontrollkästchen **Nicht-IP-Datenverkehr filtern** deaktivieren.

Sichere Nutzung des Internets

Themen:

- *Was ist Surfschutz*
- *Spam blockieren*

Surfschutz

- Sie helfen Ihnen beim sicheren Surfen im Internet, indem sie Ihnen Sicherheitsbewertungen für Webseiten auf Ihrem Browser zur Verfügung stellen.
- Sie blockieren den Zugriff auf Webseiten, die als schädlich eingestuft worden sind.
- Sie liefern Korrekturen für bekannte Schwachstellen in den auf Ihrem Computer installierten Programmen.

E-Mail-Filterung:

- Sie blockieren Spam- und Phishing-Mails oder E-Mails von bestimmten E-Mail-Adressen, die in Ihrem Postfach eingehen.
- Sie erlauben Ihnen, E-Mails von bestimmten E-Mail-Adressen entweder zu blockieren oder zuzulassen.

Was ist Surfschutz

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

Der Surfschutz ist ein Plug-In für den Browser, der Ihnen Sicherheitsbewertungen für Webseiten anzeigt, die in Ergebnissen von Suchmaschinen und in Webmails aufgelistet sind. Der Surfschutz ermöglicht es Ihnen, Webseiten zu meiden, die Sicherheitsgefährdungen wie Malware (Viren, Würmer, Trojaner) bergen könnten. Auf diese Weise helfen Ihnen die Sicherheitsbewertungen des Browser-Schutzes, den aktuellsten Internetgefahren aus dem Weg zu gehen, die von den üblichen Virenschutzprogrammen noch gar nicht erkannt werden.

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

Der Surfschutz verwendet darüberhinaus Exploit-Shields, von F-Secure entwickelte Korrekturen, die Sie vor Schwachstellen in den auf Ihrem Computer installierten Programmen schützen. Exploit-Shields identifizieren solche Schwachstellen und verhindern, dass schädliche Webseiten solche Schwachstellen nutzen, um z. B. einen nichtautorisierten Download zu erzwingen, der Malware enthält. Exploit-Shields schützen Sie nicht gegen Dateien, die Sie absichtlich heruntergeladen haben; vor dieser Art Sicherheitsrisiko schützt das Scannen nach Viren und Spyware.

Den Surfschutz ein- oder ausschalten

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

So wird der Surfschutz ein- oder ausgeschaltet:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Surfschutz**.
3. Wählen Sie eine der folgenden Optionen:
 - Um den Surfschutz einzuschalten, wählen Sie **Surfschutz einschalten** aus.
 - Um den Surfschutz auszuschalten, entfernen Sie die Auswahl **Browser-Schutz einschalten**.





4. Klicken Sie auf **OK** aus.
5. Wenn Ihr Browser geöffnet ist, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

Abhängig von Ihrer Auswahl ist der Surfschutz nun ein- oder ausgeschaltet.

Surfschutz-Sicherheitsbewertungen

Der Surfschutz zeigt Sicherheitsbewertungen für Webseiten in Ergebnislisten von Suchmaschinen und in Webmails.

Farbcodierte Symbole geben die Sicherheitsbewertung der aktuellen Webseite an (in der Symbolleiste) an. Die Sicherheitsbewertung von Links in Suchmaschinenergebnissen und in Webmails wird mit denselben Symbolen angezeigt. Es werden vier verschiedene farbcodierte Symbole verwendet:

- Grün  zeigt an, dass die Webseite sicher ist.
- Bersteinfarben  zeigt an, dass die Webseite verdächtig ist. Die Sicherheitsanalyse dieser Webseite hat ergeben, dass sie sicher ist, jedoch haben ihr einige Benutzer eine niedrige Sicherheitsbewertung erteilt.
- Rot  zeigt an, dass die Webseite schädlich ist.
- Grau  zeigt an, dass die Webseite nicht analysiert wurde und dass derzeit keine Informationen über sie vorliegen.

Sicherheitsbewertungen sind auf den folgenden Suchseiten verfügbar:

- Google
- MSN Live
- Yahoo

Sie können Sicherheitsbewertungen für Weblinks in den E-Mails einsehen, die Sie senden um empfangen. Sicherheitsbewertungen sind unter den folgenden E-Mail-Programmen verfügbar:

- Google
- MSN Hotmail Classic
- Yahoo Mail

Abhängig von Ihren Surfschutz-Einstellungen können Sie auch auf Webseiten zugreifen, die als unsicher eingestuft worden sind. Diese

Webseiten werden entweder automatisch blockiert oder Sie werden nur auf ein mögliches Risiko hingewiesen.


Beurteilungen für Weblinks anzeigen

Die Beurteilungen durch den Surfschutz können für Suchmaschinenergebnisse, Links in Webmail-Inhalten oder für beides angezeigt werden.

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

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet** ► **Surfschutz**.
3. Wählen oder entfernen Sie **Suchmaschinenergebnisse**.
Wenn diese Option ausgewählt ist, werden Surfschutz-Bewertungen für die von Suchmaschinen aufgelisteten Webseiten angezeigt (Google, Yahoo usw.).
4. Wählen oder entfernen Sie **Links in Webmails**.
Wenn diese Option ausgewählt ist, werden Surfschutz-Bewertungen für Links im Inhalt von Webmail-Nachrichten angezeigt (Gmail, Yahoo, Hotmail usw.).
5. Klicken Sie auf **OK**.

Sicherheitsbewertungen werden entsprechend den von Ihnen ausgewählten Einstellungen angezeigt.

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

Die Bewertung von Webseiten

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

So bewerten Sie eine Webseite:

1. Klicken Sie auf **Bericht** in der Symbolleiste.
Das Dialogfeld **Verständigen Sie uns** öffnet sich.
2. Wählen Sie eine Bewertung, um Ihre Einschätzung der Sicherheit einer Webseite abzugeben (**Sie ist sicher**, **Sie ist schädlich** oder **Ich weiß nicht**).

3. Klicken Sie auf **OK**.
Daraufhin öffnet sich das Dialogfeld **Bewertung bestätigen**.



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

4. Klicken Sie auf **OK**.

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

Schutz gegen schädlichen Inhalt

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

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

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet** ► **Surfschutz**.
3. Wählen oder entfernen Sie die Optionen unter **Zugriff blockieren wenn**:
 - Wählen oder entfernen Sie **Webseite enthält Exploit**. Wenn diese Option ausgewählt ist, blockiert der Surfschutz den Zugriff auf alle Webseiten, die Viren, Spyware oder Malware enthalten.
 - Wählen oder entfernen Sie **Webseite wurde als schädlich bewertet**. Wenn diese Option ausgewählt ist, blockiert der Surfschutz den Zugriff auf alle Webseiten, die von F-Secure als schädlich eingestuft wurden.
4. Klicken Sie auf **OK**.


Nun öffnet sich eine Surfschutz-Blockierungsseite, wann immer Sie zu einer Webseite navigieren, die auf der Grundlage der ausgewählten Einstellungen blockiert wird.

Sie ermöglichen den Zugriff auf vertrauenswürdige Webseiten.

Wenn der Surfschutz den Zugang zu einer Webseite, der Sie vertrauen und auf die Sie zugreifen möchten, blockiert, können Sie diese Seite als vertrauenswürdig definieren.

So fügen Sie eine vertrauenswürdige Webseite hinzu:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Surfschutz**.
3. Klicken Sie auf **Vertrauenswürdige Webseiten**.
Das Dialogfeld **Vertrauenswürdige Sites** öffnet sich und zeigt eine Liste aller Seiten an, die als vertrauenswürdige Seiten hinzugefügt worden sind.
4. Klicken Sie auf **Hinzufügen**.
In der Liste erscheint eine neue Zeile.
5. Geben Sie die Webadresse ein in das **Webseiten**-Feld:
 - Wenn Sie das Format "www.Beispiel.com/" verwenden, erlauben Sie den Zugriff auf diese bestimmte Seite, blockieren aber z. B. den Zugriff auf "www.Beispiel.com.us".
 - Wenn Sie das Format "www.Beispiel.com" verwenden, können Sie den Zugriff sowohl auf "www.Beispiel.com" wie auch auf "www.Beispiel.com.us" erlauben.

 **Hinweis:** Verwenden Sie diese Option mit Vorsicht, denn Sie definiert "www.Beispiel.com" und "www.Beispiel.com.us" gleichermaßen als vertrauenswürdige Seiten. Die zweite Seite ist u. U. sicher, aber es kann sich auch um eine gefälschte Seite handeln, die zum Phishing verwendet wird.
6. Klicken Sie auf **OK**.
Die Web-Adresse erscheint nun in der Liste **Vertrauenswürdige Sites**.
7. Klicken Sie auf **OK**.

Die Webseite wird nun nicht mehr blockiert, wenn Sie versuchen, auf sie zuzugreifen.

Exploit-Shields ein- oder ausschalten

Exploit-Shields sind Korrekturen für Schwachstellen in den auf Ihrem Computer installierten Programmen, und sie können von Hand ein- oder ausgeschaltet werden.

So schalten Sie Exploit-Shields ein oder aus:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Surfschutz**.
3. Klicken Sie auf **Exploit-Shields**.

Das Dialogfeld **Exploit-Shields** öffnet sich.

4. Wählen Sie die Exploit-Shields, die Sie ein- oder ausschalten möchten, aus der Liste.
5. Klicken Sie auf **OK**.

Was tun, wenn eine Webseite blockiert wird

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

Wenn eine Blockierungsseite erscheint:

1. Klicken Sie auf **Zur Homepage gehen**, um ohne Aufrufen der schädlichen Seite auf Ihre Homepage zuzugreifen.

Wir empfehlen Ihnen diese Maßnahme dringend.



