Was ist F-Secure Internet Security?

Der preisgekrönte Schutz von F-Secure Internet Security ermöglicht Ihnen ein sorgenfreies Surfen im Netz, Online-Shopping und -Banking. F-Secure Internet Security schützt Sie und Ihre Computer automatisch vor Malware, Hackern und Identitätsdiebstahl. Wann immer Sie online sind, werden Ihre Bankgeschäfte mit dem Banking-Schutz geschützt und Sie können entscheiden, welche Inhalte Ihre Kinder sehen können und welche nicht.

Herunterladen der aktuellen Version von F-Secure Internet Security

Die aktuelle Version von F-Secure Internet Security steht unter
http://download.edv-buchversand.de/F-SecureNetworkInstaller.exe
zum Download für Sie bereit.

Wichtiges vorab, bevor Sie die Installation beginnen.

Verwenden Sie nur eine Sicherheitssoftware auf Ihrem Computer
Wir empfehlen Ihnen, lediglich eine zuverlässige Sicherheitssoftware zu betreiben. Eine solche Software muss Dateien öffnen, um sie auf Viren scannen zu können. Wenn nun ein weiteres Sicherheitsprogramm zur selben Zeit auf dieselbe Datei zugreift, muss dieses auf die Freigabe der Datei warten. Dadurch entstehen häufig Probleme beim Programmstart. Schlimmstenfalls kann auch das gesamte System abstürzen.

F-Secure Internet Security erkennt und entfernt die Sicherheits- und Firewall-Software der bekanntesten Anbieter automatisch bei der Installation.
Sollte bei der Deinstallation ein Fehler auftreten, müssen Sie die andere Software manuell entfernen. Dies können Sie auch bereits vor Beginn der Installation tun.

Ende des Supports für Windows XP und Vista.

Der Windows XP-Support für F-Secure Internet Security oder AntiVirus ist im Juni 2016 nach einer Support-Phase für das Betriebssystem eingestellt. Microsoft hat das Ende seines Supports für Windows XP bereits im April 2014 bekanntgegeben.

Nachdem der Support eingestellt wird, können wir den Schutz Ihres Computers nicht weiter sicherstellen, da Ihr Computer unter Umständen anfälliger für Sicherheitsprobleme ist. Unsere Produkte funktionieren weiterhin auf Ihrem Computer. Wenn Sie jedoch Windows XP verwenden, erhalten Sie keine Sicherheitsupdates mehr für das Betriebssystem. Zudem werden künftige Versionen unsere Heimsicherheitsprodukte nicht länger kompatibel mit Windows XP sein. Daher werden neu installierte Versionen dieser Produkte auf diesem Betriebssystem nicht mehr funktionieren.

Wir empfehlen Ihnen, ein Upgrade des Betriebssystems Ihres Computers auf eine Windows-Version vorzunehmen, die Sicherheits-Updates von Microsoft erhält. Die aktuellste Version des Betriebssystems bietet immer auch die besten Schutztechnologien und wird vom Anbieter vollständig gewartet. So erhalten Sie mit der neusten Version frühzeitig Sicherheits-Updates und -Verbesserungen.

Mit Erscheinen der Version 17.0 wurde zusätzlich die Unterstützung für „Vista“ eingestellt.

Installation von F-Secure Internet Security

Die Installationsdatei kann unter folgendem Link heruntergeladen werden:
http://download.edv-buchversand.de/F-SecureNetworkInstaller.exe

Zu Beginn der Installation haben Sie die Möglichkeit, Ihren PC über das **Cleanup Tool** auf evtl. vorhandene Infektionen überprüfen zu lassen. Dieser Punkt kann auch übersprungen werden.

Zu Beginn der Installation werden Sie zuerst nach dem Abonnementschlüssel gefragt.

Sobald Ihr Schlüssel erfolgreich überprüft wurde, kann die Installation beginnen. Durch bestätigen des Buttons „Akzeptieren und installieren“ beginnt die Installation.

Alle erforderlichen Dateien werden nun im Hintergrund runtergeladen

Die Installation wird nach Fertigstellung automatisch mit dem Startbildschirm beendet.

Sie haben nun F-Secure Internet-Security erfolgreich installiert.

Wo finde ich den Produktabonnementschlüssel?

1. Klicken Sie auf das Produktsymbol in der Taskleiste. Das Fenster der Sicherheits-Anwendung wird geöffnet.
2. Klicken Sie auf ? , und wählen Sie Mein Abonnement anzeigen. Das Fenster mit Ihren Abonnements wird geöffnet.
3. Klicken Sie auf den Link Abonnementschlüssel anzeigen. Der Abonnementschlüssel wird unter „Abonnementenschlüssel“ angezeigt.

Kann ich meine Lizenz auf einen neuen PC oder Betriebssystem übernehmen?

Wenn Sie die Software auf einem zweiten Computer installieren, erhalten Sie automatisch die Mitteilung, dass keine Lizenz mehr verfügbar ist. Sollten Sie eine weitere Lizenz benötigen, wenden Sie sich an uns.

Sie können uns hierzu per Mail über f-secure@edv-buchversand.de oder telefonisch unter 02191/99 11 99 erreichen.

Sie werden in einer Meldung darüber informiert, dass keine Lizenz mehr verfügbar ist. Nur wenn Sie die Software künftig nur noch auf dem zweiten Computer verwenden möchten, können Sie bedenkenlos die Option „Lizenz erneut verwenden“ auswählen.

Falls nicht, können Sie das Problem beheben, indem Sie das Produkt auf beiden Computern deinstallieren und anschließend auf dem ersten Computer eine Neuinstallation durchführen. Damit wird das Abonnement auf diesem Computer wieder aktiviert.

ⓘ Vergewissern Sie sich vor Eingabe des Abonnementschlüssels, dass eine Verbindung zum Internet besteht, da der Schlüssel von F-Secure online überprüft wird

Ich habe mein F-Secure Internet Security verlängert. Wo kann ich meinen neuen Abonnementschlüssel eingeben?

Wenn Sie einen neuen Abonnementschlüssel für das Produkt erhalten haben, müssen Sie diesen online aktivieren.

Gehen Sie folgendermaßen vor, um das neue Abonnement zu aktivieren:

- Klicken Sie auf das Produktsymbol in der Taskleiste. Das Fenster der F-Secure-Anwendung wird geöffnet.
- Klicken Sie auf ? und wählen Sie Mein Abonnement anzeigen. Das Fenster mit Ihren Abonnements wird geöffnet
- Klicken Sie unten mittig auf den Button „Neues Abonnement hinzufügen
- Geben Sie Ihren Abonnementschlüssel ein, und klicken Sie auf weiter.

Was ist der Browser-Schutz?

Browser-Schutz hilft Ihnen beim sicheren Surfen im Internet, indem Sicherheitsbewertungen für Websites in Ihrem Browser zur Verfügung gestellt werden und der Zugang zu als gefährlich bewerteten Websites blockiert wird.

Welcher Vorteil bringt mir der Banking-Schutz?

F-Secure hat im November 2012 die Banking-Schutz-Funktion in F-Secure Internet Security eingeführt und mit den Jahren weiter verbessert.

Banking-Schutz ist eine weitere Sicherheitsebene in F-Secure Internet Security. Sobald eine Online-Banking-Seite in einem Webbrowser geöffnet wird, wird der Banking-Schutz automatisch aktiviert und die Sicherheitsstufe der Online-Sitzung wird erhöht. Bei der Aktivierung wird oben im Bildschirm eine Meldung angezeigt, dass der Banking-Schutz aktiviert wurde. Sobald der Banking-Schutz aktiviert wurde, werden alle neuen Verbindungen vom PC blockiert. Durch das Blockieren der Verbindungen sind Banking-Trojaner und andere Malware-Programme nicht in der Lage, Ihre persönlichen Informationen, wie beispielsweise Logins, an Kriminelle zu übermitteln.

Wie kann ich andere Websites während der Online-Banking-Sitzung zulassen?

Gehen Sie folgendermaßen vor, um während Ihrer Online-Banking-Sitzung Websites zuzulassen, die nichts mit Online-Banking zu tun haben:

1. Wählen Sie auf der Seite Virenschutz die Option Einstellungen. Anmerkung: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.
2. Wählen Sie Sicherheitseinstellungen > Banking-Schutz.
3. Klicken Sie unten auf den Button „Website-Ausnahmen anzeigen“
4. Im folgenden Fenster haben Sie nun die Möglichkeit, Webseiten zum Banking-Schutz hinzuzufügen oder abgelehnte wegzunehmen.

Wozu benötige ich den „Spielmodus“?

Mit dem Spielmodus können Sie die Nutzung Ihrer Systemressourcen durch das Produkt optimieren. Computerspiele benötigen oft große Systemressourcen, um einwandfrei zu funktionieren.

Wenn Sie den Spielmodus einschalten, wird die Auslastung des Hauptprozessors und des Netzwerks Ihres Computers gesenkt, wodurch mehr Systemressourcen für die Ausführung der Spiele auf Ihrem Computer zur Verfügung stehen. Die Funktionalität der Spiele bleibt dabei unverändert. So können beispielsweise automatische Updates oder andere Vorgänge, die große Prozessor- und Netzwerkressourcen in Anspruch nehmen, blockiert werden, solange der Spielmodus eingeschaltet ist.