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

2. Wenn Sie trotzdem auf die Webseite zugreifen möchten:
 - Wählen Sie **Diese Website niemals blockieren**, wenn Sie verhindern möchten, dass diese in Zukunft blockiert wird, und fügen Sie sie zur Liste der vertrauenswürdigen Websites hinzu. Klicken Sie dann auf **Ich möchte trotzdem auf diese Website zugreifen**.
 - Klicken Sie auf **Ich möchte trotzdem auf diese Website zugreifen**, ohne die Option **Diese Website niemals blockieren** auszuwählen, um nur dieses Mal auf die blockierte Website zuzugreifen (die Site bleibt für spätere Aufrufe blockiert).

Sicherheitszusammenfassung für eine Webseite

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

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

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

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

Spam blockieren


E-Mail-Filterung schützt Ihren Computer gegen *Spam* und *Phishing*-Mail-Nachrichten.

Eine E-Mail-Nachricht wird als *Spam* angesehen, wenn sie als Teil einer größeren Nachrichtensammlung verschickt wurde, wenn die Mails größtenteils den gleichen Inhalt haben und wenn die Empfänger nachweisbar keine Erlaubnis zum Senden der Nachricht erteilt haben. In Nachrichten vom Typ *Spam* und *Phishing* gehen erwünschte E-Mail-Nachrichten häufig unter. Auf folgende Weise können Sie Ihren Posteingang frei von Spam halten:

- Nutzen Sie E-Mail-Filter, um Spam und Phishing-Mails aufzuhalten und sie in *Spam*- und *Phishing* -Ordner zu verschieben;
- blockieren Sie Nachrichten von bestimmten E-Mail-Adressen, indem Sie diese zur Liste der gesperrten Absender hinzufügen;
- lassen Sie Nachrichten von vertrauenswürdigen E-Mail-Adressen zu, indem Sie diese zur Liste der zugelassenen Absender hinzufügen.

Wenn Sie eine Liste mit zugelassenen Sendern verwenden, erstellen Sie eine Liste mit Kontakten derjenigen von denen Sie E-Mail-Nachrichten erhalten möchten. Indem Sie Ihre Kontakte einer Liste zugelassener Sender hinzufügen, stellen Sie sicher, dass deren Nachrichten nicht im Spam- oder Phishing-Ordner landen.

Wenn Sie eine Liste gesperrter Absender verwenden, erstellen Sie eine Liste von Absendern, von denen Sie keine E-Mail-Nachrichten empfangen möchten. Indem Sie Absender zu einer Liste gesperrter Absender hinzufügen, stellen Sie sicher, dass deren Nachrichten in den Spam- oder Phishing-Ordner verschoben werden.

 **Hinweis:** Wenn die Adresse auch auf der Liste der zugelassenen Absender steht, wird die E-Mail-Nachricht nicht in den Spam- oder Phishing-Ordner verschoben, da die Liste der sicheren Absender Vorrang gegenüber der Liste der gesperrten Absender hat.

Einrichten meiner E-Mail-Programme zum Spam-Filtern

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

Das E-Mail-Filtern erstellt automatisch in Microsoft Outlook, Microsoft Outlook Express und Windows Mail (bei Windows Vista) einen *Spam*- und

einen *Phishing* -Ordner und Filterregeln. Wenn Sie ein anderes E-Mail-Programm verwenden, müssen Sie die Ordner und die Filterregeln von Hand erstellen. Wenn Sie mehrere E-Mail-Konten haben, müssen Sie für jedes Konto separate Filterregeln erstellen.



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

Wie funktioniert das Zusammenspiel zwischen meinen eigenen Filterregeln und den E-Mail-Filterregeln?

Das E-Mail-Filtern filtert E-Mail-Nachrichten auf Grundlage eigener Filterregeln. Es filtert keine E-Mail-Nachrichten, die einer von Ihnen erstellten Regel entsprechen. Wenn Sie beispielsweise eine Regel erstellt haben, die alle E-Mail-Nachrichten von einem Webstore in den Webstore-Ordner filtert, werden sowohl Ihre Nachrichten bezüglich Auftragsbestätigungen als auch Werbematerial aus diesem Webstore aus Ihrem Posteingang entfernt und in den Webstore-Ordner verschoben.

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

Microsoft E-Mail-Programme

Die E-Mail-Filterung legt in Microsoft Outlook, Microsoft Outlook Express und Windows Mail (bei Windows Vista) automatisch Ordner für *Spam* und *Phishing* -E-Mail-Nachrichten an und legt Filterregeln fest.

Leeren von Junk- und Phishing-Ordern

Sie können einstellen, dass *Spam*- und *Phishing* -Nachrichten, die älter sind als eine festgelegte Anzahl von Tagen, automatisch in Microsoft Outlook, Microsoft Outlook Express und Windows Mail (unter Windows Vista) gelöscht werden.

Wenn Sie eine E-Mail erwarten und diese nicht im Posteingang finden können, dann überprüfen Sie Ihren *Junk*- und *Phishing*-Ordner, um sicherzustellen, dass die Nachricht nicht in einen dieser Ordner verschoben wurde.

So stellen Sie ein, dass die Ordner *Junk* und *Phishing* automatisch geleert werden:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Verfahren Sie unter **Outlook Integration** wie folgt:
 - a) Wählen Sie **Leeren Sie den Junk-Ordner nach: [7] Tagen**.
 - b) Wählen Sie eine Zahl aus oder geben Sie eine ein, die festlegt, welche E-Mails in den Ordnern *Junk* und *Phishing* gelöscht werden. Wenn Sie z. B. festlegen, dass Nachrichten nach sieben Tagen aus den Ordnern gelöscht werden sollen, dann löscht das System automatisch Nachrichten, deren Sendedatum (im Header der Nachricht) mehr als sieben Tage zurückliegt.
4. Klicken Sie auf **OK**.

E-Mail-Programme Netscape und Mozilla Thunderbird

Folgen Sie der Anleitung, um Ordner für *Spam*- und *Phishing*-E-Mails sowie Filterregeln im Netscape- und Mozilla Thunderbird-E-Mail-Programm zu erstellen.

Erstellen von Ordnern für Spam- und Phishing-E-Mail-Nachrichten

Sie müssen in den Netscape- und Mozilla Thunderbird-E-Mail-Programmen *Ordner für Spam*- und *Phishing*-E-Mails von Hand erstellen.

So erstellen Sie die Ordner:

1. Wählen Sie **Datei ► Neu ► Ordner**, um einen neuen Ordner für *Spam*-E-Mails zu erstellen.
2. Verfahren Sie wie folgt:
 - a) Geben Sie *Spam* als neuen Ordnernamen ein.
 - b) Wählen Sie in der Liste **Anlegen als Unterordner von** das Verzeichnis in dem Ihr Posteingang zu finden ist.
3. Klicken Sie auf **OK**, um den neuen *Spam*-Ordner zu erstellen.
4. Wiederholen Sie die Schritte 1-3, um einen Ordner zu erstellen, in den *Phishing*-E-Mails gefiltert werden.
5. Überprüfen Sie, ob die neuen Ordner erstellt wurden und unter Ihrem Konto angezeigt werden.

Nachdem Sie die neuen Ordner erstellt haben, erstellen Sie Filterregeln für *Spam*- und *Phishing*-E-Mails.

Spam-Filterregel erstellen

Um *Spam* in den Ordner *Spam* zu filtern, müssen Sie in den E-Mail-Programmen Netscape und Mozilla Thunderbird eine Filterregel erstellen.

Bevor Sie eine *Spam*-Filterregel erstellen, müssen Sie den Ordner *Spam* erstellen.

So erstellen Sie eine *Spam* -Filterregel:

1. Wählen Sie **Extras ► Nachrichtenfilter**.
2. Klicken Sie auf **Neu**.
Das Dialogfeld **Filterregeln** wird geöffnet.
3. Geben Sie `Spam` als neuen Filternamen ein.
4. Erstellen Sie einen neuen Headereintrag, der zum Filtern von *Spam*-E-Mails verwendet wird:
 - a) Wählen Sie in der ersten Liste **Anpassen aus**.
 - b) Geben Sie im Dialogfeld **Header anpassen** `X-Spam-Flag` als neuen Nachrichten-Header ein und klicken sie auf **Hinzufügen**.
 - c) Klicken Sie auf **OK**.
5. Erstellen Sie eine neue Regel für das Verschieben einer E-Mail-Nachricht in den *Spam*-Ordner:
 - a) Wählen Sie in der ersten Liste **X-Spam-Flag** aus.
 - b) Wählen Sie in der zweiten Liste **enthält** aus.
 - c) Geben Sie im Textfeld `Yes` als den Text für die Übereinstimmung ein.
6. Verfahren Sie unter **Folgende Aktionen ausführen** wie folgt:
 - a) Wählen Sie in der ersten Liste **Nachricht verschieben nach** aus.
 - b) Wählen Sie in der zweiten Liste den zuvor erstellten *Spam*-Ordner aus.
7. Klicken Sie auf **OK**, um Ihre neue *Spam*-Filterregel zu bestätigen und um das Dialogfeld **Filterregeln** zu schließen.
8. Schließen Sie das Dialogfeld **Nachrichtenfilter**.

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

Erstellen einer Phishing-Filterregel

Um *Phishing*-E-Mails zu filtern, müssen Sie in den Netscape- und Mozilla Thunderbird-E-Mail-Programmen eine Filterregel erstellen.

Bevor Sie eine *Phishing*-Filterregel erstellen, müssen Sie den Ordner erstellen, in dem *Phishing*-E-Mails gefiltert werden.