Außerdem werden im Spielmodus keine Benachrichtigungen oder Wartungscenter-Popups angezeigt. Wichtige Benachrichtigungen werden nur dann angezeigt, wenn sie unmittelbar relevant sind oder eine Aktion erfordern. Alle übrigen Benachrichtigungen werden erst nach Beenden des Spielmodus angezeigt. Das ist auch bei ausgeschaltetem Spielmodus bei allen anderen Full-Screen-Anwendungen der Fall, beispielsweise, wenn Sie eine Präsentation, eine Slideshow oder ein Video im Full-Screen-Modus schauen.

Wie kann ich den Spielmodus aktivieren?

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

1. Wählen Sie im Startfenster > Spielmodus.
2. Die Nutzung von Systemressourcen durch das System ist jetzt optimiert, damit Spiele reibungslos auf Ihrem Computer laufen. Sie erkennen an dem aktivierten Kontrollkästchen ✓ neben dem Menüelement Spielmodus ob der Modus aktiviert ist.

So deaktivieren Sie den Spielmodus:

1. Er wird automatisch deaktiviert, wenn Sie Ihren Computer neu starten oder aus dem Standby-Modus wechseln.
2. Sie können ihn auch über das Startfenster deaktivieren > Spielemodus.

Was ist DeepGuard?

DeepGuard überwacht Anwendungen, um potenziell gefährliche Änderungen für das System zu ermitteln. Es stellt sicher, dass Sie nur sichere Anwendungen nutzen.
Die Sicherheit einer Anwendung wird durch den vertrauenswürdigen Cloud-Service verifiziert. Wenn die Sicherheit einer Anwendung nicht verifiziert werden kann, beginnt DeepGuard mit der Überwachung der Anwendung.

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

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

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

So stellen Sie sicher, dass DeepGuard is aktiviert ist:

1. Klicken Sie auf das F-Secure Symbol auf Ihren Desktop oder in der Taskleiste.
2. Klicken Sie auf Einstellungen unter Virenschutz. Das entsprechende Fenster wird geöffnet.
3. Klicken Sie hier auf DeepGuard.
4. Vergewissern Sie sich, das DeepGuard aktiviert ist: 

Entfernen des F-Secure-Produkts - Deinstallationstool

Das Tool entfernt alle installierten F-Secure-Produkte und sollte daher nicht nur mit größter Vorsicht für den F-Secure Policy Manager und damit verwaltete Produkte verwendet werden. Wenn Sie das Deinstallationstool auf einem Policy Manager-Server ausführen, ohne dass zuvor eine Datensicherung durchgeführt wurde, müssen Sie anschließend alles neu installieren.

Sie sollten das Deinstallationstool daher nur als allerletzte Möglichkeit verwenden, da es einige Risiken birgt. Sie können sich das Deinstallationspaket unter folgender Adresse herunterladen:
ftp://ftp.f-secure.com/support/tools/uitool/UninstallationTool.zip.

Überprüfen der Sicherheitssoftware auf die neuesten Updates

Automatische Updates
Die automatische Update-Funktion wird bei der Installation von F-Secure aktiviert. Das bedeutet, dass F-Secure bei bestehender Internetverbindung im Zweistundentakt automatisch eine Überprüfung auf die neuesten Updates durchführt und diese herunterlädt.