So erstellen Sie die *Phishing*-Filterregel:

1. Wählen Sie **Extras ► Nachrichtenfilter**.
2. Klicken Sie auf **Neu**.
Das Dialogfeld **Filterregeln** wird geöffnet.
3. Geben Sie **Phishing** als neuen Filternamen ein.
4. Erstellen Sie einen neuen Header-Eintrag, der zum Filtern von *Phishing*-E-Mails verwendet wird:
 - a) Wählen Sie in der ersten Liste **Anpassen** aus.
 - b) Geben Sie im Dialogfeld **Headers anpassen** **X-FS-Classification-Phishing** als neuen Nachrichten-Header ein, und klicken Sie auf **Hinzufügen**.
 - c) Klicken Sie auf **OK**.
5. Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht in den *Phishing*-Ordner:
 - a) Wählen Sie in der ersten Liste **X-FS-Classification-Phishing** aus.
 - b) Wählen Sie in der zweiten Liste **enthält** aus.
 - c) Geben Sie im Textfeld **9** als Text für die Übereinstimmung ein.
6. Verfahren Sie unter **Folgende Aktionen ausführen** wie folgt:
 - a) Wählen Sie in der ersten Liste **Nachricht verschieben nach** aus.
 - b) Wählen Sie in der zweiten Liste den zuvor erstellten *Phishing*-Ordner aus.
7. Klicken Sie auf **OK**, um Ihre neue *Phishing*-Filterregel zu bestätigen und das Dialogfeld **Filterregeln** zu schließen.
8. Schließen Sie das Dialogfeld **Nachrichtenfilter**.

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


E-Mail-Programm Opera

Folgen Sie der Anleitung, um Ordner für *Spam*- und *Phishing*-E-Mails sowie Filterregeln im Opera-E-Mail-Programm zu erstellen.

Filter für Spam- und Phishing-E-Mail-Nachrichten erstellen

Im Opera E-Mail-Programm erstellt die E-Mail-Filterung automatisch den *Spam*-Filter.

Sie müssen einen *Phishing*-Filter manuell erstellen.

 **Hinweis:** *Spam*- und *Phishing*-Filter in Opera entsprechen den *Ordner für Spam*- und *Phishing*-E-Mails in anderen E-Mail-Programmen.

So erstellen Sie einen *Phishing*-Filter:


1. Öffnen Sie **Opera Mail**.
2. Klicken Sie im Bereich **Mail** mit der rechten Maustaste auf **Alle Nachrichten** und wählen Sie **Neuer Filter** aus.
3. Geben Sie einen Namen für den *Phishing*-Filter ein. Der neue **Filter** wird im Mailbereich unter Filter angezeigt.
4. Überprüfen Sie, ob die neuen *Spam*- und *Phishing*-**Filter** erstellt wurden und unter Filter angezeigt werden.

Nachdem Sie den Filter für *Phishing*-E-Mails erstellt haben, müssen Sie *Spam*- und *Phishing*-Filterregeln erstellen.

Spam-Filterregel erstellen

Um *Spam*-E-Mails zu filtern, müssen Sie im Opera-E-Mail-Programm eine Filterregel erstellen.

Bevor Sie eine *Spam*-Filterregel erstellen, müssen Sie sicherstellen, dass der *Spam*-Filter vorhanden ist.

 **Hinweis:** Die hier angegebenen Schritte beziehen sich auf Opera Version 9.9. Die Schritte für andere Versionen können leicht abweichen.

So erstellen Sie eine *Spam*-Filterregel:

1. Öffnen Sie **Opera Mail**.
2. Klicken Sie mit der rechten Maustaste auf Ihren *Spam*-Filter und wählen Sie **Eigenschaften**.
3. Wählen Sie die in der Liste angezeigte Standardregel.

Enthält die Liste keine Regeln, klicken sie auf **Regel hinzufügen**.

- Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht in den *Spam*-Filter:

- Wählen Sie in der ersten Liste **beliebiger Header** aus.
- Wählen Sie in der zweiten Liste **enthält** aus.
- Geben Sie im Textfeld *X-Spam-Flag: Yes* als Text für die Übereinstimmung ein.


Achten Sie darauf, dass sich zwischen dem Doppelpunkt und *Yes* ein Leerzeichen befinden muss.

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

Phishing-Filterregel erstellen

Um *Phishing*-E-Mails zu filtern, müssen Sie im Opera-E-Mail-Programm eine Filterregel erstellen.

Bevor Sie eine *Phishing*-Filterregel erstellen, müssen Sie sicherstellen, dass der Filter für *Phishing*-E-Mails vorhanden ist.

 **Hinweis:** Die hier angegebenen Schritte beziehen sich auf Opera Version 9.6. Die Schritte für andere Versionen können leicht abweichen.

So erstellen Sie eine *Phishing*-Filterregel:

- Öffnen Sie **Opera Mail**.
- Klicken Sie mit der rechten Maustaste auf Ihren *Phishing*-Filter und wählen Sie **Eigenschaften**.
- Wählen Sie die in der Liste angezeigte Standardregel.
Wenn die Liste keinerlei Regeln enthält, klicken Sie auf **Regel hinzufügen**.
- Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht durch den *Phishing*-Filter:
 - Wählen Sie in der ersten Liste **beliebiger Header** aus.
 - Wählen Sie in der zweiten Liste **enthält** aus.
 - Geben Sie im Textfeld *X-FS-Classification-Phishing: 9* als den Text für die Übereinstimmung ein.
Achten Sie darauf, dass sich zwischen dem Doppelpunkt und '9' ein Leerzeichen befinden muss.
- Klicken Sie auf **OK**, um Ihre neue *Phishing*-Filterregel zu bestätigen.

E-Mail-Programm Eudora

Befolgen Sie diese Anweisungen, um Ordner für *Spam* und *Phishing* sowie Filterregeln im E-Mail-Programm Eudora zu erstellen.

Erstellen von Ordnern für Spam- und Phishing-E-Mail-Nachrichten

Im Eudora-E-Mail-Programm müssen Sie einen *Spam*-Ordner von Hand erstellen.

So erstellen Sie einen *Spam*-Ordner:

1. Wählen Sie **Postfach ► Neu**.
2. Geben Sie *Spam* als den neuen Postfachnamen ein.
3. Wiederholen Sie die Schritte 1-2, um einen Ordner zu erstellen, in den *Phishing*-E-Mails gefiltert werden.
4. Prüfen Sie, ob die neuen Ordner erstellt wurden und unter den Eudora-Postfächern erscheinen.

Nachdem Sie die Ordner erstellt haben, erstellen Sie *Spam*- und *Phishing*-Filterregeln.

Spam-Filterregel erstellen

Um *Spam*-E-Mails zu filtern, müssen Sie im Eudora-E-Mail-Programm eine Filterregel erstellen.

Bevor Sie eine Filterregel erstellen, müssen Sie einen *Spam*-Ordner erstellen.

So erstellen Sie eine Spam-Filterregel:

1. Wählen Sie **Extras ► Filter**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie unter **Übereinstimmung** die Option **Eingehend**, um eingehende E-Mail-Nachrichten zu filtern.
4. Erstellen Sie eine Regel für das Verschieben einer E-Mail-Nachricht in den *Spam*-Ordner:
 - a) Geben Sie in der Liste **Header** *X-Spam-Flag* im Feld **Header** ein.
 - b) Wählen Sie in der zweiten Liste **enthält** aus.
 - c) Geben Sie **Yes** in das Feld ein.
5. Verfahren Sie unter **Aktion** wie folgt:

- a) Wählen Sie in der ersten Liste **Übertragen an** aus.
 - b) Klicken Sie auf **In** und wählen Sie in der Liste das *Spam*-Postfach aus.
6. Schließen Sie das Dialogfeld **Filter**.
 7. Klicken Sie auf **Ja**, um die Änderungen zu speichern.

Phishing-Filterregel erstellen

Um *Phishing*-E-Mails zu filtern, müssen Sie im E-Mail-Programm Eudora eine Filterregel erstellen.

Vor dem Erstellen einer *Phishing*-Filterregel müssen Sie den Ordner erstellen, in den *Phishing*-E-Mails gefiltert werden.

So erstellen Sie eine *Phishing*-Filterregel:

1. Wählen Sie **Extras ► Filter**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie unter **Übereinstimmung** die Option **Eingehend** aus, um eingehende E-Mail-Nachrichten zu filtern.
4. Erstellen Sie eine Regel, um eine E-Mail-Nachricht in den *Phishing*-Ordner zu verschieben:
 - a) Geben Sie in der Header-Liste `X-FS-Classification-Phishing` in das Feld "Header" ein.
 - b) Wählen Sie in der zweiten Liste **enthält** aus.
 - c) Geben Sie in dem Feld `9` ein.
5. Verfahren Sie unter **Aktion** wie folgt:
 - a) Wählen Sie in der ersten Liste **Übertragen an** aus.
 - b) Klicken Sie auf **In** und wählen Sie in der Liste das *Phishing*-Postfach aus.
6. Schließen Sie das Dialogfeld **Filter**.
7. Klicken Sie auf **Ja**, um die Änderungen zu speichern.

Was passiert, wenn ich zahlreiche Spammachrichten erhalte?

Wenn Sie in Ihrem Posteingang viele *Spam*-E-Mails erhalten, sollten Sie einige Einstellungen überprüfen.

Gehen Sie wie folgt vor, um den Umfang der *Spam*-E-Mails zu reduzieren, die in Ihrem Posteingang ankommen:

1. Überprüfen Sie, ob die E-Mail-Filterung angeschaltet ist:
 - a) Klicken Sie auf der Startseite auf **Einstellungen**.
 - b) Wählen Sie **Internet ► E-Mail-Filterung**.
 - c) Wählen Sie **E-Mail-Filterung einschalten** wenn dies nicht schon geschehen ist.

2. Stellen Sie sicher, dass *Spam*- und *Phishing*-Ordner sowie Filterregeln in Ihrem E-Mail-Programm erstellt wurden.

3. Prüfen Sie, ob in Ihrem E-Mail-Programm das POP3-Protokoll ausgewählt ist.
 Die E-Mail-Filterung unterstützt nur das POP3-Protokoll. Weitere Informationen zum erforderlichen Protokoll erhalten Sie von Ihrem Internet Service Provider.

4. Stellen Sie sicher, dass die E-Mail-Filterung am gleichen Port wie Ihr E-Mail-Programm angeschlossen ist.
 Den Port müssen Sie nur ändern, falls Ihr E-Mail-Programm keinen standardmäßigen Port verwendet.
 - a) Klicken Sie auf der Startseite auf **Einstellungen**.
 - b) Wählen Sie **Internet ► Viren- und Spyware-Scan**.
 - c) Klicken Sie auf **Protokolle**.
 - d) Prüfen Sie unter **Port-Nummern**, ob die für das POP3-Protokoll verwendete Portnummer mit der übereinstimmt, die Ihr E-Mail-Programm verwendet.
 Weitere Informationen über den für das POP3-Protokoll verwendeten Port erhalten Sie von Ihrem Internet Service Provider.
 - e) Klicken Sie auf **OK**.

5. Prüfen Sie, ob Ihre Filterstufe streng genug ist:
 - a) Klicken Sie auf der Startseite auf **Einstellungen**.
 - b) Wählen Sie **Internet ► E-Mail-Filterung**.
 - c) Wählen Sie unter **Spam- und Phishing-Filtermodus** die Option **Aggressiv** aus, sofern sie nicht ausgewählt ist.
 - d) Klicken Sie auf **OK**.

Informationen zu Spam und Phishing-Filterstufen

Spam-Filterstufen bestimmen wie streng E-Mail-Filter *Spam* und *Phishing* -E-Mail-Nachrichten blocken.

Wenn beim E-Mail-Filtern *Spam* oder *Phishing*-E-Mail-Nachrichten ermittelt werden, werden diese, je nach gewählter Filterstufe, in einen besonderen *Spam*- oder *Phishing*-Ordner verschoben. Wenn Sie der Ansicht sind, dass zu viele E-Mail-Nachrichten vom Typ *Spam* in Ihrem Posteingang landen, wählen Sie eine strengere Filterungsstufe. Wenn Sie der Meinung sind, dass zu viele seriöse E-Mail-Nachrichten gefiltert werden, wählen Sie eine weniger strikte Stufe.

Sie können eine der folgenden vordefinierten Stufen auswählen:

- **Aggressiv** - wählen Sie diese Stufe aus, wenn Sie viele Spam-E-Mails erhalten und davon so viele wie möglich blockieren möchten.
- **Mittel** - (Standardeinstellung) wählen Sie diese Stufe, wenn Sie nicht viele *Spam*-E-Mails erhalten oder wenn die an Sie gerichteten seriösen E-Mail-Nachrichten nicht als *Spam* gefiltert werden.

Verändern der Filterstufe für Spam und Phishing

Durch die Auswahl einer strengeren Filterstufe, können Sie die Menge an *Spam* in Ihrem Posteingang reduzieren.

So ändern Sie die Filterstufe:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Wählen Sie unter **Spam- und Phishing-Filtermodus** eine der vordefinierten Filterstufen aus.
4. Klicken Sie auf **OK**.

Spam- und Phishing-Lernsystem zurücksetzen.

Wenn die E-Mail-Filterung Nachrichten scannt, lernt sie automatisch *Spam* und *Phishing*-E-Mail-Nachrichten genauer zu erkennen.



Hinweis: Setzen Sie das Lernsystem nur dann zurück, wenn Sie aufgefordert werden, dies zu tun.

Manchmal treten Probleme im Lernprozess auf. Dann kann es passieren, dass anschließend seriöse E-Mails als *Spam* oder *Phishing* erkannt werden. Sie können das Lernsystem zurücksetzen, um die erlernten Regeln zu löschen.

So stellen Sie die Standardeinstellungen wieder her:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Klicken Sie auf **Filter zurücksetzen**.
4. Klicken Sie in der Bestätigungsmeldung auf **OK**.

Das Lernsystem wird zurückgesetzt und das System verwendet die Standardeinstellungen.

Den Port für E-Mail-Protokolle festlegen

Wenn Ihr E-Mail-Programm keinen Standardport verwendet, müssen Sie den Port ändern, der auf *Spam* überprüft wird.

So legen Sie die Ports fest:

1. Starten Sie Ihre E-Mail-Anwendung und prüfen Sie, welche Ports für das Senden und Empfangen von E-Mails verwendet werden. Notieren Sie die Portnummern.



Hinweis: Andere E-Mail-Protokolle als POP3 werden nicht unterstützt.

2. Öffnen Sie das Produkt.
3. Klicken Sie auf der Startseite auf **Einstellungen**.
4. Wählen Sie **Internet ► E-Mail-Filterung**.
5. Klicken Sie auf **Protokolle anzeigen**.
6. Geben Sie die Portnummer für das *POP3*-E-Mail-Protokoll ein.
7. Klicken Sie auf **OK**.

Nachrichten von bestimmten E-Mail-Adressen zulassen oder sperren

Sie können Listen mit zugelassenen und gesperrten Absendern verwenden, um E-Mail-Nachrichten von bestimmten E-Mail-Adressen zuzulassen oder zu blockieren.

Mithilfe der Listen mit zugelassenen und gesperrten Absendern können Sie unerwünschte E-Mail-Nachrichten blockieren und andere E-Mail-Nachrichten durchlassen. Durch eine Liste der zugelassenen Absender wird die Anzahl der legitimen E-Mail-Nachrichten, die fälschlicherweise als E-Mail-Nachrichten vom Typ *Spam* oder *Phishing* identifiziert werden, reduziert.

E-Mail-Adressen bearbeiten, denen ich vertraue

Durch Hinzufügen von E-Mail-Adressen zu Ihrer Liste mit zugelassenen Absendern stellen Sie sicher, dass E-Mails von diesen Adressen durchgelassen werden und nie als *Spam* oder *Phishing*-Nachrichten behandelt werden.

Sie können E-Mail-Adressen oder ganze Domänen zu Ihrer Liste zugelassener Absender hinzufügen, sie bearbeiten oder entfernen. Fügen Sie beispielsweise `*@beispiel.com` zu Ihrer Liste zugelassener Absender hinzu, werden alle Nachrichten von `beispiel.com` zugelassen.

Bearbeiten Ihrer Liste vertrauenswürdiger E-Mail-Adressen:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Klicken Sie auf **Absender zulassen**.
Die Einstellungsseite **Zugelassene Absender** wird geöffnet.
4. Wählen Sie eine der folgenden Aktionen:
 - Hinzufügen einer neuen E-Mail-Adresse:
 - a) Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Absender/Domäne hinzufügen** öffnet sich.
 - b) Geben Sie im Feld **Adresse** die E-Mail-Adresse oder den Domännennamen an, dessen E-Mail-Nachrichten Sie zulassen möchten.

Sie können eine kurze Beschreibung für die neue Adresse im Feld **Beschreibung** hinzufügen.
 - c) Klicken Sie auf **OK**.
Die neue E-Mail-Adresse erscheint nun in der Liste zugelassener Absender.
 - Bearbeiten einer E-Mail-Adresse:
 - a) Wählen Sie in der Liste die E-Mail-Adresse aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
Das Dialogfeld **Absender/Domäne bearbeiten** öffnet sich.
 - b) Bearbeiten Sie die ausgewählte E-Mail-Adresse und klicken Sie auf **OK**.
 - Entfernen einer E-Mail-Adresse aus der Liste zugelassener Absender:


- a) Wählen Sie in der Liste die E-Mail-Adresse aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.
Die E-Mail-Adresse wird aus der Liste entfernt.

Kontakte in meine Liste zugelassener Absender importieren

Sie können Kontakte aus Ihren Adressbüchern in Microsoft Outlook, Microsoft Outlook Express und Windows Mail (bei Windows Vista) in die Liste zugelassener Absender importieren.

Durch den Import von Kontakten in Ihre Liste zugelassener Absender stellen Sie sicher, dass E-Mail-Nachrichten von diesen E-Mail-Adressen nicht fälschlicherweise als *Spam* oder *Phishing*-Mails gefiltert werden.

So importieren Sie Kontakte:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Klicken Sie auf **Absender zulassen**.
Die Seite **Zugelassene Absender** öffnet sich.
4. Klicken Sie auf **Kontakte aus Outlook oder Windows Mail importieren**.
Eine Meldung erscheint, die Sie darüber informiert, ob die Kontakte erfolgreich importiert wurden oder nicht.
 **Hinweis:** Falls das Importieren von Kontakten fehlschlägt, wird in der Meldung der Grund angegeben.
5. Klicken Sie auf **OK**, um die Meldung zu schließen.
6. Klicken Sie auf **OK**.

Die importierten Kontakte erscheinen nun in der Liste zugelassener Absender.

Blockieren von Nachrichten von bestimmten E-Mail-Adressen

E-Mail-Nachrichten von den Adressen oder Domänen auf Ihrer Liste mit gesperrten Absendern werden als *Spam* oder *Phishing* -Nachrichten behandelt und in die *Spam* - oder *Phishing*-Ordner gefiltert.

Sie können einzelne E-Mail-Adressen oder ganze Domains zu Ihrer Liste gesperrter Absender hinzufügen, sie bearbeiten oder entfernen. Wenn Sie

beispielsweise *@beispiel.com zu Ihrer Liste geblockter Absender hinzufügen, werden alle Nachrichten der Domäne beispiel.com geblockt.

Verändern der Liste gesperrter Absender:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► E-Mail-Filterung**.
3. Klicken Sie auf **Absender blockieren**.
4. Wählen Sie eine der folgenden Aktionen:
 - Zum Hinzufügen einer neuen E-Mail-Adresse:
 - a) Klicken Sie auf **Hinzufügen**.
Das Dialogfeld **Absender/Domäne hinzufügen** öffnet sich.
 - b) Geben Sie im Feld **Adresse** die E-Mail-Adresse oder den Domännennamen ein, deren E-Mail-Nachrichten Sie sperren möchten.

Im Feld **Beschreibung** können Sie eine kurze Beschreibung der neuen Adresse eingeben.
 - c) Klicken Sie auf **OK**.
Die neue E-Mail-Adresse wird jetzt in Ihrer Liste gesperrter Absender aufgeführt.
 - So bearbeiten Sie eine E-Mail-Adresse:
 - a) Wählen Sie in der Liste die E-Mail-Adresse aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
Das Dialogfeld **Absender/Domäne bearbeiten** öffnet sich.
 - b) Bearbeiten Sie die ausgewählte E-Mail-Adresse und klicken Sie auf **OK**.
 - Eine E-Mail-Adresse aus der Liste gesperrter Absender entfernen:
 - a) Wählen Sie in der Liste die E-Mail-Adresse aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.
Die E-Mail-Adresse wird aus der Liste entfernt.