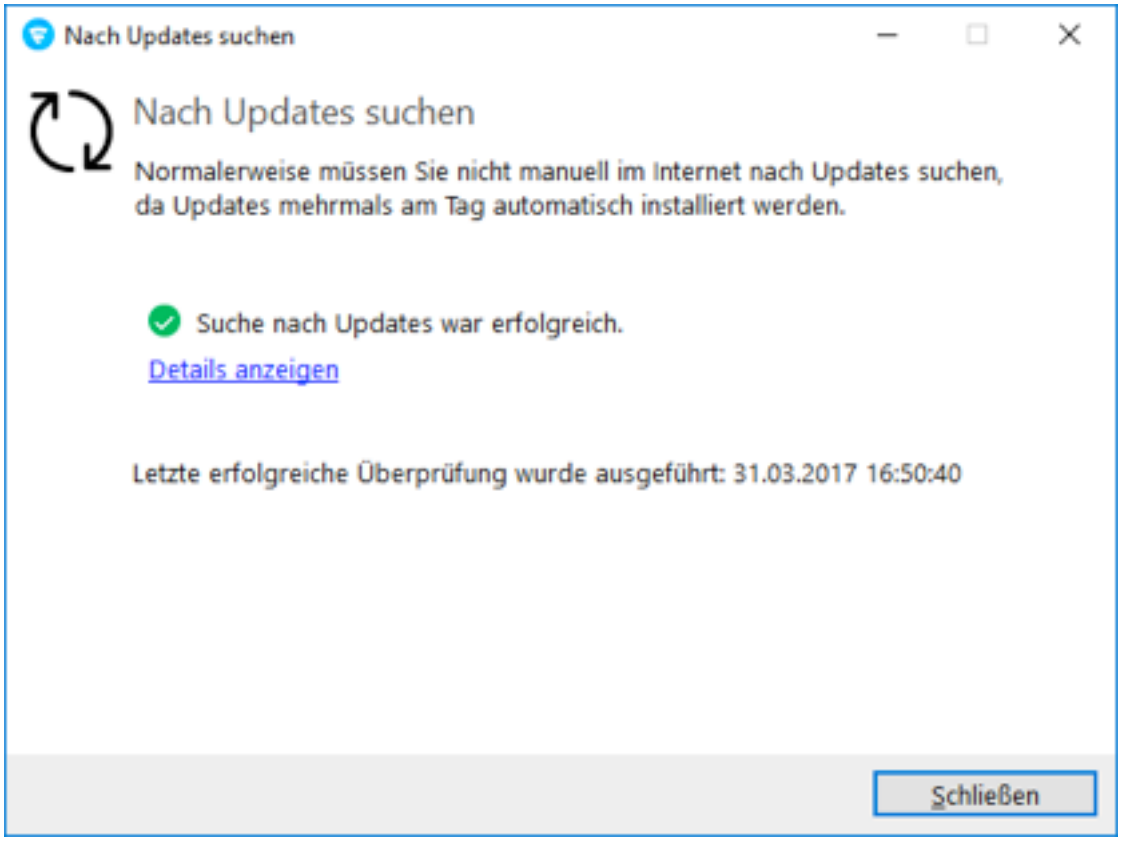
Das gesamte Update-Paket ist sehr groß; die Download-Geschwindigkeit ist abhängig von Ihrer Internetverbindung. Falls Ihr Computer in den letzten sieben Tagen nicht in Gebrauch war, wird das gesamte Update-Paket heruntergeladen und installiert. Dieser Vorgang dauert länger als bei regulären täglichen Updates.

Hinweis: Für schnelle Downloads empfehlen wir, mindestens einmal wöchentlich eine Internetverbindung herzustellen.

Manuelle Überprüfung auf Updates

Das Produkt empfängt die neuesten Updates automatisch, sobald Sie eine Internet-verbindung herstellen. So überprüfen Sie, ob Sie auch wirklich über die neuesten Updates verfügen:

- Klicken Sie in der Startansicht unter **Tools** auf den Button **Nach Updates suchen**.
- Das Fenster **Überprüfe auf Updates** wird angezeigt.
- Das Produkt sucht die neuesten Updates und installiert sie.



Eine Anwendung kann nach der Installation des Produkts keine Verbindung mit dem Internet herstellen

Dieser Artikel informiert darüber, was Sie tun können, wenn eine Anwendung nach der Installation von F-Secure keine Verbindung zum Internet herstellen kann.
Problembeschreibung:
Manchmal kann eine Anwendung nach der Installation von F-Secure keine Verbindung zum Internet herstellen.
Möglicherweise wird die Verbindung durch die Anwendungssteuerung abgelehnt.

Lösungen:

- Überprüfen Sie zunächst, ob eine Verbindung zum Internet besteht, und kontrollieren Sie anschließend die Anwendungssteuerung:
- Öffnen Sie die Startseite des Produkts.
- Klicken Sie auf **Tools**.
- Wählen Sie „**Windows Firewall-Einstellungen ändern“**.
- Es öffnet sich hier die Systemsteuerung der Windows Firewall
- Am linken Rand finden die die Option „Eine App oder Feature durch die Windows-Firewall zulassen
- Im nächsten Fenster finden Sie eine Aufstellung der Programme, die zugelassen oder abgelehnt werden. Hier können die Einstellungen separat geändert werden.
- Klicken Sie unten auf **OK**, um das Fenster zu schließen.

Wie kann ich feststellen, ob mein Computer geschützt ist und die automatischen Updates funktionieren?

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Haupt benutzeroberfläche zu öffnen.
2. Die Registerkarte Status zeigt einen kurzen Überblick über die Sicherheits-funktionen und ihren aktuellen Status.

Status-Symbol	Statusname	Beschreibung
	OK	Ihr Computer ist geschützt. Die Funktion ist aktiviert und arbeitet einwandfrei.
	Informationen	Das Produkt informiert Sie über einen speziellen Status einer Funktion. Dieses Symbol wird beispielsweise angezeigt, wenn eine Funktion aktualisiert wird.
	Warnung	Ihr Computer ist nicht vollständig geschützt. Beispielsweise wurde das Produkt längere Zeit nicht aktualisiert oder der Status einer Funktion erfordert Ihre Aufmerksamkeit.
	Fehler	Ihr Computer ist nicht geschützt. Beispielsweise ist Ihr Abonnement abgelaufen oder eine wichtige Funktion ist deaktiviert.