Schutz gegen Phishing-Versuche

E-Mail-Filterung schützt Ihren Computer gegen *Phishing*-Versuche, die gefälschte E-Mail-Nachrichten nutzen, die aussehen, als ob sie von legitimierten Unternehmen kommen, um Ihre persönlichen Informationen zu entwenden.

Diese authentisch aussehenden Nachrichten, dienen dazu, Ihnen Ihre persönlichen Daten, z. B. Kontonummern, Passwörter oder Kreditkarten- und Sozialversicherungsnummern zu entlocken. Vertrauen Sie keinen E-Mail-Nachrichten, die als *Phishing* markiert sind.

Wenn Sie eine neue E-Mail-Nachricht erhalten, die als ein *Phishing*-Versuch erkannt wird, wird diese automatisch in den *Phishing*-Ordner verschoben.

In Microsoft Outlook, Outlook Express und Windows Mail (bei Windows Vista) werden automatisch ein *Phishing*-Ordner und eine Regel erstellt. Wenn Sie ein anderes E-Mail-Programm verwenden, müssen Sie den *Phishing*-Ordner und die Filterregel manuell erstellen.

Bei diesem Produkt ist Anti-Phishing Teil der E-Mail-Filterung.

Den Internetaufenthalt für Kinder sicher machen

Themen:

- *Was sind Browsingprofile?*
- *Wozu benötige ich Eltern- und Teenagerpasswörter?*
- *Passwörter erstellen oder ändern*
- *Zugriff auf das Internet bei aktivierter Kindersicherung*
- *Webseiten freigeben und sperren*
- *Online-Zeiten festlegen*
- *Wo Sie den Browser-Verlauf überprüfen können*
- *Was tun, wenn ich mein Elternpasswort vergessen habe?*

Das Internet ist voller interessanter Websites. Es gibt aber auch viele Risiken für Kinder, die das Internet nutzen. Viele Websites bieten Inhalte an, die nicht unbedingt für Kinder geeignet sind. Es kann passieren, dass Kinder mit ungeeigneten Inhalten konfrontiert werden oder dass sie belästigende Nachrichten per E-Mail oder in einem Chat erhalten. Sie können versehentlich Dateien herunterladen, die *Viren* enthalten, die den Computer möglicherweise beschädigen. Teenager sind gefährdet, da sie häufig unbeaufsichtigt online sind und an Online-Diskussionen teilnehmen.



Hinweis: Die Kindersicherung schützt Ihre Kinder vor Chat- und E-Mail-Programmen, die im Webbrowser ausgeführt werden. Mithilfe der Sicherheitskomponente "Anwendungssteuerung" können Sie den Zugriff Ihrer Kinder auf andere Chat- oder E-Mail-Programme sperren.

Durch das Erstellen von Browsingprofilen für Ihre Kinder können Sie bestimmen, welche Webseiten die Kinder aufsuchen dürfen. Außerdem können Sie die Zeit, die sie online verbringen dürfen, festlegen.

Was sind Browsingprofile?

Mit den Browsingprofilen der Kindersicherung können Sie die Onlinezeiten und die Webseiten festlegen, die für Ihre Teenager und kleineren Kinder geeignet sind.

Sie können Teenagern mehr Freiheiten beim Surfen im Internet einräumen und gleichzeitig die Onlineaktivitäten kleinerer Kinder stärker einschränken. Eltern-, Teenager- und Kinderprofile können Sie entweder bei der Installation mit dem Start-up-Assistenten definieren oder später auf der Seite **Kindersicherung** erstellen.

Profil für kleinere Kinder Das Profil für kleinere Kinder ist aktiv, wenn Sie das Produkt installiert oder den Computer neu gestartet haben. Wenn das Profil für kleinere Kinder aktiv ist, gilt Folgendes:

- Jeder, der den Computer verwendet, kann nur auf die Websites zugreifen, die Sie explizit zugelassen haben.
- Der Zugriff auf das Internet ist nur innerhalb der geplanten Zeit erlaubt.

Alle von Ihnen zugelassenen Websites werden auf der **Startseite der Kindersicherung** aufgeführt. Diese wird im Browser angezeigt, wenn das Profil für kleinere Kinder aktiv ist.

Teenagerprofil Wenn das Teenagerprofil aktiv ist, gilt Folgendes:

- Jeder, der den Computer verwendet, kann auf alle Websites zugreifen, ausgenommen solche, die gesperrte oder unerwünschte Inhalte haben, wie z. B. Drogen oder nicht jugendfreie Inhalte.
- Der Zugriff auf das Internet ist nur innerhalb der geplanten Zeit erlaubt.

Wenn Sie sowohl ein Profil für kleinere Kinder als auch eines für Teenager auf Ihrem Computer erstellt haben, müssen Sie Ihren Teenagern das von Ihnen erstellte Passwort für das Teenagerprofil mitteilen. Wenn das Passwort eingegeben wird, können Webseiten besucht werden, die:

- keine gesperrten Inhalte aufweisen und
- explizit von Ihnen zugelassen sind.



Hinweis: Wenn Sie den Webseitenfilter ausschalten, können Ihre Teenager Webseiten und Adressen unabhängig von ihren Inhalten aufsuchen.

Elternprofil Wenn das Elternprofil aktiv ist, kann jeder Benutzer des Computers ohne zeitliche oder inhaltliche Einschränkungen auf das Internet zugreifen. Beim Erstellen der Browsingprofile werden Sie aufgefordert, das Elternpasswort festzulegen. Das Elternpasswort wird benötigt, wenn Sie:

- die Benutzeroberfläche des Produkts öffnen,
- Produkteinstellungen anzeigen oder ändern,
- mit einer neuen Anwendung eine Verbindung zum Internet herstellen oder
- das Produkt deinstallieren.

Wozu benötige ich Eltern- und Teenagerpasswörter?

Sie benötigen das Eltern- und das Teenagerpasswort, um ohne die Einschränkungen im Internet zu surfen, die für das Teenager- bzw. Kinderprofil festgelegt wurden.

Wenn Sie sowohl das Browsingprofil für Eltern- als auch für Teenager erstellt haben, benötigen Sie eigene Passwörter für jedes Profil. Das Teenagerpasswort wird nur verwendet, wenn Sie ein Browsingprofil für kleinere Kinder und eines für Teenager erstellt haben. Das Profil für kleinere Kinder hat kein Passwort.


Teenager benötigen das Teenagerpasswort für den Zugriff auf Folgendes:

- Internet zu Zeiten, die Sie für kleine Kinder nicht freigegeben haben,
- Webseiten, die Sie für kleine Kinder nicht freigegeben haben, und
- Webseiten, die Sie speziell für Ihre Teenager zugelassen haben.

Sie benötigen das Elternpasswort, um:

- die Sicherheitseinstellungen des Produkts verändern,
- uneingeschränkt auf das Internet zugreifen,
- den Zeitplan festlegen, in dessen Rahmen Kinder im Internet surfen dürfen, und
- die Liste der Webseiten ändern, auf die Kinder zugreifen dürfen oder die für Kinder gesperrt sind.

Wenn Sie das Elternpasswort vergessen haben, können Sie es durch Eingabe Ihres Abonnementschlüssels zurücksetzen.

 **Hinweis:** Den Abonnementschlüssel haben Sie beim Kauf des Produkts erhalten. Bewahren Sie Ihren Abonnementschlüssel sicher auf, damit nur Sie das Passwort ändern können.

Berücksichtigen Sie beim Erstellen von Passwörtern folgende Punkte:

- Wählen Sie ein Passwort, das leicht zu merken, aber schwer zu erraten ist.
- Ein Passwort kann beliebige Zeichen enthalten.
- Ein Passwort muss aus 3 bis 80 Zeichen bestehen.
- Je nachdem, wie Ihr Produkt eingerichtet ist, muss Ihr Passwort eventuell eine bestimmte Zeichenanzahl übersteigen.

Passwörter erstellen oder ändern

Wenn Sie ein Browsingprofil erstellen, müssen Sie ein Passwort festlegen.

Berücksichtigen Sie bei der Festlegung von Passwörtern folgende Aspekte:

- Wählen Sie ein Passwort, das leicht zu merken, aber schwer zu erraten ist.
- Ein Passwort kann beliebige Zeichen enthalten.
- Ein Passwort muss aus 3 bis 80 Zeichen bestehen.
- Je nachdem, wie Ihr Produkt eingerichtet ist, muss Ihr Passwort eventuell eine bestimmte Zeichenanzahl übersteigen.

Elternpasswort ändern

Sie benötigen das *Elternpasswort*, um mit einer neuen Anwendung eine Verbindung zum Internet herzustellen oder um das Produkt zu deinstallieren.

Sie müssen das *Elternpasswort* festlegen, bevor Sie die Kindersicherung benutzen können. Wenn Sie die Kindersicherung zum ersten Mal einschalten, leitet Sie der Kindersicherungs-Assistent durch den Erstellungsvorgang für das *Elternpasswort*.

So ändern Sie das *Elternpasswort* zu einem späteren Zeitpunkt:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Klicken Sie auf **Passwörter ändern**.
4. Wählen Sie **Eltern**, wenn Sie gefragt werden, welches Passwort geändert werden soll.
5. Geben Sie ein neues *Elternpasswort* ein, und bestätigen Sie es.
6. Klicken Sie auf **Weiter**.
7. Geben Sie den Hinweis auf Ihr Passwort ein.

Der Hinweis auf Ihr Passwort soll Sie an Ihr Passwort erinnern. Denken Sie sich etwas aus, das Ihnen bei der Erinnerung hilft, andere Personen Ihr Passwort jedoch nicht erraten lässt. Bedenken Sie, dass dieser Hinweis auch Ihren Kindern angezeigt wird.

8. Klicken Sie auf **OK**.

Teenagerpasswort ändern

Wenn Sie sowohl das Profil für kleinere Kinder als auch das Teenager-Profil verwenden, können Teenager zu Zeiten, in denen es für kleinere Kinder verboten ist, das *Teenagerpasswort* für den Zugriff auf die für Teenager freigegebenen Websites benutzen.

Sie erstellen das *Teenagerpasswort*, wenn Sie die Kindersicherung zum ersten Mal einschalten und wenn Sie Profile für kleinere Kinder und für Teenager einrichten möchten. Der Kindersicherungs-Assistent leitet Sie durch den Erstellungsvorgang für das Teenagerpasswort.

So ändern Sie das *Teenagerpasswort* zu einem späteren Zeitpunkt:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Klicken Sie auf **Passwörter ändern**.
4. Wählen Sie **Jugendlicher**, wenn Sie gefragt werden, welches Passwort geändert werden soll.
5. Geben Sie ein neues *Teenagerpasswort* ein und bestätigen Sie es.
6. Klicken Sie auf **OK**.

Zugriff auf das Internet bei aktivierter Kindersicherung

Wenn Sie auf das Internet zugreifen, nachdem Sie die Browsingprofile erstellt haben, bestimmt das derzeit aktive Profil, wann Sie das Internet nutzen können und welche Webseiten Sie besuchen dürfen.

Nachdem Sie die Profile erstellt und Ihren Computer neu gestartet haben, wird das aktive Profil wie folgt bestimmt:

- Wenn Sie das Browsingprofil für kleinere Kinder erstellt haben, so wird dieses Profil nach Neustart des Computers zum aktiven Profil.
- Wenn Sie nur das Browsingprofil für Teenager erstellt haben, wird dieses nach Neustart des Computers zum aktiven Profil.


Ist das Profil für kleinere Kinder das aktive Profil, so wird die Startseite für die Kindersicherung in Ihrem Browser geöffnet. Ist das Teenagerprofil das aktive Profil, so können Sie das Internet wie üblich benutzen. Wenn Sie jedoch versuchen, das Internet vor oder nach dem Zeitraum zu benutzen, in dem die Nutzung für Teenager gestattet ist, wird die Seite der Zeitsperrenblockierung im Browser geöffnet.

Wenn Sie das Internet ohne Einschränkungen benutzen möchten, müssen Sie zum Elternprofil umschalten. Um in das Elternprofil umzuschalten, müssen Sie das Elternpasswort eingeben.


Zwischen den verschiedenen Browsingprofilen umschalten

Wenn beispielsweise Ihre kleineren Kinder das Internet verwenden möchten, können Sie auf das Kinderprofil umschalten, um sicherzustellen, dass Sie nur auf die Webseiten oder Internetpräsenzen zugreifen können, die Sie für sie für geeignet halten.

So wechseln Sie zu einem anderen Browsingprofil:

 **Hinweis:** Sie sollten immer daran denken, nach der Benutzung des Internets wieder auf das Kinderprofil umzuschalten, da Ihre Kinder sonst auf alle Sites zugreifen können, auf die Sie selbst Zugriff haben.

1. Sie können das Profil auf verschiedene Art umschalten:
 - Klicken Sie auf der Seite **Kindersicherung** auf **Aktivieren** gleich neben dem Namen des Profils, zu dem Sie umschalten möchten.

- Klicken Sie in Ihrem Browser auf der Startseite der Kindersicherung auf das gewünschte Profil.
 - Alternativ können Sie mit der rechten Maustaste auf das Symbol  klicken, Kindersicherung auswählen und anschließend auf das gewünschte Profil klicken.
2. Wenn Sie zum Eltern- oder Teenagerprofil wechseln, müssen Sie das Passwort für das jeweilige Profil eingeben. Wenn Sie vom Elternprofil zum Teenagerprofil oder vom Teenagerprofil zum Kinderprofil wechseln, ist die Eingabe eines Passworts nicht erforderlich .
 3. Schließen Sie nach dem Öffnen des Produkts das Einstellungsfenster. Während dieses Fenster geöffnet ist, können Ihre Kinder problemlos alle Einstellungen ändern, einschließlich der Einstellungen für die Kindersicherung.

Hierdurch wechseln Sie zum ausgewählten Profil, und Sie können Webseiten ansehen, die in dem aktivierten Profil zugelassen sind.

Webseiten freigeben und sperren

Mithilfe des Webseitenfilters können Sie steuern, welche Webseiten die Kinder besuchen dürfen.

Der Webseitenfilter filtert Webseiten auf der Grundlage von Inhaltskategorien. Er analysiert Webseiten, während sie heruntergeladen werden, und sucht nach verbotenen Schlüsselwörtern. Wenn eine Website Wörter enthält, die sich in der Liste der Schlüsselwörter befinden, blockiert der Webseitenfilter den Zugriff auf die Webseite. Der Webseitenfilter filtert außerdem Webseiten, indem er ihre Webadressen (URLs) mit den in seiner Datenbank vorhandenen gesperrten Adressen vergleicht. Wenn eine Webseite oder eine Website eine Webadresse besitzt, die sich in der Liste der gesperrten Adressen befindet, blockiert der Webseitenfilter des Zugriff auf die Webseite bzw. Website.

Hinweis: Keine Blockierungssoftware ist beim Filtern aller unerwünschten Sites 100-prozentig erfolgreich. Sie können den Webseitenfilter außer Kraft setzen:

- Wenn eine Website blockiert ist, die Ihr Kind anzeigen können soll, können Sie die betreffende Seite in die Liste der zugelassenen Websites aufnehmen.
- Wenn eine Website zugelassen ist, die Sie für Ihr Kind sperren möchten, können Sie die betreffende Seite in die Liste der gesperrten Websites aufnehmen.

Wenn es sich Ihrer Ansicht nach tatsächlich um einen Fehler des Webseitenfilters handelt, können Sie uns die Adresse der Website zukommen lassen, damit wir den Filter optimieren können. Nutzen Sie hierzu folgende Website: www.f-secure.com/samples.

Internetzugriff für kleinere Kinder beschränken

Sie können die gewünschte Filterebene für den Internetzugriff kleinerer Kinder bestimmen.

Für kleinere Kinder lässt der Webseitenfilter ausschließlich den Zugriff auf die Webseiten zu, die Sie zur Liste der zugelassenen Webseiten hinzugefügt haben.

Zugriff auf Webseiten ermöglichen

Sie können Ihren Kindern Zugang zu vertrauenswürdigen Websites und Seiten ermöglichen, indem Sie sie zur Liste der zugelassenen Websites hinzufügen.

So ermöglichen Sie Kindern den Zugriff auf Webseiten:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Wählen Sie die Registerkarte **Kleines Kind** aus.
4. Wählen Sie **Nur ausgewählte Seiten zulassen** aus.
Wird diese Option nicht ausgewählt, können kleinere Kinder alle Webseiten und Adressen aufrufen.
5. Klicken Sie auf **Webseiten anzeigen**.
6. Wählen Sie die Registerkarte **Zugelassen** aus.
7. Klicken Sie auf **Hinzufügen**.
8. Geben Sie im Dialogfeld **Webseite zulassen** die Adresse der Webseite ein, auf die Sie den Zugriff gestatten möchten.
 - Um den Zugriff auf die gesamte Website `www.example.com` zuzulassen, geben Sie `www.example.com` ein
 - Um den Zugriff auf einen Teil der Website `www.example.com` zuzulassen, geben Sie `www.example.com/subsite` ein
9. Klicken Sie auf **OK**.

Die Website wird zur Liste der zugelassenen Websites hinzugefügt. Kleinere Kinder können jetzt darauf zugreifen.

Zuvor freigegebene Webseiten sperren

Sie können verhindern, dass Kinder auf eine zugelassene Webseite zugreifen, indem Sie die Webseite aus der Liste der zugelassenen Websites entfernen.

Wenn Sie die Kindersicherung eingeschaltet haben und das Kinderprofil das gerade aktuelle Profil ist, wird die **Startseite der Kindersicherung** geöffnet, sobald Ihr Kind den Webbrowser startet. Die Seite enthält eine Liste der Websites oder Seiten, auf die Ihr Kind zugreifen kann. Sie können den Zugang zu einer auf der **Startseite der Kindersicherung** aufgeführten Webseite blockieren, indem Sie die Webseite aus der Liste der zugelassenen Websites entfernen.

So blockieren Sie den Zugang zu einer zugelassenen Webseite:

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

2. Wählen Sie **Internet ► Kindersicherung**.
3. Wählen Sie die Registerkarte **Kleines Kind**.
4. Klicken Sie auf **Websites anzeigen**.
Sie werden aufgefordert, Ihr Elternpasswort einzugeben.
5. Geben Sie Ihr Elternpasswort ein und klicken Sie auf **OK**.
6. Wählen Sie auf der Registerkarte **Zugelassen** des Fensters **Website-Liste** die Adresse der Webseite aus, für die Sie den Zugriff blockieren möchten.
7. Klicken Sie auf **Entfernen**.

Die Website wird aus der Liste der zugelassenen Websites entfernt.
Kleinere Kinder können auf die Webseite nicht mehr zugreifen.

Internetzugriff für Teenager beschränken

Sie können die Filterebene für den Internet-Zugriff von Teenagern auswählen.

Sie können den Webseitenfilter wie folgt einstellen:

- Filtern von Webseiten nach Kategorie oder
- Zugriff auf alle Webseiten zulassen und die Webseiten protokollieren, die die Teenager besuchen.



Hinweis: Sie sollten diese Option nur verwenden, wenn Sie Ihren Teenagern vertrauen. Sie können später überprüfen, welche Websites sie besucht haben. Wenn Sie unangemessene Websites finden, sollten Sie die automatische Filterung aktivieren.

Webseiten anhand ihres Inhalts sperren

Mit dem Webseitenfilter können Sie den Zugriff auf Websites und Webseiten zulassen, blockieren oder lediglich protokollieren.