Was kann ich tun, wenn das Produkt anzeigt, dass die Virendefinitionen veraltet sind?

Aktualisierungen werden nach sieben Tagen als veraltet betrachtet. Sie sollten immer versuchen, Ihre Virendefinitionsdatenbank aktuell zu halten, da sich Viren sehr schnell ändern können. F-Secure kann mehrmals täglich Aktualisierungen herausgeben.

Wenn der Computer in den letzten sieben Tagen zum ersten Mal eingeschaltet wurde, z.B. nach einem Urlaub, wird das gesamte Update-Paket automatisch heruntergeladen und innerhalb von 30 Minuten installiert.

Wenn das Produkt weiterhin angibt, dass die Virendefinitionen veraltet sind, probieren Sie Folgendes:

1. Klicken Sie mit der rechten Maustaste auf das Produktsymbol in der Taskleiste, und wählen Sie im angezeigten Popup-Menü Nach Updates suchen.
2. Klicken Sie mit der rechten Maustaste auf das Produktsymbol in der Taskleiste, und wählen Sie Meine Abonnements anzeigen. Im Fenster „Abonnementschlüssel“ können Sie den Status Ihres Abonnements überprüfen.
3. Überprüfen Sie, dass Windows-Datum und -Uhrzeit korrekt sind, da falsche Einstellungen dazu führen können, dass das Produkt meldet, dass Ihre Viren-definitionen veraltet seien, obwohl dies nicht der Fall ist. Sie können Datum und Uhrzeit in der Windows-Taskleiste sehen. Sie können die Uhrzeiteinstellungen in den Eigenschaften für Datum und Uhrzeit ändern. Zum Öffnen der Eigen schaften klicken Sie auf die Uhr.

Wenn die oben genannten Schritte nicht helfen, empfehlen wir, das Produkt zuerst zu deinstallieren und dann neu zu installieren.

Einrichten eines geplanten Prüfvorgangs

Sie können das Programm so einstellen, dass Ihr Computer in regelmäßigen Zeitab-ständen überprüft wird, z.B. wöchentlich, täglich oder monatlich. So starten Sie einen geplanten Prüfvorgang:

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzer-oberfläche zu öffnen.
2. Klicken Sie auf Einstellungen im Bereich Virenschutz
3. Wählen Sie unter „Sonstige Einstellungen“ die Option Geplantes Scannen.
4. Schieben Sie den Regler nach rechts, um „Geplantes Scannen“ zu aktivieren: 

5. Wählen Sie, an welchen Tagen regelmäßig nach Viren und Spyware gesucht werden soll:

Option	Beschreibung
Täglich	Für eine tägliche Überprüfung.
Wöchentlich	Für eine Überprüfung an ausgewählten Wochentagen. Wählen Sie in der Liste auf der rechten Seite die Tage aus, an denen eine Überprüfung erfolgen soll.
Monatlich	Für eine Überprüfung an bis zu drei Tagen im Monat. Zum Auswählen der Tage: 1. Wählen Sie eine der Optionen unter Tag. 2. Wählen Sie den Tag des Monats aus der Liste neben dem ausgewählten Tag aus. 3. Wiederholen Sie die Schritte, wenn Sie an einem weiteren Tag eine Überprüfung durchführen möchten.

6. Wählen Sie, wann die Überprüfung an den ausgewählten Tagen beginnen soll:

Option	Beschreibung
Startzeit	Der Zeitpunkt, an dem die Überprüfung beginnt. Wählen Sie eine Uhrzeit, zu der Sie den Computer voraussichtlich nicht verwenden.
Nachdem der Computer nicht verwendet wurde für	Wählen Sie eine Ruheperiode, nach der der Prüfvorgang startet, wenn der Computer nicht verwendet wird.

7. Klicken Sie auf OK.

Wie kann ich eine Anwendung vom Scannen ausschließen?

Anwendungen können nicht direkt ausgeschlossen werden. Neue Anwendungen werden erst dann in die Ausschlussliste aufgenommen, wenn Sie sie während des Scannens ausgeschlossen haben.

Wenn während des Scannens eine Anwendung erkannt wird, die sich wie Spyware oder Riskware verhält, von der Sie jedoch wissen, dass sie sicher ist, können Sie diese vom Scannen ausschließen, sodass das Produkt keine Warnungen mehr ausgibt. Wenn sich eine Anwendung jedoch wie ein Virus oder bösartige Software verhält, kann diese nicht ausgeschlossen werden.

Sie können die Anwendungen anzeigen, die Sie vom Scannen ausgeschlossen haben und diese aus der Liste der ausgeschlossenen Elemente entfernen, wenn sie zukünftig gescannt werden sollen. So zeigen Sie die vom Scannen ausgeschlossenen Anwendungen an:

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzer-oberfläche zu öffnen.
2. Klicken Sie auf Einstellungen im Bereich Virenschutz.
3. Sie haben mehrere Möglichkeiten:
   - ➜ Wählen Sie unter „Sicherheitseinstellungen“ die Option „Virenschutz“.
   - ➜ Wählen Sie unter „Sonstige Einstellungen“ die Option „Manuelles Scannen“.
4. Klicken Sie auf den Link „Quarantäne anzeigen“. Das Dialogfeld „Vom Scanning ausschließen“ wird angezeigt.
5. Auf der Registerkarte Anwendungen werden die vom Scannen ausgeschlossenen Anwendungen angezeigt.

Bereinigen von Adware-Dateien

Was ist Adware?

Bei einer „Advertising-Supported Software“, kurz Adware, kann es sich um eine beliebige Software handeln, die Anzeigen einblendet. Adware wird oftmals auch als Spyware eingestuft. Häufig sind auf Computern viele Adware-Dateien vorhanden, insbesondere dann, wenn der Benutzer den Internet Explorer zum Surfen verwendet. Adware kann versehentlich über eine Webseite oder während der Installation einer kostenlosen Software mit gebündeltem Adware-Paket auf Ihrem Computer installiert werden. So enthalten z.B. einige Peer-to-Peer-Clients wie Kazaa und Grokster gebündelte Adware.

Bereinigen von Adware-Dateien

Wenn Ihnen während des Browsens im Internet unerwünschte Popups angezeigt werden oder Sie auf Ihrem Computer eine ungewöhnliche Aktivität entdecken, ist auf Ihrem Computer möglicherweise Adware vorhanden.
Ihr F-Secure-Produkt entfernt Adware normalerweise automatisch. Um sicherzugehen, sollten Sie jedoch einen Viren- oder Spyware-Scan ausführen:

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzeroberfläche zu öffnen.
2. Wählen Sie Virenscan. Der Scanassistent wird gestartet.
3. Befolgen Sie die Anweisungen des Assistenten, um den Scan abzuschließen.

Sollten Sie Adware finden, die nicht von Ihrem F-Secure-Produkt entdeckt wurde, schicken Sie uns ein Beispiel. Verwenden Sie hierfür das **Sample Analysis System:** https://www.f-secure.com/en/web/labs_global/submit-a-sample

Wie kann ich allen Netzwerkverkehr vorübergehend zulassen?

Wenn Sie die Firewall deaktivieren, lassen Sie den gesamten Netzwerkverkehr zu.

Warnung: Es wird empfohlen, die Firewall immer aktiviert zu lassen. Wenn Sie die Firewall deaktivieren, ist Ihr Computer durch Netzwerkangriffe gefährdet. Wenn eine Anwendung nicht mehr funktioniert, weil sie keine Verbindung zum Internet herstellen kann, ändern Sie die Firewall-Einstellungen, anstatt die Firewall zu deaktivieren.

So aktivieren oder deaktivieren Sie die Firewall:

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzer-oberfläche zu öffnen.
2. Auf der Registerkarte Virenschutz wählen Sie Einstellungen.
   Hinweis: Zum Deaktivieren von Sicherheitsfunktionen müssen Sie Administrator rechte besitzen.
3. Wählen Sie in den Sicherheitseinstellungen Firewall aus.
4. Klicken Sie auf den entsprechenden Schieberegler, um die Firewall mit Ein  bzw. Aus  zu aktivieren oder deaktivieren.

Wie kann ich den Browser-Schutz aktivieren bzw. deaktivieren

Wenn der Browser-Schutz aktiviert ist, wird der Zugriff auf schädliche Websites blockiert.

Aktivieren des Browser-Schutzes

Wenn der Browser-Schutz aktiviert ist, blockiert er den Zugriff auf schädliche Websites.
So stellen Sie sicher, dass der Browser-Schutz aktiviert ist:

1. Wählen Sie auf der Seite Virenschutz die Option Einstellungen.
2. Anmerkung: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.
3. Wählen Sie Sicherheitseinstellungen > Browser-Schutz.
4. Aktivieren Sie die Option Browser-Schutz.
5. Wenn Ihr Browser geöffnet sie, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

Verwenden von Reputationswert-Symbolen

Der Browser-Schutz kann bei Suchergebnissen von Google, Yahoo oder Bing die Reputationswerte von Websites anzeigen.