So wählen Sie die Typen von Webinhalten aus, auf die Teenager zugreifen dürfen:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Wählen Sie die Registerkarte **Jugendlicher** aus.
4. Wählen Sie **Webseitenfilterung einschalten** aus.
5. Wählen Sie eine der folgenden Optionen aus:

- **Webseiten nach Inhalt blockieren** - Der Webseitenfilter analysiert Webseiten und blockiert den Zugang zu unerwünschten Webseiten anhand des Inhalts.



Hinweis: Klicken Sie auf **Kategorien anzeigen**, um ein Dialogfeld zu öffnen, in dem Sie neue Inhaltstypen einfügen oder vorhandene ausschließen können.

- **Zulassen und zur Liste der besuchten Webseiten hinzufügen** - erlaubt den Zugriff auf alle Webseiten, fügt aber alle Webseiten, die ihre Kinder besucht haben oder auf die sie zugreifen wollten, zur Websiteliste hinzu.

6. Klicken Sie auf **OK** .

Eine bestimmte Website sperren

Sie können den Zugriff auf eine Webseite sperren, die Sie für ungeeignet für Teenager halten.

Es kann Fälle geben, in denen Sie nicht mit dem Webseitenfilter übereinstimmen. Wenn Sie glauben, dass es sich dabei um einen echten Fehler des Webseitenfilters handelt, können Sie uns die Adresse der Website senden, damit wir den Filter verbessern können. Nutzen Sie hierfür folgende Website: www.f-secure.com/samples. So blockieren Sie den Zugriff auf eine Webseite:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet** ► **Kindersicherung**.
3. Klicken Sie auf **Website-Listen anzeigen**.
4. Wählen Sie **Jugendlicher**.
5. Klicken Sie auf die Registerkarte **Abgelehnt**.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie im Dialogfeld **Webseite sperren** die Adresse der Webseite ein, für die der Zugriff gesperrt werden soll.
 - Um den Zugriff auf die gesamte Website www.beispiel.com zu sperren, geben Sie ein: www.beispiel.com
 - Um den Zugriff auf einen Teil der Website www.beispiel.com zu sperren, geben Sie ein:
www.beispiel.com/untergeordnete_site

- Um den Zugriff auf Websites, wie beispielsweise `www2.beispiel.com`, `http://a123.beispiel.com`, zu sperren, geben Sie ein: `beispiel.com`

8. Klicken Sie auf **OK**.

Die Webseite wurde zur Liste der gesperrten Webseiten hinzugefügt und Ihre Teenager können nicht darauf zugreifen.

9. Klicken Sie auf **Schließen**.

Webseiten freigeben, die ich zuvor gesperrt hatte

Sie können zulassen, dass Teenager auf eine Webseite zugreifen, die aufgrund ihres Inhalts automatisch blockiert wurde.

Wenn die Kindersicherung eingeschaltet ist und ein Teenager versucht, eine Webseite aufzurufen, die gesperrte Inhalte enthält, wird die Seite **Sperrseite der Kindersicherung** angezeigt. Sie können den Zugriff auf diese Webseite erlauben, indem Sie sie zur Liste der zugelassenen Websites hinzufügen.

Wenn es sich Ihrer Ansicht nach tatsächlich um einen Fehler des Webseitenfilters handelt, können Sie uns die Adresse der Website zusenden, damit wir den Filter optimieren können. Nutzen Sie hierzu folgende Website: www.f-secure.com/samples. So erlauben Sie den Zugriff auf eine blockierte Webseite:

- 1.** Klicken Sie auf der **Seite durch Kindersicherung blockiert auf Diese Website für Jugendliche zulassen**.
- 2.** Geben Sie im Dialogfeld **Webseite zulassen** die Adresse der Webseite ein, auf die Sie den Zugriff gestatten möchten.
 - Um den Zugriff auf die gesamte Website `www.example.com` zuzulassen, geben Sie `www.example.com` ein
 - Um den Zugriff auf einen Teil der Website `www.example.com` zuzulassen, geben Sie `www.example.com/subsite` ein
- 3.** Klicken Sie auf **OK**.
Sie werden aufgefordert, Ihr Elternpasswort einzugeben.
- 4.** Geben Sie Ihr Elternpasswort ein und klicken Sie auf **OK**.


Die Website wird zur Liste der zugelassenen Websites hinzugefügt. Die Webseite wird erneut geladen und Teenager können darauf zugreifen.


Wie prüfe ich nach, ob Kinder nicht auf gesperrte Webseiten zugreifen können?

Sie können festlegen, dass Ihre Kinder nur die Webseiten oder Sites anzeigen können, die Sie dafür zulassen.

Diese Anleitung gilt nur, wenn Sie ein Kinderprofil, ein Teenagerprofil oder beide erstellt haben.

So können Sie festlegen, dass Ihre Kinder nicht auf unerwünschte Webseiten zugreifen:

1. So stellen Sie sicher, dass Ihre kleinen Kinder nur die Webseiten anzeigen können, die Sie der Liste **Zugelassene Websites** hinzugefügt haben:
 - a) Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das Symbol  und wählen Sie **Kindersicherung** ► **Kleines Kind**.
 - b) Öffnen Sie Ihren Browser.
Startseite der Kindersicherung sollte in Ihrem Browser geöffnet werden und alle Websites und Seiten auflisten, die Sie für kleine Kinder zugelassen haben.

2. So stellen Sie sicher, dass Teenager nicht auf Webseiten zugreifen können, die gesperrte oder unerwünschte Inhalte besitzen:
 - a) Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das Symbol  und wählen Sie dann **Kindersicherung** ► **Jugendlicher**.
 - b) Geben Sie das Teenagerpasswort ein.
Wenn Sie vom Elternprofil zum Teenagerprofil umschalten, ist kein Passwort erforderlich.
 - c) Starten Sie Ihren Browser und greifen Sie auf eine Website zu, für die Sie den Zugriff für Teenager blockiert haben.
Wenn Sie z. B. den Zugriff auf Chat- Websites blockiert haben und versuchen, auf eine bestimmte Seite der Kategorie Chat zuzugreifen, sollte in Ihrem Browser **Sperreseite der Kindersicherung** erscheinen und Ihnen mitteilen, dass die Webseite, auf die Sie zugreifen möchten, gesperrte Inhalte enthält und daher durch die Kindersicherung blockiert wird.

Online-Zeiten festlegen

Mithilfe der Zeitsperre können Sie steuern, wie viel Zeit Ihre Kinder im Internet verbringen.

Für Kinder und Teenager können Sie unterschiedliche Zeiten festlegen. Mit der Zeitsperre können Sie Folgendes steuern:

- Zu welchen Zeiten sich Ihre Kinder im Internet aufhalten dürfen. Sie können Ihren Teenagern beispielsweise erlauben, das Internet nur vor 20 Uhr zu benutzen.
- Wie lange Ihre Kinder im Internet surfen können. Sie können Ihren Kindern beispielsweise nur eine Stunde täglich im Internet erlauben.



Hinweis: Wenn Sie die Zeitsperre abschalten, können Ihre Kinder ohne zeitliche Begrenzung im Internet surfen.

Wenn die Zeitsperre die Verbindung mit dem Internet blockiert, sehen Ihre Kinder auf der **Sperrseite der Zeitsperre** im Webbrowser, wann sie wieder auf das Internet zugreifen können. Sie können die Surfzeiten verlängern, indem Sie das Elternpasswort eingeben und einen längeren Zeitraum zulassen.

Was versteht man unter der Kindersicherungs-Uhr?

Die Kindersicherungs-Uhr verhindert, dass Ihre Kinder die Computeruhr zurücksetzen, um sich längere Internetzeiten zu verschaffen.

Die Kindersicherungs-Uhr funktioniert unabhängig von der Computeruhr. Daher können die Kinder die Computeruhr nicht manipulieren. Im Elternprofil können Sie eine Zeitzone für die Kindersicherungs-Uhr auswählen. Die Uhr zeigt die aktuelle Uhrzeit in der ausgewählten Zeitzone an.

Tägliche Internetzeiten einschränken

Sie können die täglichen Internetzeiten für Ihre Kinder einschränken.

Sie können unterschiedliche Tageszeiten für kleinere Kinder und Teenager festlegen.

So schränken Sie die täglichen Internetzeiten ein:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Wählen Sie die Registerkarte **Jugendlicher** oder **Kleines Kind**.

4. Stellen Sie sicher, dass **Zeit, die im Internet verbracht wird, einschränken** ausgewählt ist.
5. Klicken Sie unter **Tägliche Internetzeit auf Bearbeiten**. Das Fenster **Zeitsperre** wird geöffnet.
6. Wenn Sie die Internetzeiten von montags bis freitags einschränken möchten, wählen Sie **Tägliche Internetzeiten an Werktagen**. Schieben Sie den Regler auf die maximale Stundenzahl, für die Ihr kleines Kind oder Ihr Teenager an einem Werktag auf das Internet zugreifen darf.
7. Wenn Sie die Internetzeiten von samstags bis sonntags einschränken möchten, wählen Sie **Tägliche Internetzeiten am Wochenende**. Schieben Sie den Regler auf die maximale Stundenzahl, für die Ihr kleines Kind oder Teenager an Samstagen oder Sonntagen auf das Internet zugreifen darf.
8. Klicken Sie auf **OK**.

Wenn Ihre Kinder die tägliche Internetzeit überschritten haben, ist der weitere Zugriff auf das Internet gesperrt.

Internetzeiten festlegen

Sie können die Zeiten auswählen, zu denen Ihre Kinder Zugriff auf das Internet haben sollen.

Sie können unterschiedliche Zeitbeschränkungen für kleinere Kinder und Teenager festlegen.