So zeigen Sie in Suchergebnissen Reputationswert-Symbole an:

1. Wählen Sie auf der Seite Virenschutz die Option Einstellungen.
   Anmerkung: Sie benötigen Administratorrechte, um die Einstellungen zu ändern.
2. Wählen Sie Sicherheitseinstellungen > Browser-Schutz.
3. Stellen Sie sicher, dass der Browser-Schutz aktiviert ist.
4. Wählen Sie Reputationswerte für Websites in Suchergebnissen anzeigen.

Wenn Ihr Browser geöffnet sie, starten Sie ihn neu, um die geänderten Einstellungen wirksam werden zu lassen.

Wie kann ich alle meine Sicherheitsfunktionen deaktivieren?

Sie sollten die Sicherheitsfunktionen nicht deaktivieren, da Ihr Computer dadurch Angriffen ausgesetzt sein kann. Sollten Sie jedoch alle Sicherheitsfunktionen des Produkts deaktivieren müssen, gehen Sie wie folgt vor.

Deaktivieren aller Sicherheitsfunktionen

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzeroberfläche zu öffnen.
2. Wählen Sie die Registerkarte Tools.
3. Wählen Sie Alle Sicherheitsfunktionen deaktivieren.
   Hinweis: Es wird eine Warnmeldung angezeigt, da Ihr Computer durch das Deaktivieren aller Sicherheitsfunktionen Angriffen ausgesetzt sein kann.
4. Bestätigen Sie Ihre Auswahl mit Deaktivieren.

Aktivieren aller Sicherheitsfunktionen

1. Klicken Sie auf das Produktsymbol in der Taskleiste, um die Hauptbenutzeroberfläche zu öffnen.
2. Alle Sicherheitsfunktionen werden aktiviert, wenn die Hauptbenutzeroberfläche geöffnet wird.

Wie kann ich einen vollständigen Computerscan durchführen?

Führen Sie einen vollständigen Computerscan durch, wenn Sie sicher sein möchten, dass sich keine Malware oder Riskware auf Ihrem Computer befindet. Diese Art von Scan dauert am längsten. Er kombiniert den schnellen Malware-Scan und den Festplattenscan. Dieser Scan sucht auch nach Objekten, die möglicherweise durch ein Rootkit versteckt sind.

So führen Sie einen vollständigen Computerscan durch

1. Klicken Sie auf das Produktsymbol, um das Produkt zu öffnen.
2. Klicken Sie auf Tools > Virenscan-Optionen, und wählen Sie **vollständiger Scan des Computers**.
3. Der Scan wird nun automatisch gestartet:

Was ist Ransomware und wie schützen Sie sich davor?

Stellen Sie sich vor, Sie verlieren alle Fotos, Videos und Nachrichten, die auf Ihrem Computer gespeichert sind. Wie viel wären Sie bereit, zu zahlen, um das alles zurückzubekommen? Ransomware ist eine Malware, die Ihren Computer infiziert, sperrt und dann Geld dafür verlangt, ihn zu entsperren. Im Folgenden finden Sie unsere Kurzanleitung zu Ransomware. Sie erfahren, worum es geht und Sie erhalten fünf Tipps, wie Sie verhindern, dass Sie Opfer von Ransomware werden.

Was macht Ransomware?

Crypto-Ransomware verschlüsselt die Dateien auf einem Computer und chiffriert im Prinzip die Inhalte einer Datei, damit Sie sie ohne einen Schlüssel, der die Datei korrekt dechiffrieren kann, nicht mehr öffnen können. Um den Schlüssel zu erhalten, müssen Sie eine Art Lösegeld zahlen. Sobald die Malware einen Computer infiziert hat, kann sie sich auf weitere Geräte im Netzwerk ausbreiten und so den Betrieb lahmlegen. Das Lösegeld beträgt in der Regel 300 bis 500 US-Dollar für einen Computer und muss oft in Bitcoins gezahlt werden, eine virtuelle Währung, die sich schwer nachverfolgen lässt.

Wie kann Ransomware Ihren Computer infizieren?

Es gibt mehrere Möglichkeiten, wie Ransomware auf Ihren Computer gelangen kann: als E-Mail-Anhang, schädliche Links oder über Exploit Kits.
Sie können mit Exploit Kits in Berührung kommen, wenn Sie eine infizierte Website besuchen, auf eine infizierte Werbeanzeige auf einer ansonsten unschädlichen Website klicken oder wenn Sie zu einer schädlichen Website weitergeleitet werden. Das Exploit Kit sucht auf Ihrem Computer nach Schwachstellen, die sich häufig in veralteter Software finden. Sobald es eine Lücke findet, lädt das Exploit Kit die Ransomware herunter und installiert sie auf Ihrem Computer. Dies kann passieren, ohne dass Sie etwas davon merken.

Wie bekommen Sie Ihre Dateien zurück?

F-Secure rät davon ab, das Lösegeld zu zahlen. Zwar ist das eine Möglichkeit, die Kontrolle über Ihren Computer und Ihre Daten zurückzuerlangen, aber wirksamer ist es, Vorkehrungen zu treffen, bevor Sie angegriffen werden, indem Sie regelmäßig Sicherungen erstellen. Wenn Sie dann angegriffen werden, können Sie gelassen bleiben und alle Ihre Daten aus den Sicherungen wiederherstellen. Und obwohl in den meisten Ransomware-Fällen die Kontrolle zurückerlangt wurde, ist das möglicherweise nicht immer so. Es kann durchaus sein, dass Sie zahlen, aber trotzdem nicht die Kontrolle zurückerhalten.

Wenn Ihre Dateien gekapert wurden und Sie keine Sicherungen haben, dann sollten Sie im Internet nach einem Entschlüsselungs-Tool für die Ransomware suchen, von der Sie angegriffen wurden. Diese Liste bietet einen guten Einstieg. Entschlüsselungs-Tools sind jedoch häufig nur für ältere Versionen verfügbar.

Bedenken Sie auch, dass Angreifer Ihre Vorgehensweise ändern und Ransomware verwenden, für die es kein Entschlüsselungstool gibt. Es kann auch hilfreich sein, wenn Sie Ihre Situation in einem Forum wie Bleeping Computer schildern. Dort finden Sie Threads, die Hilfe bei Locky, TeslaCrypt, CryptoWall, Petya, CryptXXX, Locker und vielen anderen Schadprogrammen bieten. Außerdem empfehlen wir, dass Sie den Vorfall den entsprechenden Behörden melden, in der Regel der Polizei.

5 Tipps: Schutz vor Ransomware

Vorsorge ist besser als Nachsorge. Dies gilt in jedem Fall auch für Ransomware. Hier sind unsere 5 besten Tipps, wie Sie Ihre Geräte vor Ransomware schützen:

Implementieren Sie eine solide Sicherheitslösung, die all Ihre Geräte umfasst (PCs, Macs, Smartphones und Tablets) und Schutz bietet. F-Secure Internet Security schützt vor allen bekannten Ransomware-Bedrohungen und kann auch ganz neue Zero-Day-Bedrohungen blockieren. Da in letzter Zeit immer mehr neue Ransomware-Varianten auftauchen, ist das sehr wichtig.

Führen Sie regelmäßig Sicherungen Ihrer Daten durch. Speichern Sie Sicherungen online, damit sie nicht infiziert werden können. Testen Sie die Wiederherstellung von Zeit zu Zeit, damit Sie sicherstellen, dass sie auch tatsächlich funktionieren. Wenn Sie über gute Sicherungen verfügen, können Sie bei einem Angriff schneller zum normalen Betrieb zurückkehren und müssen an die Verbrecher kein Geld zahlen. Acronis True Image ist hier unser Software-Tipp: www.acronis-shop.de

Achten Sie darauf, dass die Software auf all Ihren Geräten aktuell ist, um Schwachstellen zu vermeiden. Wenn Sie unsicher sind, wie Sie alles auf dem neuesten Stand halten, können Sie auch ein Tool nutzen, das alte Software erkennt und Updates vorschlägt.

Seien Sie bei E-Mail-Anhängen besonders vorsichtig, insbesondere bei ZIP-Dateien und Office-Dokumenten (Word, Excel und PowerPoint). Öffnen Sie keine E-Mail-Anhänge, die Ihnen jemand geschickt hat, den Sie nicht kennen. Deaktivieren Sie außerdem Makro-Skripte in allen Office-Dateien, die Sie per E-Mail erhalten.

Grenzen Sie die Verwendung von Browser-Plug-ins ein. Deaktivieren Sie Plug-ins, die häufig Schwachstellen aufweisen, beispielsweise Flash Player und Silverlight, wenn Sie sie nicht verwenden. Sie können diese über die Plug-in-Einstellungen in Ihrem Browser deaktivieren.

Bei Fragen zur Installation neuer Versionen, Fehlermeldungen oder Problemen stehen Ihnen unsere geschulten und von F-Secure zertifizierten Experten gerne zur Verfügung. Wir verschaffen Ihnen einen Überblick, wie Sie am besten vorgehen und was Sie beachten sollten.

Rufen Sie uns an unter 02191- 99 11 99 (Mo.-Fr. 8.30 - 17 Uhr)
oder schicken Sie Ihre Anfrage per E-Mail an f-secure@edv-buchversand.de.

Ihr Team vom

edv-buchversand.de