So legen Sie die täglichen Internetzeiten fest:


1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Wählen Sie die Registerkarte **Jugendlicher** oder **Kleines Kind**.
4. Stellen Sie sicher, dass **Zeit, die im Internet verbracht wird, einschränken** ausgewählt ist.
5. Klicken Sie unter **Festgelegte Internetzeiten auf Bearbeiten**. Das Fenster **Zeitsperre** wird angezeigt.
6. Wenn Sie die Internetzeiten von montags bis freitags einschränken möchten, wählen Sie **Internetnutzung an Werktagen einschränken** aus.
Klicken Sie auf der Zeitlinie auf die Stunden, in denen werktags kein Internetzugriff erlaubt ist, so dass eine rote Markierung erscheint.

7. Wenn Sie die Internetzeiten von samstags bis sonntags einschränken möchten, wählen Sie **Internetnutzung an Wochenenden einschränken** aus.
Klicken Sie auf der Zeitlinie auf die Stunden, in denen samstags und sonntags keine Internetnutzung erlaubt ist, so dass eine rote Markierung erscheint.
8. Klicken Sie auf **OK**.

Ihre Kinder können jetzt nur noch während der Stunden ohne rote Markierung auf das Internet zugreifen.

Verlängern der Surfzeiten

Sie können die Surfzeiten Ihrer Kinder verlängern, indem Sie das Elternpasswort eingeben und mehr Zeit einplanen.

 **Hinweis:** Hinweis für Kinder und Teenager: Nur die Eltern können die Internet-Surfzeit verlängern. Wenn du niemanden findest, der das Passwort der Eltern kennt, kannst du erst dann wieder im Internet surfen, wenn das Passwort wieder verfügbar ist.

1. Die Surfzeit kann nur geändert werden, wenn sie in Kürze abläuft oder bereits abgelaufen ist.
 - Wenn Ihre Internet-Surfzeit bald abläuft, wird ein Popup-Fenster angezeigt, in dem die verbleibende Internet-Surfzeit angezeigt wird. Wenn Sie auf dieses Popup-Fenster geklickt haben:
Klicken Sie im Dialogfeld **Kindersicherung**, das über das Popupfenster zur verbleibenden Zeit geöffnet wird, auf **Internet-Surfzeit verlängern**.
 - Wenn die zulässige Nutzungszeit bereits abgelaufen ist:
Klicken Sie auf der **Sperreseite der Zeitsperre**, die in Ihrem Browser geöffnet wird, auf **Internet-Nutzungszeit verlängern**.
2. Geben Sie im Dialogfeld Ihr Elternpasswort ein, und klicken Sie auf **OK**.
3. Legen Sie im Dialogfeld **Zeitsperre** eine Zeit fest und klicken Sie auf **OK**.


Die Zeitsperre erlaubt den Zugriff und blockiert ihn nach Ablauf der genehmigten Zeit erneut.

Wie prüfe ich nach, ob Kinder nur während der erlaubten Zeiten zugreifen?

Sie können prüfen, ob Ihre Kinder nur während der Zeiten surfen können, für die Sie dies erlaubt haben.

Diese Anleitung gilt nur, wenn Sie ein Kinderprofil, ein Teenagerprofil oder beide erstellt haben.

So prüfen Sie, ob Ihre Kinder ausschließlich innerhalb der zulässigen Zeiten surfen können:

1. Klicken Sie in der Windows-Systemleiste mit der rechten Maustaste auf das Symbol , wählen Sie **Kindersicherung** und dann entweder das Profil **Kleines Kind** oder **Jugendlicher**. Das ausgewählte Profil wird zum aktiven Profil.
2. Starten Sie Ihren Browser außerhalb der Surfzeiten, die Sie für kleinere Kinder festgelegt haben.

Seite für die Blockierung durch die Zeitsperre. Diese Seite sollte in Ihrem Browser angezeigt werden. Sie teilt Ihnen mit, dass der Zugriff auf das Internet gesperrt ist. Außerdem zeigt sie an, zu welcher Uhrzeit das Internet wieder benutzt werden darf.

Wo Sie den Browser-Verlauf überprüfen können

Die Liste der Webseiten zeigt Ihnen, welche Websites und Seiten Ihre Kinder besucht haben.

Wenn der Webseitenfilter eingeschaltet ist, werden die Webadressen (URLs) aller Webseiten, die Ihre Kinder besucht haben oder besuchen wollten, zu einer Liste hinzugefügt. Anhand der Websiteliste können Sie nachvollziehen, wo sich Ihre Kinder online aufhalten.

- | | |
|---------------------------|---|
| Zulässige Websites | Die Liste der zugelassenen Websites enthält sichere Webseiten, auf die Sie den Zugriff für Ihre Kinder zugelassen haben. Wenn Sie beispielsweise den Zugang zu Chat-Websites blockiert haben, können Sie den Zugriff auf eine bestimmte Seite oder Website der Kategorie Chat zulassen, indem Sie sie zur Liste der zugelassenen Websites hinzufügen. |
| Gesperrte Websites | Die Liste der gesperrten Websites enthält Webseiten, auf die Ihre Kinder nicht zugreifen sollen. Wenn Sie beispielsweise den Zugang zu Web-Mail-Websites zugelassen haben, können Sie den Zugriff auf eine bestimmte Seite oder Website in der Web-Mail-Kategorie blockieren, indem Sie sie zur Liste der gesperrten Websites hinzufügen. |
















Adressen von Webseiten sind farblich wie folgt kodiert:


- | | |
|------|--|
| Rot | Die Webseite oder Website befindet sich in der Liste der gesperrten Websites. |
| Grün | Die Webseite oder Website befindet sich in der Liste der zugelassenen Websites. |
| Blau | Die Website enthält sowohl Seiten, für die der Webseitenfilter den Zugriff genehmigt hat, als auch Seiten, für die er den Zugriff blockiert hat. |

Schwaz Die Website befindet sich weder in der Liste der zugelassenen Websites noch in der der gesperrten Websites und kann frei besucht werden.

Der Webseitenfilter filtert Webseiten auf der Grundlage von Inhaltskategorien. Das Inhaltskategoriesymbol neben der besuchten Webadresse zeigt an, aus welchem Grund der Zugriff auf die Webseite blockiert wurde.

Die Inhaltstypen, für die der Zugriff blockiert werden kann, lauten:

-  Nicht jugendfreie Inhalte
-  Blogs
-  Chat
-  Dating
-  Drogen
-  Foren
-  Glücksspiel
-  Hass
-  Soziale Netzwerke
-  Sport
-  Reisen
-  Unbekannt
-  Gewalt
-  Waffen
-  Webmail

 **Hinweis:** Keine Blockierungssoftware ist beim Filtern aller unerwünschten Sites 100-prozentig erfolgreich. Wenn es sich Ihrer Ansicht nach tatsächlich um einen Fehler des Webseitenfilters handelt, können Sie uns die Adresse der Website zukommen lassen, damit wir den Filter optimieren können. Nutzen Sie hierzu folgende Website: www.f-secure.com/samples.

Webseiten anzeigen, die meine Kinder besucht haben

Mit der Kindersicherung können Sie nachvollziehen, wo sich Ihre Kinder online aufhalten.

So zeigen Sie die Webseiten an, die Ihre Kinder besucht haben oder besuchen wollten:

1. Klicken Sie auf der Startseite auf **Einstellungen**.
2. Wählen Sie **Internet ► Kindersicherung**.
3. Klicken Sie auf **Website-Liste anzeigen**.
4. Wählen Sie im Fenster **Website-Liste** das Profil aus, dessen Surfverlauf Sie sich ansehen möchten.
5. Klicken Sie auf die Registerkarte **Verlauf**.

Die Registerkarte **Verlauf** zeigt alle Webseiten bzw. Websites, die Ihre Kinder oder Teenager besucht haben bzw. besuchen wollten. Das Symbol für den Inhaltstyp neben der besuchten Webadresse zeigt an, aus welchem Grund der Zugriff auf die Webseite blockiert wurde. Die Registerkarte zeigt außerdem, wie oft eine bestimmte Webseite besucht wurde und wann die Webseite zum letzten Mal besucht wurde.

Was tun, wenn ich mein Elternpasswort vergessen habe?

Wenn Sie das Elternpasswort vergessen haben, können Sie es durch Eingabe Ihres Abonnementschlüssels zurücksetzen.

So setzen Sie das Passwort zurück:

1. Öffnen Sie die Produktoberfläche.
Ein Dialogfeld wird geöffnet, in dem Sie aufgefordert werden, das Elternpasswort einzugeben.



Hinweis: Um einen Hinweis auf Ihr Passwort anzuzeigen, bewegen Sie den Mauszeiger zu **Passworthinweis anzeigen**. Dieser Hinweis soll Ihnen helfen, sich an Ihr Passwort zu erinnern.

2. Klicken Sie auf **Passwort vergessen?**.
3. Geben Sie die ersten vier Stellen Ihres Abonnementschlüssels ein und klicken Sie auf **Weiter**.

Den Abonnementschlüssel haben Sie beim Kauf des Produkts erhalten.

4. Verfahren Sie wie folgt:

- a) Geben Sie ein neues Passwort ein.



Hinweis: Beachten Sie beim Erstellen von Passwörtern Folgendes:

- Wählen Sie ein Passwort, das leicht zu merken, aber schwer zu erraten ist.
- Ein Passwort kann beliebige Zeichen enthalten.
- Ein Passwort muss aus 3 bis 80 Zeichen bestehen.
- Je nachdem, wie Ihr Produkt eingerichtet ist, muss Ihr Passwort eventuell eine bestimmte Zeichenanzahl übersteigen.

- b) Geben Sie das neue Passwort noch einmal ein, um es zu bestätigen.
- c) Klicken Sie auf "**Weiter**".
- d) Hinweis auf Ihr Passwort

Der Hinweis für Ihr Passwort soll Sie an Ihr Passwort erinnern. Denken Sie sich etwas aus, das Ihnen bei der Erinnerung hilft, andere Personen Ihr Passwort jedoch nicht erraten lässt. Bedenken Sie, dass dieser Hinweis auch Ihren Kindern angezeigt wird.

e) Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die besagt, dass Sie das Passwort erfolgreich zurückgesetzt haben.

5. Klicken Sie auf **OK**.

